Masterarbeit

EVALUIERUNG DER OT-SECURITY IN TUNNELSTEUERUNGSSYSTEMEN

ausgeführt am

Fachhochschul-Masterstudiengang
Automatisierungstechnik-Wirtschaft

von
Anika Jaindl, BSc
2010322009

betreut und begutachtet von
Dipl.-Ing. Dr. techn. Florian Hollomey

Graz, im November 2021

.....
Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

Unterschrift

DANKSAGUNG

Meinem Freund Stefan, meinen Freundinnen und Freunden, meinem Vorgesetzten Stefan Fuchs, meinen Abteilungskolleg*innen und meiner gesamten Familie, besonders meiner Mama Claudia, meinem Bruder Julian und meiner lieben Schwägerin Nadine möchte ich herzlich für die ständige Unterstützung danken. Ein besonderer Dank gilt meinem Betreuer, Herrn Dipl.-Ing. Dr. techn. Florian Hollomey, für die ausgezeichnete Betreuung, die ständige Unterstützung mit seiner positiven Einstellung und für Rat und Tat in sämtlichen Angelegenheiten.

KURZFASSUNG

Industrielle Steuerungssysteme und somit die Operational Technology (OT) werden immer verletzlichere Angriffsziele. Da Industrieanlagen, ebenso Tunnelanlagen, größtenteils mit der Office-IT vernetzt sind und häufig auch eine Verbindung zum Internet aufweisen, besteht ein Fernzugriff, der ausgenutzt werden kann. Zusätzlich besteht die Möglichkeit, dass ein Eindringen über die physischen Schnittstellen stattfindet. Daher müssen für einen gesamtheitlichen Schutz entsprechende OT-Security-Prozesse angewendet werden.

Das Ziel dieser Arbeit ist die Verbesserung der zurzeit von der Dürr Austria GmbH verwendeten OT-Security-Prozesse in Tunnelsteuerungssystemen. Dazu werden die Informationssicherheit, mögliche Attacken und Angreifer*innen, sowie anwendbare Normen und Standards evaluiert. Der Fokus liegt dabei auf der IEC 62443, der Norm für die IT-Sicherheit für Netze und Systeme.

Die zurzeit angewendeten OT-Security-Prozesse werden definiert und darauf aufbauend Optimierungen aus den anwendbaren Teilen der IEC 62443 analysiert. Weitere Security-Maßnahmen werden mithilfe von ergänzenden Standards erforscht. Als Resultat werden die gefundenen Verbesserungsmaßnahmen zusammengeführt, um eine Integration in die Prozesse zu ermöglichen. Auf dieser gesamtheitlichen Basis wird das Defense-in-Depth-Modell definiert.

Die Ergebnisse dieser Arbeit werden in den bestehenden Informationssicherheitsprozess des Unternehmens betreffend der Tunnelsteuerungssysteme integriert.

ABSTRACT

Industrial control systems and therefore the Operational Technology (OT) have become more vulnerable goals for attackers. Due to the fact that these systems are linked with the Office IT and partly with the Internet hacking can occur easily. Additionally, the infiltration of the physical interfaces in the critical infrastructure of tunnels needs to be considered. For a holistic protection of the systems, defined OT security processes are inevitable.

The aim of this master thesis is to enhance the current OT security processes in tunnel control systems of Dürr Austria GmbH. Therefore, information security, possible attacks and attackers, as well as potentially usable standards with focus on the IEC 62443, which deals with security for industrial automation and control systems, are evaluated.

The currently used OT security processes are defined and optimization processes resulting from the applicable parts of the IEC 62443 are analysed. Further security actions were found in additional standards. All the results of the various standards are merged for a uniform integration in the processes resulting in the creation of a holistic defence in depth model.

The recommended measurements will be integrated in the organisation’s existing information security process regarding the tunnel control systems.

INHALTSVERZEICHNIS

1 EINLEITUNG

> „Das Thema Cybersicherheit und Cyberkriminalität ist in Österreich mittlerweile fast täglich präsent, und die Bewusstseinsbildung hat sich im vergangenen Jahr, in Zeiten der Pandemie, durch den enormen Digitalisierungsschub und die stetige Weiterentwicklung neuer Technologien erhöht. […] Die Anzahl jener Unternehmen, die von Datenangriffen betroffen ist, ohne es je zu bemerken, ist also hoch. Wie man es auch dreht und wendet, im Bereich Cybersecurity besteht deutlicher Handlungsbedarf.“[1]

Cyberangriffe sind längst keine Seltenheit mehr, unabhängig davon, ob es sich um die Informationstechnologie (Information Technology, *IT*) oder die Betriebstechnologie (Operational Technology, *OT*) handelt. Angriffe auf OT-Systeme werden jedoch durch die zunehmende Vernetzung der Industrieanlagen immer lukrativer und häufiger. Daher muss die OT-Security auch in Tunnelsteuerungssystemen künftig viel umfassender behandelt und berücksichtigt werden, um jegliche Personenschäden und längerfristige Ausfälle von Anlagen weitestgehend vermeiden zu können.

1.1 Motivation

Die Informationssicherheit, sie umfasst IT-, und OT-Security, wird vor allem in den kritischen Infrastrukturen immer wichtiger, zu welchen auch Tunnelanlagen zählen. Daher wurde das Netz- und Informationssystemsicherheits-Gesetz (NIS-Gesetz, *NISG*), infolge der entsprechenden EU-Richtlinie verabschiedet, in welchem der Umgang mit der Informationssicherheit in kritischen Infrastrukturen vorgegeben wird. Von Seiten des Auftraggebers (*AG*) werden somit die Konformität mit diesem Gesetz und die damit einhergehenden gesteigerten Sicherheitsansprüche gefordert. Im Unternehmen Dürr Austria GmbH wird bereits auf die Informationssicherheit und die Forderungen des Auftraggebers geachtet. Dabei wird jedoch großteils nur auf die ISO/IEC 27001, die Norm für die Anforderungen an Informationssicherheitsmanagementsysteme, und damit einhergehend auf die IT-Security Bezug genommen. Die OT-Security wurde bisweilen kaum bewusst berücksichtigt, stellt aber eine große Relevanz in Tunnelanlagen dar und muss ebenso kontinuierlich adaptiert werden. Die Basis der OT-Security bildet die Operational Technology, die sich mit Komponenten auf allen Automatisierungsebenen in Industrieanlagen, befasst.

1.2 Problemstellung

Cyberangriffe werden aus unterschiedlichen Motiven immer häufiger durchgeführt. Das Bewusstsein für die Gefahr solcher Angriffe wird immer stärker, vor allem in Bezug auf die IT-Sicherheit in der Office-IT. Industrieanlagen und somit die OT-Sicherheit werden dabei sehr oft in den Hintergrund gerückt, oder sogar vergessen. Diesen ist aber zumindest die gleiche Aufmerksamkeit zu widmen.

[1] Breuss/Lukac/Tonweber/Weissmann (2021), Online-Quelle [25.11.2021].

Durch Industrie 4.0 und dem Internet der Dinge (Internet of Things, *IoT*) werden OT-Systeme immer beliebtere Angriffsziele mit weitaus größeren Auswirkungen auf die Verfügbarkeit kritischer Systeme, die im schlimmsten Fall Konsequenzen auf Menschenleben haben können.

Da die OT und die IT immer mehr miteinander verschmelzen, können viele Backdoors, das sind beabsichtigte Umgehungen des Zugriffsschutzes, auf beide Kategorien angewendet werden. Daher muss so gut wie möglich eine Linie gefunden werden, die aufzeigt in welche Kategorie sich die jeweiligen Komponenten der Tunnelanlagen zuordnen lassen.

Da Verfügbarkeitseinschränkungen oder Angriffe in der kritischen Infrastruktur katastrophal enden können, ist die OT-Security von immer größer werdendem Interesse und steigender Relevanz. Dazu wurde die IEC 62443, die Norm für IT-Sicherheit für industrielle Automatisierungssysteme, eingeführt. Diese muss auf Anwendbarkeit im Unternehmen untersucht werden. Unabhängig davon sind weitere Normen und Richtlinien, die dieses Thema behandeln, zu prüfen und auf Synergien oder zusätzlichen Vorgaben zur IEC 62443 zu erforschen. Dafür werden zuvor mögliche Angriffe evaluiert, um die entsprechenden Maßnahmen ableiten zu können.

1.3 Zielsetzung

Die Zielsetzung dieser Arbeit ist es die OT-Security, zusätzlich zur IT-Security, im Unternehmen zu optimieren und dabei möglichst normkonform vorzugehen. Als Resultat soll hervorgehen, welche Teile der IEC 62443 anwendbar sind. Zusätzlich soll es eine Erläuterung geben, welche ergänzenden Normen noch anwendbar sind.

Im Großen und Ganzen soll ein einheitliches Gesamtbild zur OT-Security in Tunnelsteuerungssystemen der Dürr Austria GmbH als Resultat hervorgehen. Dabei sollen die Umsetzungsmöglichkeiten und -maßnahmen berücksichtigt sein. Die gefundenen Ergebnisse werden in den Unternehmensstandard integriert. Somit soll die Angriffsfläche für Attacken auf Tunnelanlagen weiter minimiert werden.

1.4 Unternehmen

Die Dürr Austria GmbH tritt als Spezialist im Infrastruktur-Anlagenbau und der Verkehrsleittechnik auf. In den letzten 40 Jahren hat das Unternehmen 274.894 Tunnelmeter mit Sicherheitstechnik in über 250 Projekten ausgestattet.[2]

Zu den Kernkompetenzen zählen das Projekt- und Sitemanagement, Planungs- und Dokumentationsleistungen, die Montage auf der Baustelle und die Prozessleittechnik mit allen damit verbundenen Aktivitäten: von der Pflichtenhefterstellung, der System-Programmierung, der Systemvisualisierung bis hin zur Inbetriebnahme des Gesamtsystems.[3]

[2] Vgl. Dürr Austria GmbH 1 (2021), Online-Quelle [25.11.2021].

[3] Vgl. Dürr Austria GmbH 2 (2021), Online-Quelle [25.11.2021].

1.5 Begriffserklärungen

Um ein Verständnis für benötigte Begriffe in den folgenden Kapiteln zu schaffen, werden relevante Terminologien definiert. Somit wird eine einheitliche Grundlage geschaffen.

1.5.1 Informationstechnologie (IT)

Die Informationstechnologie beschreibt alle technischen Ressourcen zur Generierung, Speicherung, Archivierung und Verwendung von digitaler Information. Als Grundlage dafür werden Hardware, Software und Kommunikationsnetze benötigt.[4]

Die Kommunikationsnetze basieren auf der Kommunikationstechnologie. Damit sind sämtliche Methoden, Grundlagen und Prinzipien zum Daten- und Informationsaustausch gemeint. Für den organisierten Umgang mit den Datenmengen steht der Begriff Datenverarbeitung, welcher für die IT wesentlich ist, da diese für einen äußerst innovativen Prozess der digitalen Datenverarbeitung steht.[5]

1.5.2 Operational Technology (OT)

Die Operational Technology beschreibt nach der Definition des National Institute of Standards and Technology (*NIST*) programmierbare Systeme oder Geräte, die mit einer physischen Umgebung interagieren. Das umfasst eine direkte Änderung durch die Überwachung und/oder Steuerung von Geräten und Prozessen oder die Detektion von Ereignissen.[6]

Der Begriff wird von Gartner[7] gleichwertig beschrieben.

Dabei waren OT-Systeme in der Vergangenheit abgekapselte OT-Netzwerke mit zahlreichen proprietären Protokollen. Heutzutage stehen die speicherprogrammierbaren Steuerungen (*SPS*) immer häufiger mit TCP/IP-Netzwerken in Verbindung, wodurch die Sicherheitsrisiken stets zunehmen.[8]

1.5.3 Industrielle Steuerungssysteme (ICS)

Industrielle Steuerungssysteme (Industrial Control Systems, *ICS*) sind Steuerungssysteme zur Überwachung und Steuerung von Prozessen in industriellen Anlagen.[9] Sie sind Teil der OT, wobei Supervisory Control and Data Acquisition (*SCADA*) und Distributed Control Systems (*DCS*) Bestandteile von Industrial Control Systems sind.[10]

---

[4] Vgl. Lachenmaier/Kemper (2020), Online-Quelle [25.11.2021].

[5] Vgl. Eigner/Gilz/Gerhardt/Nem (2012), S. 2.

[6] Vgl. NIST SP 800-37 Revision 2 (2018), S. 101.

[7] Vgl. Gartner, Inc. (2021), Online-Quelle [25.11.2021].

[8] Vgl. TKmag (2021), Online-Quelle [25.11.2021].

[9] Vgl. Wege/Porwitzki (2020), Online-Quelle [25.11.2021].

[10] Vgl. Securicon Team (2019), Online-Quelle [25.11.2021].

Zur Veranschaulichung soll die nachstehende Abbildung dienen:

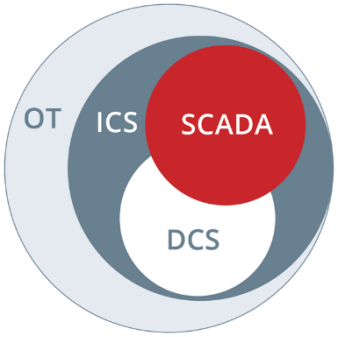

Abb. 1: Teile der OT (OT: Operational Technology, ICS: Industrial Control Systems, SCADA: Supervisory Control and Data Acquisition, DCS: Distributed Control Systems), Quelle: Securicon Team (2019), Online-Quelle [25.11.2021].

Die Definitionen von OT und ICS sind sehr ähnlich und werden oft auch gleichwertig verwendet. Versucht man die beiden Begriffe abzugrenzen, bezieht sich die OT auf jegliche Hard- und Software, die Änderungen überwachen oder anstoßen und der Begriff ICS behandelt gesamte Computersysteme, die Prozesse steuern.[11]

Bei SCADA-Systemen werden über ein zentrales Kontrollzentrum weitläufig verteilte Assets gesteuert und deren Feldinformationen gesammelt. Für das zentrale Monitoring und die Steuerung in beinahe Echtzeit wird ein Human-Machine Interface (*HMI*) verwendet. Die Steuerung einer Aufgabe kann sowohl automatisch als auch durch Bediener stattfinden. Typische verteilte Hardware von SCADA-Systemen sind Control Server im Control Center, jegliches Kommunikationsequipment wie zum Beispiel Switches oder Remote Terminal Units (*RTU*), sowie Programmable Logic Controller (*PLC*, Speicherprogrammierbare Steuerung, SPS). Die Software beinhaltet akzeptable Grenzwerte und das Verhalten bei Über- und Unterschreitung von Grenzwerten. Alarming, Reporting und Trend-Analysen sind ebenfalls zentralisiert. Die Steuerung von Aktuatoren und die Überwachung von Sensoren finden wiederum lokal statt.[12]

DCS finden Einsatz bei der Steuerung von Produktionssystemen innerhalb der gleichen geographischen Lage. Sie werden hauptsächlich für die Prozesssteuerung, oder für Steuerungssysteme von diskreten Teilen eingesetzt. Die vielen Subsysteme, welche für die detaillierte Steuerung verantwortlich sind, werden mittels einer Steuerungsebene überwacht. Die Prozesskonditionen und Schlüsselprodukte werden automatisch bei der Erreichung der Grenzwerte von Sollwerten erzielt. Die PLCs werden so getunt, dass sie innerhalb der gewünschten Toleranzgrenzen bleiben. Der automatische Ablauf ist durch die Feedback- bzw. Feedforward-Meldungen des Kontrollsystems möglich.[13]

[11] Vgl. Abercrombie (2019), Online-Quelle [25.11.2021].

[12] Vgl. NIST SP 800.82 Rev. 2 (2015), S. 2-5 f.

[13] Vgl. NIST SP 800.82 Rev. 2 (2015), S. 2-10.

1.5.4 Cyberphysische Systeme (CPS)

Cyberphysische Systeme (Cyber Physical Systems, *CPS*) steuern über ein Netzwerk physische Maschinen oder Anlagenteile in Echtzeit. Diese Systeme stehen in direktem Zusammenhang mit der Industrie 4.0 und dem Internet der Dinge.[14]

1.5.5 IT/OT-Konvergenz

Die Bedeutung von Sicherheit unterscheidet sich für IT und OT, da die beiden Sparten andere Anforderungen an die Produktivität, die Relevanz von Daten und den Produktlebenszyklus haben. Jedoch entwickeln sie sich ständig weiter und wachsen durch die Industrie 4.0 und das Internet of Things immer weiter zusammen. Da die beiden Bereiche beinahe dieselben Sicherheitsanforderungen haben, welche mit unterschiedlichen Blickwinkeln betrachtet werden, ergibt sich eine Kluft, welche beseitigt werden muss.[15]

Die zunehmende Vernetzung wird zusätzlich durch das industrielle Internet der Dinge (Industrial Internet of Things, *IIoT*) vorangetrieben.[16]

Die IT/OT-Konvergenz beschreibt eine direkte Steuerung beider Systeme. Da IT und OT unterschiedliche Anforderungen haben, muss eine entsprechende Zuordnung der Komponenten stattfinden. Das ist vor allem für das Netzwerkdesign von Vorteil, um IT- und OT-Netzwerk voneinander bestmöglich getrennt zu halten.[17]

Die Konvergenz wurde vor allem durch die COVID-Krise sichtbar, da durch vermehrtes Homeoffice über die IT-Systeme von der Ferne auf OT-Systeme zugegriffen wird. Dadurch wird auch die Angriffsfläche vergrößert und das Ziel attraktiver. Daher werden in Unternehmen gesamtheitliche Maßnahmen zur Risikominimierung empfohlen.[18]

Ob die Kluft durch eine strikte Trennung oder eine Vermischung der beiden Bereiche beseitigt wird, kann sich je nach Anwendungsfall unterscheiden. Jedoch ist eine Einteilung in die Bereiche ein erster Schritt, um Klarheit zu schaffen und somit mögliche Synergien zu generieren.

1.5.6 Industrielle Informationstechnologie (IIT)

Die industrielle Informationstechnologie (Industrial Information Technology, *IIT*) wird als Schnittstelle zwischen IT und OT erwähnt.[19] Jedoch wird diese auch als Synonym für die OT verwendet.[20]

[14] Vgl. Bendel (2021), Online-Quelle [25.11.2021].

[15] Vgl. Beeson (2020), Online-Quelle [25.11.2021].

[16] Vgl. ComputerWeekly.de (2020), Online-Quelle [25.11.2021].

[17] Vgl. Nolle (2019), Online-Quelle [25.11.2021].

[18] Vgl. Antova (2021), Online-Quelle [25.11.2021].

[19] Vgl. Indu-Sol GmbH (2021), Online-Quelle [25.11.2021].

[20] Vgl. Rohr/Juschkat (2021), Online-Quelle [25.11.2021].

Da es zu diesem Thema nicht ausreichend Literatur gibt, um einen konkreten Ansatz zu verifizieren, wird für die IIT im Rahmen dieser Arbeit, sofern sie benötigt wird, erstere Beschreibung verfolgt. Das kann folgendermaßen veranschaulicht werden:

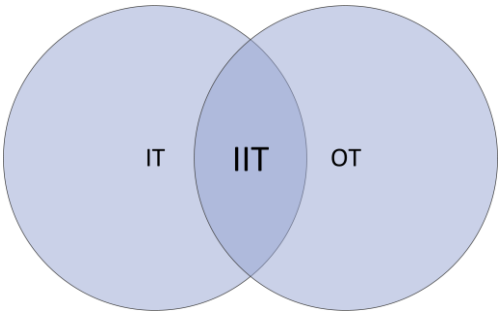

Abb. 2: Industrial Information Technology (IIT) als Bindeglied zwischen Information Technology (IT) und Operational Technology (OT), Quelle: Eigene Darstellung.

Im operativen Umfeld, vor allem in Bezug auf Netzwerke, könnten IT, OT und IIT folgendermaßen gegliedert werden:

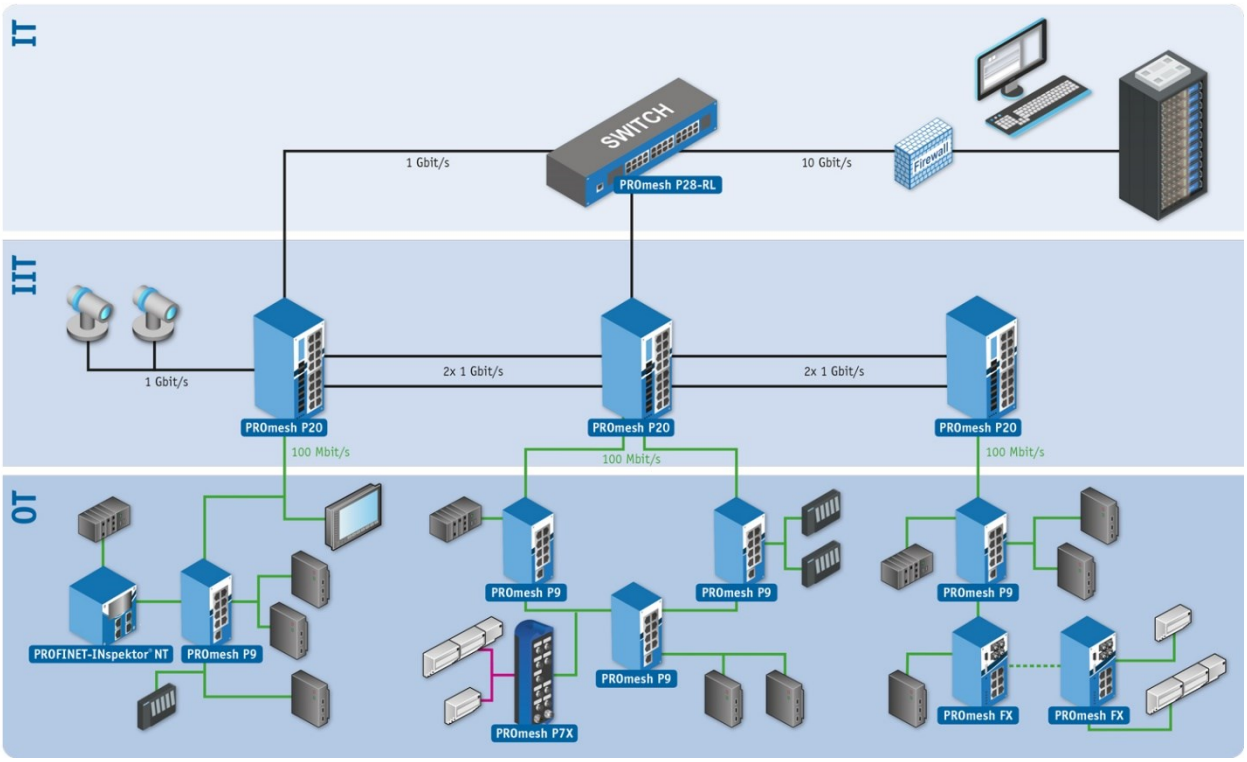

Abb. 3: Netzwerkaufbau von Information Technology (IT), Operational Technology (OT) und Industrial Information Technology (IIT), Quelle: Indu-Sol GmbH (2021), Online-Quelle [25.11.2021].

Dabei befinden sich Firewall, Server und Bedienstationen (*BST*) in der IT, Überwachungskameras werden der IIT zugeordnet und speicherprogrammierbare Steuerungen, Buskoppler und Bedieneinheiten wie zum Beispiel Touchpanels (*TP*) sind dem Bereich der OT eingeordnet. Switches finden sich in jeder der dargestellten Netzwerkschichten wieder.

1.5.7 Internet der Dinge (IoT)

Der Begriff Internet der Dinge hat mehrere Bedeutungen, die sich je nach Fachbereich und Anwendungsfall unterscheiden.[21] Die im Allgemeinen passendste Definition stammt von Gershenfeld. Dieser definiert IoT als Internetprotokoll über verteilte Geräte, was bedeutet, dass jedes Gerät ein vollumfänglicher Teil des Internets sein muss. Daher gelten Sensoren, welche nicht unmittelbar mit dem Internet, sondern lediglich mit einem zentralen Server verbunden sind, nicht als IoT-Device.[22]

Der Begriff Internet der Dinge ergibt sich aus der Zusammenschaltung von Dingen. Als Dinge werden Geräte bezeichnet. Das IoT ist daher eine direkte „Gerät-zu-Gerät-Verbindung“ über das Internet. Allein von 2015 bis 2021 konnte das IoT einen Anstieg von rund 40 Milliarden Geräten verzeichnen, womit in Summe 46 Milliarden Geräte weltweit Teil des Internet der Dinge sind.[23]

Durch das wachsende Internet der Dinge nähern sich IT und OT immer weiter an. Zusätzlich hat sich dadurch die Angriffsoberfläche für Cyberangriffe enorm gesteigert.[24]

1.5.8 Industrielles Internet der Dinge (IIoT)

Das industrielle Internet der Dinge beschreibt, wie der Name schon erkennen lässt, das IoT im industriellen Umfeld. Der größte Unterschied ist, dass das Internet der Dinge menschliche Interaktionen mit Geräten und Objekten darstellt und das IIoT weitreichendere Möglichkeiten zur Überwachung und Steuerung von Produktionsprozessen beinhaltet, aber nicht für die Interaktion mit Menschen gedacht ist. Beide Technologien behandeln intelligente und vernetzte Geräte. Die IIoT-Devices sind grundsätzlich qualitativ hochwertiger und präziser, da sie für ein industrielles Umfeld konzipiert werden. Daher funktionieren sie auch bei widrigen Umgebungsbedingungen zuverlässig.[25]

Es vereint die „4 M“ der Produktion: Maschine, Mensch, Material und Methode. Gemeinsam mit der Vernetzung, Big Data, den Advanced Analytics und der Applikationsentwicklung ergeben sich daraus weitreichende Synergien.[26]

Da das IIoT zumeist von der IT betrieben wird, jedoch OT-Systeme regelt, verlaufen die Grenzen beider Systeme immer weiter zusammen.[27]

---

[21] Vgl. Euchner (2018), S. 10.

[22] Vgl. Gershenfeld/Euchner (2015), S. 16 f.

[23] Vgl. Ramos (2021), Online-Quelle [25.11.2021].

[24] Vgl. Fretty (2020), S. 21.

[25] Vgl. Luber/Litzel (2017), Online-Quelle [25.11.2021].

[26] Vgl. Seetharaman/Patwa/Saravanan/Sharma (2019), S. 1161.

[27] Vgl. Huber (2021), Online-Quelle [25.11.2021].

Eine Übersicht über die unterschiedlichen Anwendungsbereiche von IIoT und IoT bietet die folgende Abbildung:

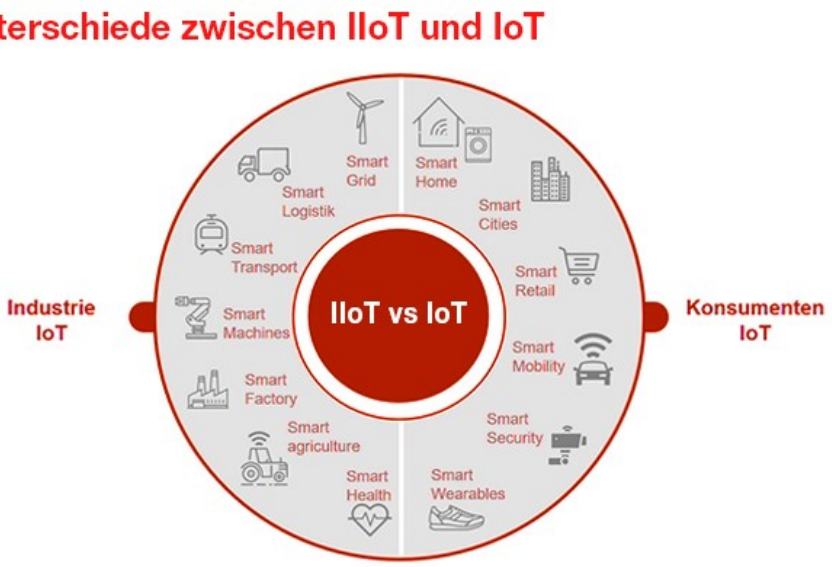

Abb. 4: Unterscheidung von Industrial Internet of Things (IIoT) und Internet of Things (IoT), Quelle: Logicalis Group (2021), Online-Quelle [25.11.2021].

1.5.9 Industrie 4.0

Im Laufe der Zeit gab es mehrere industrielle Revolutionen. Die Industrie 4.0 wird als vierte industrielle Revolution bezeichnet, da es sich um einen grundlegenden und strukturellen Wandel handelt.[28] Es handelt sich dabei um eine ständige Neuerung der weltweiten Produktions-Industrie.[29] Der Fokus liegt in der Kombination von Produktion, IT und dem Internet.[30]

Sie zeichnet sich vor allem durch das IoT und Big Data aus, da sämtliche Daten ausgewertet und neue Erkenntnisse gewonnen werden können. Sie besteht jedoch auch aus weiteren relevanten Elementen, die sich eher branchen-, produkt- oder fachspezifisch ergeben.[31]

[28] Vgl. Andelfinger/Hänisch (2017), S. 3.

[29] Vgl. Matt/Modrák/Zsifkovits (2020), S. VII.

[30] Vgl. Matt/Modrák/Zsifkovits (2020), S. 3.

[31] Vgl. Andelfinger/Hänisch (2017), S. 14 – 16.

2 INFORMATIONSSICHERHEIT

Der deutsche Begriff Sicherheit macht keinen Unterschied zwischen den englischen Bezeichnungen „Security“ und „Safety“. Da für die Informationssicherheit ein generelles Verständnis für die Sicherheit im Sinne der Security gegeben sein muss, müssen die Bedeutungen zunächst abgegrenzt werden.

Die nachfolgende Abb. 5 stellt einen Überblick über den Sicherheitsbegriff in Kombination mit der Security und Safety dar. Dabei wird die Informationssicherheit in IT-Security und OT-Security unterteilt, um den Aufbau für die folgenden Kapitel strukturiert darzustellen. Die Cybersecurity stellt weiters die Sicherheit von elektronischen Daten, zum Beispiel mit Daten-Backups dar und ist ein Teilbereich der IT-Security.[32] Da elektronische Daten ebenfalls in der OT zu finden sind, trifft Cybersecurity in diesem Bereich gleichermaßen zu. Die Informationssicherheit und die Betriebssicherheit umfassen weitaus mehr Parameter als dargestellt sind. Diese werden in diesem Kontext nicht berücksichtigt.

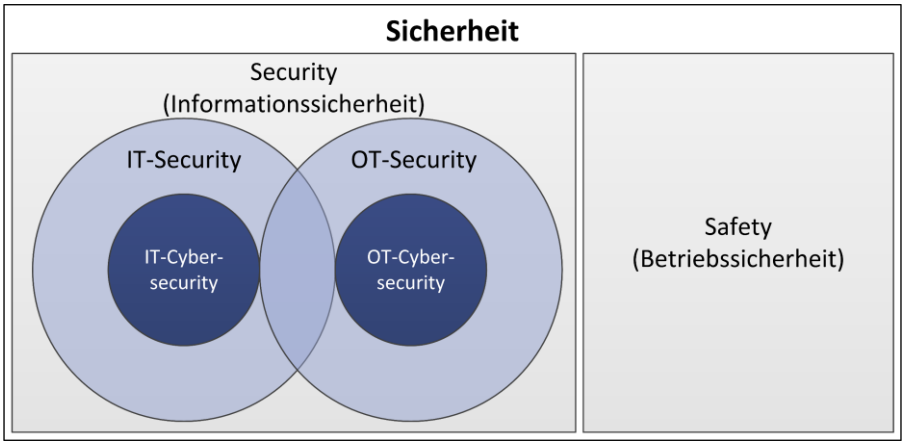

Abb. 5: Übersicht über den Sicherheitsbegriff (IT: Information Technology, OT: Operational Technology), Quelle: Eigene Darstellung.

Safety beschreibt die Sicherheit von Menschenleben und der Umwelt vor Maschinen. Zum Beispiel Notausgangstüren für den Brandfall. Security hingegen bezeichnet die Sicherheit von Maschinen gegenüber kriminellen Handlungen von Menschen. Als Beispiel hierfür kann eine versperrte Tür herangezogen werden, welche nur von Personen mit dem passenden Schlüssel geöffnet werden kann.[33]

[32] Vgl. Buchy (2016), Online-Quelle [25.11.2021].

[33] Vgl. Springer (2016), Online-Quelle [25.11.2021].

2.1 Schutzziele

Die Informationssicherheit hat als oberstes Ziel den Schutz von Daten.[34] Dabei kann es sich sowohl um personenbezogene Daten, die den Datenschutz betreffen, sowie Geschäfts- und Unternehmensgeheimnisse handeln.[35] Informationen können sowohl physisch als auch digital sein.

Um einen Missbrauch solcher Daten möglichst zu vermeiden, müssen die Schutzziele der Informationssicherheit definiert und aufrechterhalten werden. Dabei handelt es sich um die Integrität, die Verfügbarkeit und die Verbindlichkeit. Optional können auch weitere Ziele, wie die Authentizität, die Zurechenbarkeit und die Nichtabstreitbarkeit angestrebt werden.[36]

In der folgenden Abbildung werden die Schutzziele grafisch visualisiert:

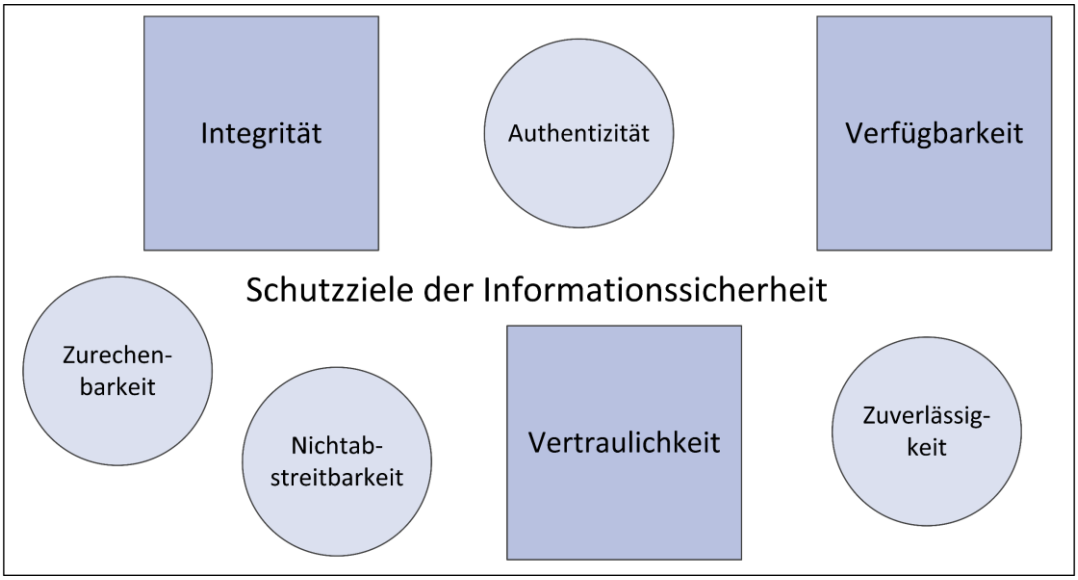

Abb. 6: Schutzziele der Informationssicherheit, Quelle: Eigene Darstellung.

Die Informationssicherheits-Schutzziele sind nach Ali Ismail Awad gemäß den Definitionen von *ISO* (Internationale Organisation für Normung) und NIST folgendermaßen zusammengefasst:[37]

Integrität (Integrity)

Die Integrität ist das Ziel der vollständigen und richtigen Informationen und dessen Schutz vor ungewollten oder fehlerhaften Änderungen und Vernichtungen.

[34] Vgl. Siriu (2021), Online-Quelle [25.11.2021].

[35] Vgl. Hanschke (2020), S. 1 f.

[36] Vgl. Reiss/Reiss (2019), S. 213 f.

[37] Vgl. Awad/Fairhurst (2018), S. 16 f.

Verfügbarkeit (Availability)

Die Verfügbarkeit beschreibt die Eigenschaft, dass die benötigten Informationen, wenn sie gebraucht werden, verfügbar und zugänglich sind und dies in einer angemessenen Zeit erfolgen kann.

Vertraulichkeit (Confidentiality)

Bei der Vertraulichkeit geht es darum, dass Informationen nicht an unberechtigte Personen, Unternehmen oder Prozesse weitergegeben oder offengelegt werden. Die Autorisierung soll dabei aufrechterhalten werden, um die Identifikation und Verifikation von Personen, Prozessen und Geräten für die Zugriffe durchzuführen.

Authentizität (Authenticity)

Die Authentizität behandelt die Eigenschaft, dass eine Entität ist, was sie vorgibt zu sein, um somit das nötige Vertrauen in die Gültigkeit einer Nachrichtenübertragung oder eines -absenders zu haben.

Nichtabstreitbarkeit (Non-repudiation)

Nichtabstreitbarkeit ist die Fähigkeit der eindeutigen Zuordnung der Herkunft oder des Ziels einer Information. Das Schutzziel dient der Vermeidung von der Verleugnung der Kommunikationspartner, sodass die Kommunikationsteilnehmer den Informationsaustausch nicht abstreiten können.

Zurechenbarkeit (Accountability)

Das Sicherheitsziel der Zurechenbarkeit soll sicherstellen, dass Aktionen eindeutig auf die entsprechende Entität zurückverfolgt werden.

Zuverlässigkeit (Reliability)

Bei der Zuverlässigkeit geht es darum, dass die Ergebnisse und das Verhalten stets wie erwartet eintreffen.

2.2 IT- vs. OT-Security

Die IT-Security nimmt sich dem Schutz von IT-Geräten vor Bedrohungen an,[38] wohingegen die OT-Security den Schutz von Prozessen, Menschen und Profit zur Basis hat.[39] Die OT hat verglichen zur IT einen viel längeren Lifecycle, aber bei Weitem nicht die gleichen Fortschritte, wenn es um das Identifizieren und Eliminieren von Schwachstellen geht.[40] Das hat vor allem den Hintergrund, dass OT-Systeme von jeher abgekapselte Systeme ohne Verbindung zur Außenwelt waren, diese durch das IoT aber immer weiter vernetzt werden und somit auch eine größere Aufmerksamkeit benötigen.[41]

IT und OT unterliegen unterschiedlichen Anwendungsfällen und haben daher andere Anforderungen. Die Unterscheidungen reichen von der Hardware, über die Software bis zu den Daten und Kommunikationsprotokollen. Die nachstehende Tabelle soll die Unterscheidungen bzgl. Hardware, Software und Daten vereinfacht darstellen:

	IT	**OT**
Hardware	Switches, Router, Kabel, Server, Speicher, generell benötigte Geräte wie z.B. PCs	Netzwerkkameras, Sensoren, Aktuatoren, Messgeräte, smarte Geräte zur Datensammlung
Software	Firmware, Betriebssysteme, Software für die Funktion der Geräte	Spezifische Software, um entsprechendem Anwendungsfall gerecht zu werden
Daten	Logs, Betriebssystemdaten, Programmdaten	Rohdaten, Anlagendaten

Tab. 1: Unterscheidung der Hardware, Software und Daten von Information Technology (IT) und Operational Technology (OT), Quelle: In Anlehnung an Dolan (2018).

Tab. 1 soll nur einen Überblick für die Einteilung bieten und dient nicht der detaillierten Kategorisierung aller bestehenden Komponenten.

[38] Vgl. Reiss/Reiss (2019), S. 215.

[39] Vgl. Infradata Inc. (2019), Online-Quelle [25.11.2021].

[40] Vgl. Fretty (2020), S. 21 f.

[41] Vgl. Seiden/Johnson/Barber/Campara (2020), S. 22.

Eine deutlichere Unterscheidung zwischen IT und OT ist in der folgenden Grafik übersichtlich dargestellt:

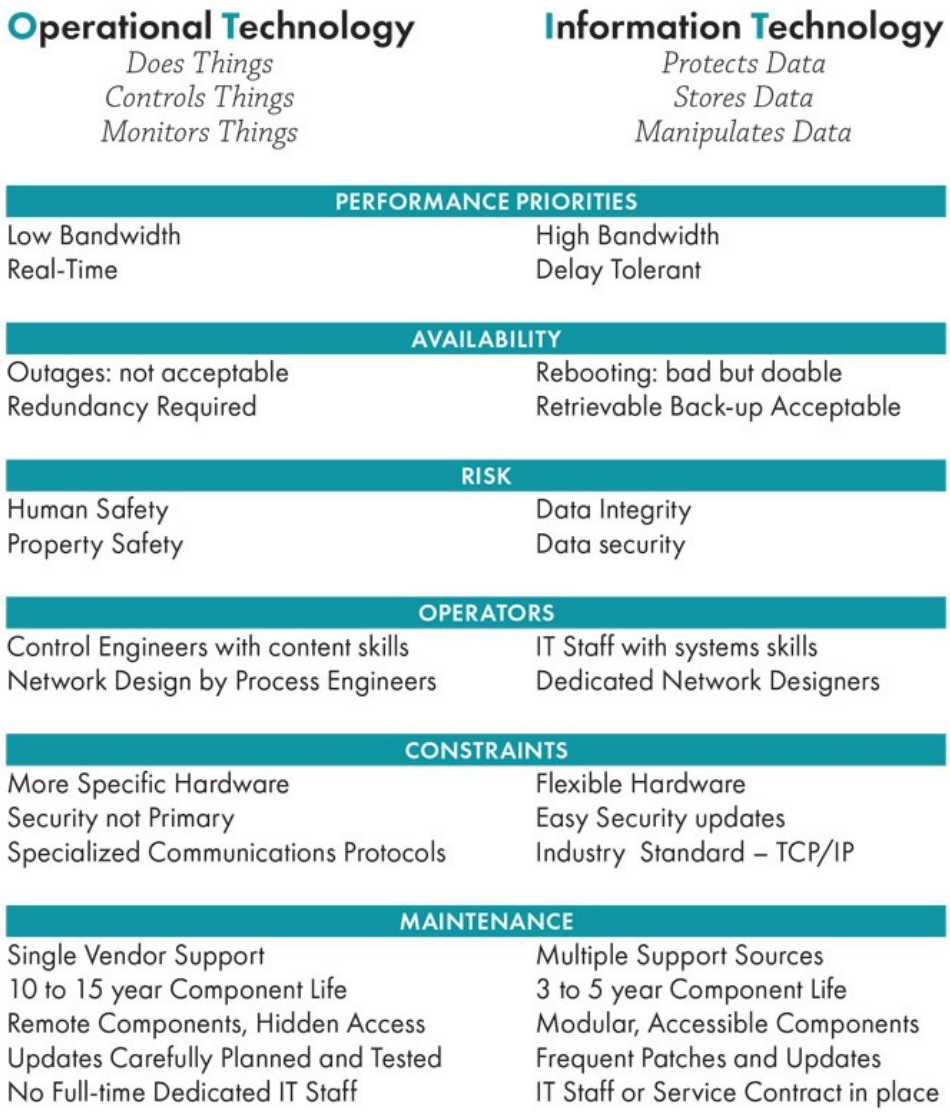

Abb. 7: Unterscheidung von Operational Technology (OT) und Information Technology (IT), Quelle: Frontier Computer Corp. (2021), Online-Quelle [25.11.2021] (leicht modifiziert).

Abb. 7 zeigt deutlich, dass sich die OT hauptsächlich mit Dingen und die IT sich mit Daten befasst. Es handelt sich um komplett unterschiedliche Prozessgeschwindigkeiten der beiden Bereiche. Sensoren müssen die Daten im Mikrosekundenbereich an Steuerungen übermitteln können. Denkt man im Gegensatz dazu an eine E-Mail, ist es nicht relevant, ob diese eine Minute früher oder später zugestellt wird. Ausfälle verzeiht die Operational Technology ebenso nicht so leicht wie die Information Technology. Daher werden bei ersterer Neustarts soweit wie möglich vermieden. Da in der Industrie meistens spezifische Hardware mit proprietären Kommunikationsprotokollen zum Einsatz kommt, wird versucht diese aus wirtschaftlichen Gründen so lange wie möglich zu betreiben, bevor es zu einem Tausch kommt. Das wiederum führt häufig zu veralteten Komponenten, mit denen sich hauptsächlich das geschulte Anlagenpersonal auskennt.

Da IT und OT verschiedene Ansätze verfolgen, auch im Sinne der Schutzziele, sich jedoch nicht den Interessenskonflikten zueinander bewusst sind, kann die IT/OT-Konvergenz zu einem großen Problem für viele Unternehmen werden.[42] Die Relevanz der Schutzziele ist in der folgenden Abbildung dargestellt:

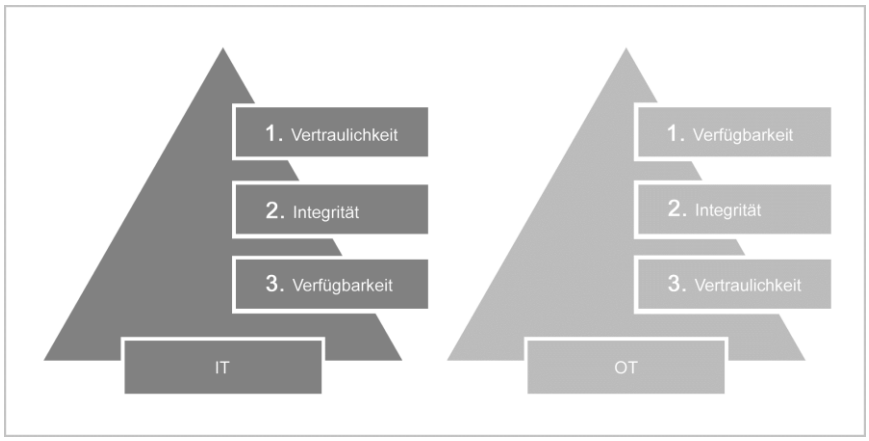

Abb. 8: Priorität der Schutzziele von Information Technology (IT) und Operational Technology (OT), Quelle: Mullane (2021), Online-Quelle [25.11.2021] (leicht modifiziert).

So hat die IT als oberstes Ziel die Vertraulichkeit (Confidentiality) der Daten, darauffolgend die Integrität (Integrity) und als drittrelevantestes Schutzziel die Verfügbarkeit (Availability). Daher werden die IT-Schutzziele auch als „CIA-Triade“ bezeichnet. Bei der OT stehen zwar die gleichen Schutzziele im Vordergrund, jedoch werden diese genau in der umgekehrten Reihenfolge priorisiert.[43]

Wenn man die unterschiedlichen Anwendungsbereiche von IT und OT bedenkt, ist es verständlich, dass in der OT, bei der es vorrangig um funktionale Sicherheit und Menschenleben geht, die Verfügbarkeit das oberste Ziel ist. Bei der IT hingegen, die sich vor allem mit (teils sensiblen) Daten beschäftigt steht, daher die Vertraulichkeit im Vordergrund.

Anhand der Automatisierungspyramide können OT und IT klar dargestellt werden. Dabei werden die ersten drei Ebenen, also Produktebene, cyberphysische Systeme und Linienebene als OT kategorisiert und die Produktions- und Unternehmensebene in die IT gegliedert.

[42] Vgl. Beeson (2020), Online-Quelle [25.11.2021].

[43] Vgl. Rohr/Juschkat (2021), Online-Quelle [25.11.2021].

Das erweiterte ISA-95-Modell stellt dabei zusätzlich zu den Unternehmens- und Anlagenschichten auch alle Ebenen vernetzt mit der IIoT Cloud dar:

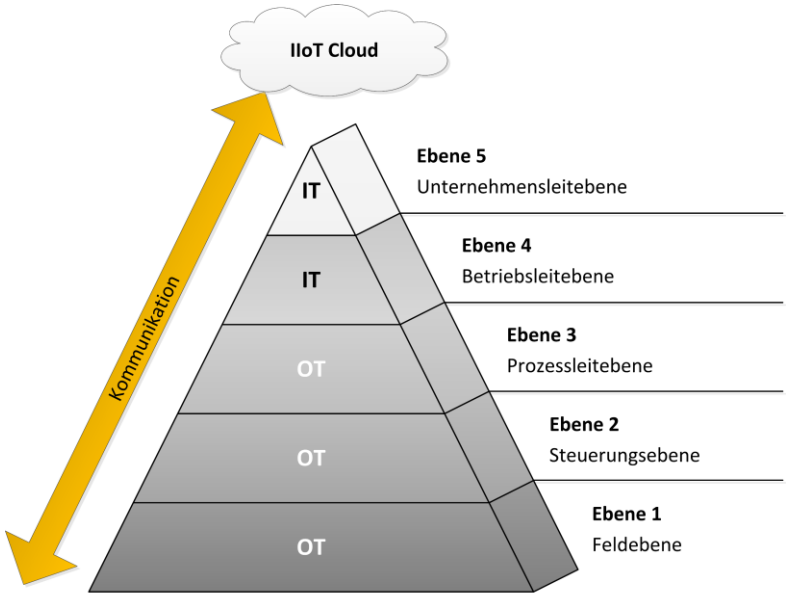

Abb. 9: Erweitertes ISA-95-Modell (IT: Information Technology, OT: Operational Technology, IIoT: Industrial Internet of Things), Quelle: In Anlehnung an Huber (2021), Online-Quelle [25.11.2021].

Das ISA-95-Modell stammt von der ISA 95, einer Norm für die Integration von Unternehmens- und Betriebsleitebene. Dieses zeigt, dass sämtliche Ebenen voneinander abhängig sind und auch, dass die IT auf der OT aufbaut. Daher müssen die Zusammenhänge auch im Bezug der IT- und OT-Sicherheit berücksichtigt werden.

Findet eine strikte Trennung von IT und OT statt, kann das zu blinden Flecken bzgl. der Cybersecurity führen. Daher sollten diese soweit wie möglich gesamtheitlich betrachtet werden. Das ist durch Sichtbarmachen der Komponenten durch das Führen von Asset-Listen möglich. Dabei ist es wichtig, dass IT- und OT-Teams eng zusammenarbeiten.[44]

Die Best Practices zur Security-Risikominimierung sind unter anderem[45]

- die Erstellung separater Netzwerke,
- IoT-Geräte im Hinterkopf behalten,
- Firmware von Geräten aktuell halten,
- Cybersecurity-Framework(s) anwenden, sowie
- die Erstellung eines Notfallplans.

Doch auch das Patchen, von Schwachstellen und sichere Remote-Verbindungen müssen berücksichtigt werden.[46]

[44] Vgl. Fretty (2020), S. 22 f.

[45] Vgl. Fretty (2020), S. 22 f.

[46] Vgl. Ku (2021), S. 28.

2.3 Angriffe

Angriffe jeglicher Art auf IT-Systeme sind längst keine Seltenheit mehr. Da OT-Systeme immer häufiger mit der IT verknüpft sind, wird die mögliche Angriffsfläche vergrößert. Eine mangelnde oder eingeschränkte Funktion von OT-Systemen kann weitreichende und teure Folgen haben.[47]

Daher werden mögliche Angriffsflächen und Arten von Angreifer*innen eruiert, um in einem späteren Schritt die möglichen Kombinationen daraus zu definieren und potenzielle Maßnahmen darauf abzustimmen.

2.3.1 Angriffsvektoren

Die Angriffsvektoren sind Wege bzw. Möglichkeiten, um in ein System zu gelangen. Dazu zählen unter anderem:[48]

Network Hacking
Angriffe vorrangig auf Server, die über das Netzwerk/Internet durchgeführt werden, welche als Ziel die Manipulation oder Entwendung von Daten und die Verursachung des größtmöglichen Schadens haben.

Gestohlene/Verlorene Smartphones oder Notebooks
Smartphones oder Notebooks, die in die Hände von Hacker*innen gelangen und nicht passwortgeschützt sind sowie kein verschlüsseltes Dateisystem haben, stellen für Angreifer*innen ein leichtes Ziel dar.

Zugriff auf Firmengeräte außerhalb des Unternehmens
Durch unsichere WLANs oder Bluetooth können Angreifer*innen Schwachstellen ausnutzen. Abhilfe schaffen die Nutzung der virtuellen privaten Netzwerke (Virtual Private Network, *VPN*) der Firmen, das Vermeiden von Passworteingaben und/oder die Bekanntgabe von Informationen.

Malware, Viren
Vor allem über E-Mails, infizierte Webseiten oder Malware-Apps haben Angreifer*innen auf nicht auf aktuellsten Stand upgedatete Geräte ein leichtes Spiel und können Schwachstellen ausnutzen sowie Schadsoftware oder Schadcode ausführen.

Manipulierte Hardware
Hardware, die z.B. als harmloser USB-Stick ausgegeben wird, jedoch den Zweck des maximalen Schadens, wie zum Beispiel die Zerstörung von Hardware, verfolgt.

Angriffe auf die Cloud
In der Cloud sind in der Regel sämtliche Daten gespeichert. Daher ist diese ein begehrtes Ziel. Vor allem die Zugangsdaten zur Cloud sind erstrebenswert.

[47] Vgl. Dolan (2018), S. 84 – 86.

[48] Vgl. Kofler/Zingsheim/Gebeshuber/Kania/Widl/Kloep/Aigner/Hackner/Neugebauer (2020), S. 31 – 35.

Angriffe auf die Netzwerkinfrastruktur

Dabei handelt es sich vor allem um die verwendete Technik für das Mobilfunknetzwerk und aktuell um die Mobilfunktechnologie 5G. Beispielsweise befürchtet die USA, dass Huawei und somit China Backdoors in Hard- und Software implementieren und folglich Spionage betreiben könnte. Umgekehrt könnte mit 3G und 4G dieselbe Möglichkeit seitens der USA bestehen. Hier handelt sich jedoch um staatliches Interesse, was bedeutet, dass Angriffe auf solche Netzwerkstrukturen in der Regel nicht von „normalen" Hacker*innen, sondern von staatlichen Organisationen ausgehen.

Phishing

Beim Phishing wird versucht Passwörter über eine „Fake"-Passworteingabe zu erbeuten.

Social Engineering

Social Engineering beschreibt das Herausfinden von Passwörtern oder Zugangsdaten mit rein menschlichen Komponenten, ohne die Anwendung von technischen Maßnahmen.

Physischer Zugang

Häufig sind offenstehende Räume oder vergessene bzw. gestohlene Geräte der Grund für einen leichten physischen Zugang zur Hardware.

Angriff von innen

Mitarbeitende können viele Sicherheitsmaßnahmen, wie zum Beispiel die Firewall, umgehen. Verursacht durch Zorn, Frust oder Bezahlung ist eine Sabotage von innen möglich.

Konkretere Angriffstypen, welche noch nicht erwähnt wurden, sind unter anderem:[49]

Botnet

Ein Botnet besteht aus mehreren gehackten und von Hacker*innen gesteuerten Geräten, die über das Internet verteilt sind. Das Netzwerk aus Systemen wird verwendet, um Schaden auf weiteren Geräten anzurichten.

Denial of Service (*DoS*)

Ein Netzwerkgerät wird durch unzählige Anfragen überlastet und somit lahmgelegt. Distributed Denial of Service (*DDoS*) ist ähnlich einer DoS-Attacke, nur dass die Anfragen von mehreren verteilten Geräten versendet werden.

Backdoors

Beschreiben Hintereingänge, die in Software eingebaut werden, die zwar für die Nutzer*innen nicht sichtbar sind, jedoch von Hacker*innen ausgenutzt werden.

Eavesdropping

Es wird unverschlüsselter Kommunikation zwischen mehreren Geräten gelauscht, um sensible Daten zu erlangen.

[49] Vgl. Dolan (2018), S. 84.

Generell können diese vier spezifischeren Angriffstypen dem Network-Hacking zugeordnet werden, da solche Angriffe nur über ein Netzwerk stattfinden können. Alle beschriebenen Angriffsvektoren sind wesentlich, es gibt aber noch unzählige weitere Möglichkeiten, um in ein System einzudringen. Vor allem auch in Bezug auf spezifische Angriffsarten, die nicht erwähnt wurden. Man sollte sich dessen bewusst sein und daher so gut wie möglich vor sämtlichen Attacken schützen und weitreichende Maßnahmen ergreifen.

2.3.2 Arten von Angreifer*innen

Ebenso wie Angriffsvektoren gibt es unterschiedliche Angreifer*innen, die zum Teil böse Absichten und zum anderen keine konkreten Ziele verfolgen. Laut der Ausbildung zum „Certified OT Security Practicioner“ handelt es sich dabei unter anderem um:[50]

- Script Kiddies
- Erfahrene Hacker*innen
- Sicherheitsforscher*innen
- Systemadministrator*innen
- Bediener*innen
- Lieferanten
- Mitbewerber
- Staatlich gelenktes Hacking

Diverse Angreifer*innen haben unterschiedliche Motive für ihre Taten. Script Kiddies sind in der Regel Jugendliche, die sich dem Ausmaß ihres Tuns, dem Ausführen von Skripten, nicht bewusst sind. Auch sind ungezielte Angriffe von Hacker*innen möglich. Dabei spielt hauptsächlich das Erpressungsgeld selbst eine Rolle, nicht aber die Herkunft des Geldes. Das findet vor allem bei Festplattenverschlüsselungen Anwendung. Doch auch gezielte Spionage oder Sabotage sind keine Seltenheit, um Firmengeheimnisse oder sensible Daten zu erhalten, oder das Unternehmen weitestgehend zu schädigen. Gegenüber Geheimdiensten anderer Länder sollte man ebenso misstrauisch sein und vor allem Daten, die sich in der Cloud befinden, verschlüsselt halten. Staatlich gestützte Cyberkriege stellen ein weiteres Szenario dar, um die Wirtschaft anderer Staaten lahmzulegen. Zukünftig sind auch Terrorangriffe auf kritische Infrastruktur denkbar.[51]

Ebenso könnten gezielte Spionage und/oder Sabotage von Lieferanten oder Mitbewerbern in Auftrag gegeben werden. Bei den Bediener*innen besteht die Gefahr, dass diese aus Langeweile und bei Systemadministrator*innen aus Zorn am System tätig sind und wichtige Sicherheitsparameter beeinflussen könnten.

[50] Vgl. ICS.201 (2021), S. 217.

[51] Vgl. Kofler/Zingsheim/Gebeshuber/Kania/Widl/Kloep/Aigner/Hackner/Neugebauer (2020), S. 36 f.

3 IEC 62443

Die IEC 62443 ist eine Reihe von Standards für die Security von Industrial Automation and Control Systems (*IACS*) die über den gesamten Lebenszyklus dieser Systeme festgelegt sind. Bei IACS handelt es sich um alle Bestandteile, die im industriellen Automatisierungsumfeld benötigt werden. Aus Gründen der Interkonnektivität werden IACS in Bezug auf Cyberattacken immer gefährdeter. Da IT-Standards den Anforderungen von IACS bzgl. Sicherheit, Integrität und Zuverlässigkeit nicht gerecht werden, wurde die Notwendigkeit einer eigenen Norm für industrielle Systeme immer größer. Aus diesem Grund wurde die Normenreihe vom ISA99 Committee und dem IEC Technical Committee 65 / Working Group 10 entwickelt. Diese Normen behandeln Komponententypen, die zu IACS-Systemen zusammengefasst werden können. Das können verteilte Geräte, Host-Geräte, Netzwerkgeräte und Software sein. Durch die Anwendung der IEC 62443 kann die Wahrscheinlichkeit von Cyberangriffen auf die IACS und somit die OT verringert werden.[52]

Die IEC 62443 verfolgt einen gesamtheitlichen Ansatz, der nicht rein technisch ist, da es auch Risiken mit nicht-technischen Hintergründen gibt. Daher ist sie nach dem Defense-in-Depth-Prinzip aufgebaut.[53]

Die Normenreihe ist für die folgenden Rollen von Relevanz:[54]

- Asset Owner
- Service Provider
- Product Supplier

Asset Owner, übersetzt Betreiber, sind für ein oder mehrere IACS-Systeme verantwortlich. Service Provider oder auch Dienstleister sind Organisationen, die Unterstützungsdienste anbieten und erbringen, und die damit verbundene Verantwortung tragen. Product Supplier bzw. Produktlieferanten sind die Hersteller von Hard- und/oder Software.[55]

3.1 Grundsätze

Die Normenreihe IEC 62443 verfolgt einige Konzepte, welche für die Anwendung der einzelnen Normen von Relevanz sind.

[52] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 2 – 10.

[53] Vgl. IEC (2021), Online-Quelle [25.11.2021].

[54] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 10.

[55] Vgl. OVE EN IEC 62443-3-3 (2020), S. 17 – 21.

3.1.1 Zonen und Conduits

Zonen und Conduits dienen der Zusammenfassung von Assets, welche sich die gleichen Sicherheitscharakteristiken teilen, wodurch das Risiko für erfolgreiche Cyberangriffe minimiert wird. Im Teil 3-2 wird eine Gruppierung nach Geschäfts- und Steuerungskomponenten, funktionalen Sicherheitsanforderungen, temporär verbundener Geräte, kabelloser Geräte und Geräte, die über ein externes Netzwerk verbunden sind, empfohlen.[56]

Zonen sind eine Zusammenfassung von logischen oder physischen Assets mit gleichen IT-Sicherheitsanforderungen. Conduits sind die Kommunikationskanäle mit gleichen Anforderungen zwischen zwei oder mehreren Zonen. Diese werden im Teil 3-2 im Zuge des System Designs definiert.[57]

3.1.2 Grundlegende Anforderungen

Die grundlegenden Anforderungen (Foundational Requirements, *FR*, Basisanforderungen), sind die technischen Basisanforderungen, die für die gesamte Normenreihe herangezogen werden. Damit werden die Anforderungen von IACS in entsprechende, standardisierte Gruppen gegliedert.[58]

Die sieben grundlegenden Anforderungen sind:[59]

- Identifizierung und Authentifizierung (Identification and Access Control*, IAC*)
- Nutzungskontrolle (Use Control, *UC*)
- Systemintegrität (System Integrity, *SI*)
- Vertraulichkeit der Daten (Data Confidentiality, *DC*)
- Eingeschränkter Datenfluss (Restricted Data Flow, *RDF*)
- Rechtzeitige Reaktion auf Ereignisse (Timely Response to Events, *TRE*)
- Verfügbarkeit der Ressourcen (Resource Availability, *RA*)

Die Foundational Requirements werden weiterführend noch in eine Reihe von Systemanforderungen (System Requirements, *SR*) und konkreter in weitergehende Anforderungen (Requirement Enhacements, *RE*) unterteilt, die bei der Vergabe der Security-Levels (Sicherheitslevel, *SL*) von Relevanz sind.[60]

[56] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 7.

[57] Vgl. OVE EN IEC 62443-3-3 (2020), S. 14 – 23.

[58] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 8.

[59] Vgl. OVE EN IEC 62443-3-3 (2020), S. 16.

[60] Vgl. OVE EN IEC 62443-3-3 (2020), S. 14.

3.1.3 Security-Levels

Die Security-Levels (SL) dienen der Bewertung von Sicherheitsanforderungen pro Zone und Conduit und basieren auf den sieben Foundational Requirements.[61] Sie sind im Teil 3-3 der Norm definiert und werden pro SL-Art vergeben, welche im Folgenden aufgelistet sind:[62]

Target Security Levels (*SL-T*): Sind die zu erreichenden Security-Levels eines Systems. Dieser SL wird in der Regel über eine Risikobewertung des Systems ermittelt und definiert.

Achieved Security Levels (*SL-A*): Sind die tatsächlich erreichten Security-Levels eines Systems. Sie werden nach der Verfügbarkeit eines Systementwurfs oder dem Aufbau eines Systems gemessen. Damit wird geprüft, ob die Security-Levels den definierten SL-T-Levels entsprechen.

Capability Security Levels (*SL-C*): Sind die erreichbaren Security-Levels, die durch richtige Konfiguration von Systemen oder Komponenten erreicht werden können. Dadurch sind diese Assets von sich aus in der Lage, ohne zusätzliche Maßnahmen, die definierten SL-T-Levels zu erreichen.

Jeglicher SL-Art wird für jede Zone und Conduit pro Basisanforderung ein Level zugeordnet und dann entsprechend im Vektorformat dargestellt.[63] Die 5 verschiedenen Security-Levels sind:[64]

„SL 0: Keine besonderen Anforderungen oder Schutzmaßnahmen notwendig“

„SL 1: Schutz gegen gelegentlichen oder zufälligen Missbrauch“

„SL 2: Schutz gegen einen absichtlichen Missbrauch mit einfachen Mitteln und geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation“

„SL 3: Schutz gegen einen absichtlichen Missbrauch mit raffinierten Mitteln und mittlerem Aufwand, IACS-spezifische Fertigkeiten und mittlerer Motivation“

„SL 4: Schutz gegen einen absichtlichen Missbrauch mit raffinierten Mitteln und erheblichem Aufwand, IACS-spezifische Fertigkeiten und hoher Motivation“

[61] Vgl. OVE EN IEC 62443-3-3 (2020), S. 72 – 77.

[62] Vgl. OVE EN IEC 62443-3-3 (2020), S. 73.

[63] Vgl. OVE EN IEC 62443-3-3 (2020), S. 73 – 77.

[64] OVE EN IEC 62443-3-3 (2020), S. 79 f.

Der Sicherheitslevel im Vektorformat setzt sich dann folgendermaßen zusammen:

„SL-?([FR,]Bereich) = { IAC UC SI DC RDF TRE RA }“[65]

SL-? Stellt eine der drei beschriebenen SL-Arten dar. FR ist eine der grundlegenden Anforderungen in abgekürzter Darstellung. Wird diese optional vor dem Bereich angegeben, wird damit nur der entsprechende, skalare Wert dieses FRs dargestellt. Ein Bereich kann eine Zone, ein Automatisierungssystem, ein Subsystem oder eine Komponente sein. Das darauffolgende Ergebnis stellt den SL pro FR im Vektorformat dar.[66]

3.1.4 Reifegradmodell

Das Reifegradmodell der IEC 62443 wird in den Teilen 2-1, 2-2, 2-4 und 4-1 herangezogen.[67] Nachdem der Teil 2-2 noch nicht veröffentlicht wurde, wird nur auf die übrigen drei Normen Bezug genommen.

Das Reifegradmodell legt Vergleichswerte für die Einhaltung von Anforderungen fest. Die Reifegrade entsprechen den Reifegraden des Reifegradmodells des Capability Maturity Model Integration (*CMMI*) und liefern dabei Aufschluss über die Sorgfältigkeit der Erfüllung von Requirements.[68]

Jeder Reifegrad ist dem vorherigen überlegen.[69] Die Reifegrade werden verwendet, um den Fortschritt von Prozessen von anfänglichen bis hin zu weiterentwickelten Stufen zu bewerten.[70]

Die Reifegrade (die an die fünf Stufen des CMMI-Modells angelehnt sind) sind in der nachfolgenden Tabelle 2 beschrieben:

Reife-grad	**CMMI (Capability Maturity Model Integration)**	**IEC 62443**	**Beschreibung**
1	Anfang	Anfang	Keine oder unausgereifte Dokumentation. Wiederholbarkeit ist eingeschränkt.
2	Verwaltet	Verwaltet	Erbringung einer Leistung nach schriftlich festgelegter Leitlinie. Personal verfügt über benötigte Kenntnisse und Fähigkeiten und/oder kann schriftliche Anweisungen befolgen. Prozesse sind auch während Stressphasen wiederholbar.
3	Definiert	Definiert/ Eingeführt	Leistungsfähigkeit ist nachweislich wiederholbar. Überprüfbare Nachweise für die Durchführung von Prozessen.

[65] OVE EN IEC 62443-3-3 (2020), S. 80.

[66] Vgl. OVE EN IEC 62443-3-3 (2020), S. 80.

[67] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 9.

[68] Vgl. OVE EN IEC 62443-4-1 (2018), S. 20.

[69] Vgl. OVE EN IEC 62443-2-4 (2020), S. 16.

[70] Vgl. OVE EN IEC 62443-2-1 (2019), S. 22.

Reife-grad	CMMI (Capability Maturity Model Integration)	IEC 62443	Beschreibung
4	Quantitativ verwaltet	Ständige Verbesserung	Die Stufen 4 und 5 des CMMI sind zusammengefasst. Mittels Prozessmessgrößen wird die Wirksamkeit und Leistungsfähigkeit von Prozessen kontrolliert und dadurch eine ständige Verbesserung erzielt.
5	Ständige Optimierung		

Tab. 2: Reifegrade der IEC 62443, Quelle: In Anlehnung an OVE EN IEC 62443-4-1 (2018), S. 21 f; OVE EN IEC 62443-2-1 (2019), S. 24; OVE EN IEC 62443-2-4 (2020), S. 17.

3.1.5 Designprinzipien

Die Normenreihe basiert auf den in den folgenden Unterkapiteln beschriebenen Designprinzipien. Die Übersicht der Prinzipien wurde aus der IEC 62443 Guideline[71] entnommen.

3.1.5.1 Secure by Design

Sicherheitsmaßnahmen werden bereits am Beginn des Lifecycles implementiert und nicht erst zu einem späteren Zeitpunkt. Die Sicherheit wird dabei im gesamten Lebenszyklus berücksichtigt. Durch die Berücksichtigung der Sicherheit in der Komponente und/oder im Automatisierungssystem selbst wird die Notwendigkeit von zusätzlichen Maßnahmen reduziert.[72]

3.1.5.2 Defense in Depth

Die Defense-in-Depth-Strategie basiert auf mehreren unterschiedlichen und voneinander unabhängigen Maßnahmen für die Abwehr eines Angriffes und dient somit dem Schutz eines Systems. Die Maßnahmen befinden sich in unterschiedlichen Schichten, die sich in der Funktionalität und den Ausfallsarten unterscheiden. Wenn eine Verteidigungsschicht eine Schwachstelle aufweist, kann diese durch die nächste Schicht abgeschwächt und somit die Gefahr eines erfolgreichen Angriffs verringert werden.[73]

3.1.5.3 Reduktion der Angriffsfläche

Eine Reduktion der Angriffsfläche kann durch das Minimalprinzip erreicht werden. Das bedeutet, dass nur minimal benötigte Rechte und Funktionen vergeben werden. Zusätzlich wird dieses Prinzip durch die Netzwerksegmentierung zur Steuerung des Netzwerkverkehrs und die Zugriffskontrolle für die Limitierung der physischen und logischen Zugriffe bestärkt.[74]

[71] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 9.

[72] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 9.

[73] Vgl. OVE EN IEC 62443-4-1 (2018), S. 13 f.

[74] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 9.

3.1.5.4 Wesentliche Funktionen

Die wesentlichen Funktionen bezeichnen die benötigten Funktionen, die für den Erhalt der Betriebssicherheit (Safety), der Gesundheit, der Umwelt und der Verfügbarkeit der relevanten Komponenten des Systems benötigt werden. Dazu zählen unter anderem sicherheitstechnische Funktionen, Steuerungs- und Regelfunktionen, sowie die Bedien- und Überwachbarkeit.[75]

Die wesentlichen Funktionen dürfen durch die Verwendung von IT-Sicherheitsmaßnahmen nur eingeschränkt werden, wenn das von einer Risikobeurteilung unterstützt wird.[76]

3.2 Abschnitte und Teile der Norm

Wie bereits erwähnt ist die IEC 62443 eine Reihe von Standards. Sie besteht aus vier Abschnitten, die wiederum Teildokumente enthalten. Dabei handelt es sich um folgende Dokumententypen:[77]

- IS – International Standard (Internationaler Standard)
- TR – Technical Report (Technische Beschreibung)
- TS – Technical Specification (Technische Spezifikation)

Die Dokumente unterliegen einem fünfjährigen Update-Zyklus, in dem sie revidiert und angepasst werden. In der untenstehenden Abb. 10 sind die Teile der Norm gemeinsam mit den entsprechenden Jahren der Erstveröffentlichung und den Dokumententypen, sofern bekannt und vorhanden, dargestellt.[78]

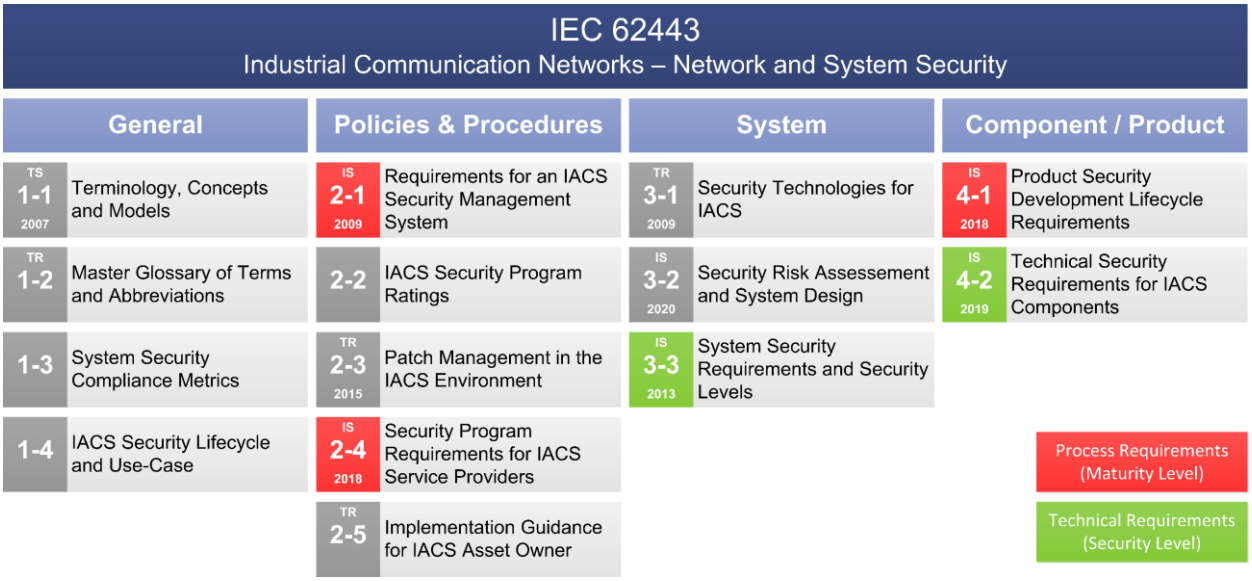

Abb. 10: Teile der IEC 62443 (IACS: Industrial Automation and Control Systems, IS: International Standard, TR: Technical Report, TS: Technical Specification), Quelle: In Anlehnung an ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021].

[75] Vgl. OVE EN IEC 62443-3-3 (2020), S. 20.

[76] Vgl. OVE EN IEC 62443-3-3 (2020), S. 27.

[77] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 6.

[78] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 6.

Lediglich das Datum der Erstveröffentlichung für den Teil 3-1 wurde ergänzt.[79]

Reifegrade sind Teil der Prozessanforderungen, wohingegen die Security-Levels in den technischen Anforderungen inkludiert sind. Ebenso ist ersichtlich, dass noch nicht alle Teile veröffentlicht wurden.

In den folgenden Unterkapiteln werden die einzelnen Abschnitte mit deren enthaltenen Teilen und Inhalten erläutert.

3.2.1 1. Abschnitt: General

In diesem Abschnitt befinden sich sämtliche Informationen, die für die gesamte Normenreihe relevant sind:[80]

1-1. Terminology, Concepts and Models (TS)

Dieser Teil gibt eine Einführung in sämtliche Konzepte und Modelle, die über die Serie verteilt verwendet werden. Er ist für all jene bestimmt, die sich mit der fundamentalen Basis der Norm auseinandersetzen wollen.

1-2. Master Glossary of Terms and Abbreviations (TR)

In diesem Teil sind Begriffe und Abkürzungen definiert, die in der gesamten Normenreihe relevant sind.

1-3. System Security Compliance Metrics

Dieser Teil beschreibt Methoden zur Entwicklung von quantitativen Metriken, die von Prozessanforderungen und technischen Anforderungen in den Standards abgeleitet sind.

1-4. IACS Security Lifecycle and Use-Cases

Dieser Teil enthält eine Beschreibung für den Lifecycle der IACS-Security und Use-Cases zur Darstellung von unterschiedlichen Anwendungen der Norm.

3.2.2 2. Abschnitt: Policies & Procedures

Die Normen dieses Abschnitts befassen sich mit den Richtlinien und Prozeduren, die für die IACS-Security notwendig sind:[81]

2-1. Requirements for an IACS Security Management System (IS)

Der Teil behandelt die Notwendigkeiten zur Definition und Implementierung eines effektiven IACS-Cybersecurity-Management-Systems. Das ist vor allem für die Asset Owner relevant, welche die Verantwortung für Design und Implementierung tragen.

[79] Vgl. IEC (2021), Online-Quelle [25.11.2021].

[80] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 4 – 5.

[81] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 5.

2-2. IACS Security Program Ratings

In diesem Teil sind die Methoden zur Evaluierung des Security-Levels im Vergleich zu den Anforderungen der vorliegenden Normenreihe definiert.

2-3. Patch Management in the IACS Environment (TR)

Teil 2-3 enthält eine Anleitung für das Patch Management für IACS, welches für alle gedacht ist, die Design- und Implementierungsverantwortung bzgl. des Patch Managements tragen.

2-4. Security Program Requirements for IACS Service Providers (IS)

Das Dokument enthält die Spezifikationen für Anforderungen an Service Provider, wie System- oder Wartungsintegratoren.

2-5. Implementation Guidance for IACS Asset Owners (TR)

Beinhaltet eine Anleitung für den Betrieb eines effektiven IACS-Cybersecurity-Programms. Der Teil ist vor allem für Asset Owner relevant, welche die Verantwortung für den Einsatz eines solchen Programms tragen.

3.2.3 3. Abschnitt: System Requirements

Der Abschnitt 3 behandelt die Anforderungen auf der Automatisierungssystem-Ebene:[82]

3-1 Security Technologies for IACS (TR)

Das Dokument beschreibt die Anwendung von diversen Sicherheitstechnologien für eine IACS-Umgebung. Der Teil ist für all jene interessant, die mehr über die Anwendung der diversen Sicherheitstechnologien erfahren möchten.

3-2 Security Risk Assessment and System Design (IS)

Hierbei geht es um das System-Design und die Risikobewertung. Der Standard behandelt das Zonen-und-Conduit-Modell und dessen entsprechende Risikobewertung sowie die Sicherheitslevels für diverse Ziele. Der Teil ist hauptsächlich für Asset Owner und Systemintegratoren interessant.

3-3 System Security Requirements and Security Levels (IS)

Dieser Teil beschreibt die Anforderungen für ein IACS-System, je nach Security-Level. Er betrifft die Lieferanten von Steuerungssystemen, die Systemintegratoren und die Asset Owner.

[82] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 5 – 6.

3.2.4 4. Abschnitt: Component / Product

Der letzte Abschnitt enthält Dokumente mit spezifischeren und detaillierteren Anforderungen, die für die Entwicklung von IACS-Produkten relevant sind:[83]

4-1 Product Security Development Lifecycle Requirements (IS)

Dieser Teil enthält Anforderungen an den Sicherheitsentwicklungslebenszyklus für Produktentwickler. Das Dokument ist vor allem für die Lieferanten von Steuerungssystemen und Produktkomponenten relevant.

4-2 Technical Security Requirements for IACS Components (IS)

Dieser Teil definiert die Anforderungen für die Komponenten, je nach Sicherheitslevel. Ebenso wie 4-1 ist dieser Teil für Lieferanten von Komponenten in Steuerungssystemen von Bedeutung.

[83] Vgl. ISA Global Cybersecurity Alliance (2020), Online-Quelle [25.11.2021], S. 6.

4 ERGÄNZENDE NORMEN UND RICHTLINIEN

In diesem Kapitel wird auf weitere relevante Normen und Richtlinien eingegangen, die für die IT/OT-Security als Ergänzung zur IEC 62443 Anwendung finden, um ein gesamtheitliches OT-Sicherheitskonzept zu erstellen. Für die Schaffung einer überblicksmäßigen Basis zur Evaluierung der Anwendbarkeit sind die Ansätze der Normen und Richtlinien beschrieben.

Die erarbeiteten Normen und Richtlinien, auf die aufgebaut wird, sind

- das NIS-Gesetz,
- die ISO/IEC 27001,
- die ISO/IEC 15408,
- der IT-Grundschutz-Katalog des Bundesamtes für Sicherheit in der Informationstechnik (*BSI*),
- die NIST SP 800-82,
- das NIST Cybersecurity Framework,
- Information Technology Infrastructure Library (*ITIL*),
- COBIT und
- die Center for Internet Security (*CIS*) Controls.

Die Anzahl von Normen und Richtlinien, die sich mit dem Thema Security beschäftigen und relevante Inhalte liefern, ist groß. Diese Arbeit beschränkt sich auf die verbreitetsten und relevantesten Standards.

4.1 NIS-Gesetz

Das Netz- und Informationssystemsicherheitsgesetz wurde auf Basis der entsprechenden EU-Richtlinie von 2016 zur Erhöhung des Sicherheitsniveaus von Netz- und Informationssystemen erlassen. Darin sind die entsprechenden nationalen Strategien zur Vermeidung etwaiger Sicherheitsvorfälle, die zu Versorgungsengpässen oder einer Gefährdung der öffentlichen Sicherheit führen würden, festgelegt.[84]

Das Gesetz betrifft Betreiber wesentlicher Dienste, sowie Anbieter von digitalen Diensten und Einrichtungen der öffentlichen Verwaltung.[85] Wesentliche Dienste sind:[86]

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasserversorgung
- Digitale Infrastruktur

[84] Vgl. Republik Österreich – Parlamentsdirektion (2018), Online-Quelle [25.11.2021], S. 1.

[85] Vgl. Netz- und Informationssystemsicherheitsgesetz – NISG (2021), S. 2.

[86] Vgl. Netz- und Informationssystemsicherheitsgesetz – NISG (2021), S. 2.

All jene müssen entsprechende und dem Stand der Technik angemessene Sicherheitsvorkehrungen treffen und diese in dreijährigen Intervallen dem Bundesministerium für Inneres vorweisen. Vorfälle oder Risiken in diesen Sektoren können an Computer-Notfallteams übermittelt werden. Diese Teams leiten Meldungen an das Bundesministerium für Inneres weiter und bieten weitere Hilfestellungen. Bei Sicherheitsvorfällen von wesentlichen Diensten muss das unverzüglich geschehen.[87]

4.2 ISO/IEC 27001

Die ISO 27001 ist die Norm, welche die Anforderungen an ein Informationssicherheitsmanagementsystem beschreibt. Die ISMS-Normenfamilie befasst sich mit Informationssicherheitsmanagementsystemen (*ISMS*). Die Norm ist auf Organisationen jeglicher Art und Größe skalierbar. Informationssicherheitsmanagementsysteme befassen sich mit dem Schutz von Informationen und stellen das Rahmenwerk für die Informationssicherheit in Organisationen dar. Sie verfolgen die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.[88]

Die Norm gliedert sich in die folgenden sieben Abschnitte, welche Anforderungen enthalten:[89]

4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Betrieb
9. Bewertung der Leistung
10. Verbesserung

Die Kapitel eins bis drei liefern generelle Informationen, die für die Anwendung der Norm von Relevanz sind, aber keine Anforderungen beinhalten.[90] Im Anhang A sind die entsprechenden Maßnahmen für Abschnitte fünf bis zehn niedergeschrieben, die getroffen werden müssen.

Weitere relevante Teile der ISMS-Normenfamilie sind die ISO 27000, die einen Überblick und die Begrifflichkeiten der ISMS-Normenreihe liefert[91] und die ISO 27002, in der die Anforderungen der ISO 27001 als Leitfaden für die Anwendung implementiert sind.[92] Weiters ist die ISO 27005 für das Risikomanagement von Bedeutung.[93]

[87] Vgl. Netz- und Informationssystemsicherheitsgesetz – NISG (2021), S. 2 – 13.

[88] Vgl. EN ISO/IEC 27001 (2017), S. 5 f.

[89] Vgl. EN ISO/IEC 27001 (2017), S. 6 – 16.

[90] Vgl. EN ISO/IEC 27001 (2017), S. 6.

[91] Vgl. EN ISO/IEC 27000 (2020), S. 7.

[92] Vgl. EN ISO/IEC 27002 (2017), S. 8.

[93] Vgl. EN ISO/IEC 27000 (2020), S. 25.

Die Norm ist vor allem auf die IT ausgerichtet und deshalb für die OT nicht optimal anwendbar, da auf wesentliche Funktionen und deren Ausfallssicherheit keine Rücksicht genommen wird.

Von weiterem Interesse ist das Whitepaper des Bundesverbands der Energie- und Wasserwirtschaft (*BDEW*). Dieses enthält Sicherheitsanforderungen der Systeme betreffend die Steuerung und Telekommunikation in der Energieversorgung. Dabei sind branchenspezifische Empfehlungen berücksichtigt, die auf die entsprechenden Anforderungen in den Normen ISO/IEC 27001 und ISO/IEC27019 aufbauen.[94]

4.3 ISO/IEC 15408

Die ISO/IEC 15408 ist der Standard der Evaluationskriterien für IT-Sicherheit. Als Evaluierungsgegenstand, welcher in der Norm mit *TOE* (Target of Evaluation) abgekürzt wird, kann jegliches Produkt herangezogen werden, wie beispielsweise eine Sammlung von Software, Firmware und Hardware. Der Scope, das ist der betrachtete Umfang, ist frei definierbar, daher kann es sich um die Betrachtung einer Kombination aus IT-Produkten, oder auch nur einen Teil davon handeln. Die Norm ist entsprechend aufgebaut, dass sie für die drei Zielgruppen Verbraucher*innen, Entwickler*innen und Evaluator*innen gleichermaßen verwendet werden kann. Zusätzlich bietet der Standard interessante Informationen für Systemverwalter*innen, Systemsicherheitsbeauftragte, Auditor*innen, Akkreditierer*innen, Sponsor*innen, Evaluierungsinstanzen, sowie Sicherheitsarchitekt*innen und -designer*innen.[95]

Die Norm ist in drei Teile untergliedert:[96]

Teil 1: Einführung und allgemeines Modell

Dieser Teil legt allgemeine Konzepte und Prinzipien der IT-Sicherheitsevaluierung fest und bestimmt ein allgemeines Evaluierungsmodell als Grundlage für die Evaluierung der Sicherheitseigenschaften von IT-Produkten.

Teil 2: Sicherheitsfunktionskomponenten

In diesem Teil sind Standard-Funktionskomponenten definiert und kategorisiert. Die Funktionskomponenten dienen als Grundlage für die funktionalen Anforderungen der TOEs.

Diese Sicherheitsfunktionskomponenten beschreiben das gewünschte Sicherheitsverhalten, um die angegebenen Sicherheitszielsetzungen zu erreichen.[97]

[94] Vgl. Österreichs Energie/BDEW (2018), Online-Quelle [25.11.2021], S. 5.

[95] Vgl. EN ISO/IEC 15408-1 (2020), S. 29 – 32.

[96] Vgl. EN ISO/IEC 15408-1 (2020), S. 32.

[97] Vgl. EN ISO/IEC 15408-2 (2020), S. 21.

Teil 3: Komponenten zur Sicherheitskontrolle

In diesem Teil sind Standard-Vertrauenswürdigkeitskomponenten definiert und kategorisiert, deren Zweck es ist, den TOEs eine Grundlage für die Vertrauenswürdigkeitsanforderungen zu bieten. Als Vertrauenswürdigkeit ist das Vertrauen für die Erreichung der Sicherheitszielsetzung von Komponenten definiert.[98] Zusätzlich beinhaltet dieser Teil Evaluierungskriterien für Schutzprofile (Protection Profile, *PP*) und Sicherheitsvorgaben (Security Target, *ST*), sowie sieben vordefinierte Sicherheitspakete, die auch Vertrauenswürdigkeitsstufen genannt werden.

Die Teile der Norm sind für die Interessensgruppen folgendermaßen relevant:

	Verbraucher*innen	**Entwickler*innen**	**Evaluator*innen**
Teil 1	Verwendung als Hintergrund-information und verpflichtend für Verweisungszwecke. Leitfadenstruktur für PPs.	Verwendung als Hintergrund-information und für Verweisungs-zwecke. Verpflichtend für die Entwicklung von Sicherheitsspe-zifikationen für TOEs.	Verpflichtend für Ver-weisungszwecke und als Leitfaden für die Struktur von PPs und STs.
Teil 2	Verwendung als Leitfaden und zur Verweisung bei der Festlegung von Aussagen zu Anforderungen für ein TOE.	Verpflichtend zur Verweisung bei der Interpretation von Aussagen zu funktionalen Anforderungen und bei der Formulierung von funktionalen Spezifikationen für TOEs.	Verpflichtend zur Verweisung bei der Interpretation von Aussagen zu funktionalen Anforderungen.
Teil 3	Verwendung als Leitfaden bei der Bestimmung der erforderlichen Sicherheitslevels	Verwendung als Verweisung bei der Interpretation von Aussagen zu Sicherheitsanforderungen bei der Bestimmung von Sicherheitskonzepten für TOEs.	Verwendung als Verweisung bei der Interpretation von Aussagen zu Sicherheitsanforderungen.

Tab. 3: Roadmap der ISO/IEC 15408 (PP: Protection Profile, ST: Security Target, TOE: Target of Evaluation), Quelle: EN ISO/IEC 15408-1 (2020), S. 32 (leicht modifiziert).

4.4 BSI IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium des deutschen Bundesamtes für Sicherheit in der Informationstechnik verfolgt die Aufrechterhaltung der Werte der Informationssicherheit und somit die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Das Kompendium enthält standardisierte Bausteine, die Geschäftsprozesse und Bereiche des IT-Umfelds thematisieren. Die darin enthaltenen Anforderungen werden mit den entsprechenden Sicherheitsmaßnahmen immer am aktuellsten Stand der Technik gehalten. Damit dient das Kompendium dem Erreichen eines höheren Sicherheitsniveaus.[99]

[98] Vgl. EN ISO/IEC 15408-3 (2021), S. 15.

[99] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021a), S. 1 – 2.

Der Aufbau der Bausteine ist stets derselbe und ist folgendermaßen standardisiert:[100]

- Allgemeine Beschreibung
- Zielsetzung
- Abgrenzung und Modellierung
- Spezifische Gefährdungen
- Anforderungen
    - Basisanforderungen
    - Standardanforderungen
    - Anforderungen bei erhöhtem Schutzbedarf
- Zuständige Rolle
- Weiterführende Informationen und Verweise
- Kreuzreferenztabelle für elementare Gefährdungen

Die Basisanforderungen sind mit minimalem Aufwand und maximalem Nutzen zu erzielen. Die Standardanforderungen erfüllen hingegen ihren Zweck entsprechend dem Stand der Technik für einen normalen Schutzbedarf. Anforderungen bei erhöhtem Schutzbedarf werden bei kritischen Objekten benötigt. Weiters ist der Part des Informationssicherheitsbeauftragten bei strategischen Entscheidungen stets miteinzubeziehen. Dieser trägt auch die Verantwortung für die Umsetzung der in den Konzepten festgehaltenen Anforderungen. Als Hilfsmittel zu den Bausteinen werden separat veröffentlichte, detaillierte Umsetzungsanleitungen, welche die Möglichkeiten entsprechender Sicherheitsmaßnahmen für die Umsetzung der Anforderungen erläutern, zur Verfügung gestellt.[101]

Es wird zwischen prozess- und systemorientierten Bausteinen unterschieden, wobei erstere für eine Gesamtheit von Informationen anwendbar sind und letztere auf einzelne Objekte oder Gruppen zutreffen. Diese beiden unterschiedlichen Schichten bestehen wiederum aus Teilschichten, wie in der folgenden Abb. 11 ersichtlich ist.[102]

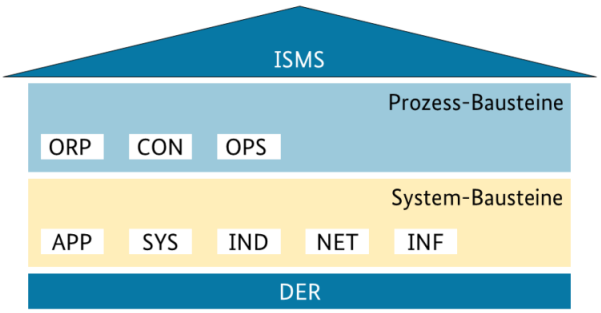

Abb. 11: Schichtenmodell des IT-Grundschutz-Kompendiums (ISMS: Informationssicherheitsmanagementsystem, ORP: Organisation und Personal, CON: Konzepte und Vorgehensweisen, OPS: Betrieb, APP: Anwendungen, SYS: IT-Systeme, IND: Industrielle IT, NET: Netze und Kommunikation, INF: Infrastruktur, DER: Detektion und Betrieb), Quelle: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021b), S. 1.

[100] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021a), S. 5.

[101] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021a), S. 5 – 6.

[102] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021b), S. 1 – 2.

Die einzelnen Bausteine werden den folgenden weiterführenden Schichten zugeordnet:[103]

- ISMS: Grundlage für weitere Aktivitäten im Informationssicherheitsprozess
- ORP: Organisatorische und personelle Sicherheitsaspekte
- CON: Konzepte und Vorgehensweisen
- OPS: Sicherheitsaspekte betrieblicher Art
- DER: Überprüfung der Maßnahmen, Detektion von Sicherheitsvorfällen und entsprechende Reaktion
- APP: Absicherung von Anwendungen und Diensten
- SYS: Einzelne IT-Systeme des Informationsverbunds
- IND: Sicherheitsaspekte industrieller IT
- NET: Vernetzungsaspekte
- INF: Infrastrukturelle Sicherheit

Die Schichten ISMS und DER sind Teil der Prozess-Bausteine-Schicht. Weiters kann für jeden Baustein einzeln entschieden werden, ob und wie dieser angewendet wird.[104]

Das IT-Grundschutz-Kompendium bietet zusätzlich einen Katalog mit 47 elementaren Gefährdungen, die für die Risikoanalyse optimiert, möglichst neutral und mit anderen Standards kombinierbar sind. Diese sind entsprechend in die Bausteine des IT-Grundschutzes integriert.[105]

4.5 NIST SP 800-82 Rev. 2

Die NIST Special Publication 800-82 ist eine Richtlinie für die Implementierung von sicheren industriellen Steuerungssystemen (ICS). Das Dokument liefert einen Überblick über die industriellen Steuerungssysteme und deren häufigsten Architekturen und Topologien, sowie die zugehörigen Schwachstellen und Bedrohungen mit möglichen Maßnahmen zur Risikominimierung. Weiters ist ein „Security Control Overlay“, das ist eine Sammlung von Anforderungen, die von der NIST SP 800-53 Rev. 4, dem Standard für Security- und Datenschutz-Anforderungen, entnommen und entsprechend an ICS angepasst wurde, enthalten. Da ICS sich je nach Anwendungsbereich unterscheiden, sind eine Reihe von unterschiedlichen Maßnahmen und Techniken, um die ICS-Security zu unterstützen, beschrieben. Damit sollen Interessierte ermutigt werden einen risikobasierten Ansatz auf die Systeme anzuwenden und durch die Nutzung der Richtlinie die Security entsprechend anzupassen.[106]

[103] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021b), S. 1 – 2.

[104] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021b), S. 1 – 2.

[105] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2021a), S. 4.

[106] Vgl. NIST SP 800.82 Rev. 2 (2015), S. 1-1.

Der Standard ist in sechs Abschnitte unterteilt:[107]

Abschnitt 1: Einführung

Abschnitt 2: Überblick über ICS und Vergleich von ICS und IT-Systemen

Abschnitt 3: ICS-Risikomanagement und -Risikobewertung

Abschnitt 4: Überblick über die Entwicklung und Verteilung eines ICS-Sicherheitsprogramms, um Schwachstellen zu minimieren

Abschnitt 5: Empfehlungen für die Integration in ICS-typische Netzwerkarchitekturen

Abschnitt 6: Zusammenfassung von ICS-spezifischen Anforderungen, die von der „NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations“ abgeleitet sind

Anhänge: Weiterführende Inhalte, wie ein Glossar, ein Abkürzungsverzeichnis, eine Liste mit Bedrohungen, Schwachstellen und Ereignissen, sowie eine Liste mit Security-Aktivitäten. Des Weiteren sind eine Liste mit Security-Möglichkeiten und -Werkzeugen, ein Quellenverzeichnis, sowie das vollständige „Security Control Overlay“ für ICS enthalten.

Diese technische Richtlinie richtet sich an alle, die mit ICS und deren Security zu tun haben, das sind Techniker*innen, Integrator*innen, Architekt*innen, Systemadministrator*innen, Security-Berater*innen, (Senior-)Manager*innen, Verkäufer*innen von ICS-Produkten, sowie Forscher*innen und Analyst*innen, die an den Sicherheitsbedürfnissen von ICS interessiert sind.[108]

4.6 NIST Cybersecurity Framework

Das Cybersecurity Framework des amerikanischen National Institute of Standards and Technology wurde entwickelt, da ein priorisierter, flexibler, wiederholbarer, performancebezogener und preiswerter Ansatz für Informationssicherheitsanforderungen und -maßnahmen für kritische Infrastrukturen für die Cyber-Risikoanalyse, -bewertung und das -management notwendig wurde. Das Framework ist sowohl für die IT, ICS, CPS und (zum Beispiel über das IoT) verbundene Systeme entwickelt worden. Weiters ist es ebenfalls für die Anwendung in allen Bereichen von Organisationen ausgelegt und nicht nur für kritische Infrastrukturen. Daher ergeben sich auch unterschiedliche Arten der Anwendung, die von den Organisationen selbst definiert werden. Aus diesem Grund kann das Framework auch nicht überall gleichermaßen angewendet werden, da sich die Bedrohungen, Schwachstellen und Risikotoleranzen und somit die Risiken unterscheiden.[109]

[107] Vgl. NIST SP 800.82 Rev. 2 (2015), S. 1-2.

[108] Vgl. NIST SP 800.82 Rev. 2 (2015), S. 1-1 f.

[109] Vgl. NIST Cybersecurity Framework (2018), S. 1 – 3.

Das Framework ist in drei Teile unterteilt. Den “Framework Core”, die “Framework Implementation Tiers” und das “Framework Profile”.[110]

Framework Core

Der sogenannte Kern des Frameworks beinhaltet eine Sammlung von Aktivitäten für die Erreichung von speziellen Cybersecurity-Outcomes. Die Outcomes weisen vier Elemente auf. Diese sind Funktionen, Kategorien, Subkategorien und informative Referenzen. Die Funktionen (Functions) dienen der Organisation von Informationen, dem Treffen von Risikomanagemententscheidungen, der Zuordnung von Bedrohungen sowie der Berücksichtigung von vergangenen Aktivitäten und werden in fünf Gruppen untergliedert, die unterschiedliche Entwicklungen und Implementierungen verfolgen.[111]

Diese sind: [112]

- **Identify (Identifizieren)**: Organisatorisches Verständnis für Sicherheitsrisiken
- **Protect (Schützen)**: Schutzmaßnahmen für kritische Services
- **Detect (Erkennen)**: Ermittlung von Sicherheitsvorfällen
- **Respond (Reagieren)**: Umgang mit Sicherheitsvorfällen
- **Recover (Wiederherstellen)**: Wiederherstellung nach Sicherheitsvorfällen

Die Kategorien (Categories) sind Gruppen von Outcomes innerhalb der Funktionen, die mit entsprechenden Aktivitäten verbunden sind. Die Subkategorien (Subcategories) unterteilen die Kategorien in spezifischere Anforderungen der Outcomes. Diesen werden informative Referenzen (Informative References) auf relevante Normen, Richtlinien und Standards zugeordnet, aus denen Methoden zur Erreichung der Outcomes entnommen werden können.[113]

Die vier Elemente sind im Framework Core, wie im folgenden Auszug ersichtlich, dargestellt:

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8

Abb. 12: Anforderung aus dem NIST Cybersecurity Framework, Quelle: NIST Cybersecurity Framework (2018), S. 41 (leicht modifiziert).

[110] Vgl. NIST Cybersecurity Framework (2018), S. 3 f.

[111] Vgl. NIST Cybersecurity Framework (2018), S. 6 f.

[112] Vgl. NIST Cybersecurity Framework (2018), S. 7 – 8.

[113] Vgl. NIST Cybersecurity Framework (2018), S. 6 f.

Framework Implementation Tiers

Die Framework-Implementierungsstufen (Framework Implementation Tiers) beschreiben den Grad der Genauigkeit und Detailliertheit des Risikomanagements der Organisation. Dafür muss die angezielte Stufe definiert werden. Es muss sichergestellt werden, dass die Ziele der Organisation erreicht werden, die Implementierung möglich ist und die Sicherheitsrisiken von kritischen Assets reduziert werden und somit für die Organisation vertretbar sind. Jedoch sind die Stufen kein Maßstab für die erfolgreiche Anwendung des Frameworks, sondern nur eine Hilfestellung dafür. Der Erfolg wird über die Profile gemessen.[114]

Es wird zwischen den folgenden vier Stufen (Tiers) unterschieden, die von einer teilweisen Anwendung bis zu einer ständigen Verbesserung reichen:[115]

- Tier 1: Partial (Teilweise)
- Tier 2: Risk Informed (Risikobewusst)
- Tier 3: Repeatable (Wiederholbar)
- Tier 4: Adaptive (Ständige Verbesserung)

Framework Profile

Das Framework-Profil (Framework Profile) ist eine Zuordnung von Funktionen, Kategorien und Subkategorien entsprechend den Anforderungen, der Risikotoleranz und den Ressourcen der Organisation. Daraus ergibt sich eine Roadmap für die Reduktion von Sicherheitsrisiken. Je nach Größe und Komplexität von Organisationen kann es auch mehrere Profile geben, die auf spezifische Komponenten angewendet werden. Ebenso können die Profile zur Definition und zum Vergleich des IST- und SOLL-Zustands verwendet werden, um mögliche Sicherheitslücken aufzudecken.[116]

4.7 ITIL V4

ITIL ist eine Bibliothek von universal anwendbaren Richtlinien und Best Practices für die IT. Da dieses Framework beschreibt WAS und nicht WIE etwas zu tun ist, kann es weitläufig angewendet werden.[117]

Diese definierten Rahmenbedingungen können von Organisationen verwendet und angepasst werden, um die Umsetzung von IT-fähigen Services im Rahmen des IT-Service-Managements (*ITSM*) zu verbessern. Das Service Management ist für die Umsetzung der im Unternehmen zurzeit benötigten IT-Services verantwortlich. Es wird ein praktischer Ansatz verfolgt, der sich über einige Jahre entwickelt hat. Der Erfolg von ITIL ergibt sich durch die Unabhängigkeit von Lieferanten, die Best-Practice-Strategie und dem Fehlen von Vorschriften für die Umsetzung der Elemente.[118]

[114] Vgl. NIST Cybersecurity Framework (2018), S. 8 f.

[115] Vgl. NIST Cybersecurity Framework (2018), S. 9 f.

[116] Vgl. NIST Cybersecurity Framework (2018), S. 11.

[117] Vgl. ClydeBank Technology (Hrsg.) (2016), S. 9.

[118] Vgl. Agutter (2020), S. 17 – 19.

In der ITIL V4 sind vier Dimensionen, auf die sich Organisationen bestenfalls beziehen sollten, um gesamtheitlich Werte zu schöpfen, für das Service-Werte-System von Bedeutung:[119]

- Organisationen und Menschen
- Information und Technologie
- Partner und Lieferanten
- Wertströme und Prozesse

Ein weiteres Merkmal der ITIL V4 ist das Service-Werte-System (Service Value System). Dieses beschreibt, wie sämtliche Komponenten und Aktivitäten einer Organisation als System zusammenarbeiten, um Werte zu schaffen. Es umfasst folgende kollaborierende Elemente, die gesamtheitlich betrachtet werden:[120]

- Möglichkeit/Nachfrage
- Wert
- Richtlinien
- Kontrolle
- Service-Wertschöpfungskette
- Praktiken
- Kontinuierliche Verbesserung

Die vier Dimensionen und das Service-Werte-System werden für die Anwendung der Methoden benötigt. Dabei handelt es sich um eine Zusammenfassung von Ressourcen für die Durchführung einer Arbeit, oder das Erreichen eines Ziels. Insgesamt gibt es 34 Methoden, welche sich auf General Management Practices (Allgemeine Management-Methoden), Service Management Practices (Service-Management-Methoden) und Technical Management Practices (Technische Management-Methoden) aufteilen.[121]

[119] Vgl. Agutter (2020), S. 41.

[120] Vgl. Agutter (2020), S. 53 – 56.

[121] Vgl. Agutter (2020), S. 86.

4.8 COBIT 2019

COBIT ist ein Framework, dass sich mit der sogenannten „Enterprise Governance of Information and Technology“ (*EGIT*), also der Steuerung von Informationen und Technologie für das gesamte Unternehmen befasst. Es wird zwischen Management und Verwaltung (Governance) unterschieden, da sich daraus unterschiedliche Anforderungen und Zielsetzungen (Objectives) ergeben.[122]

Das COBIT 2019 Framework umfasst derzeit vier Teile:[123]

- COBIT 2019 Framework: Introduction and Methodology
  (Einführung und Methodik)
- COBIT 2019 Framework: Governance and Management Objectives
  (Governance- und Managementziele)
- COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution
  (Designen einer Informations- und Technologie-Governance-Lösung)
- COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance
  (Implementieren und Optimieren einer Informations- und Technologie-Governance)

Das Framework enthält in Summe 40 Verwaltungs- und Management-Objectives zur Erreichung der Unternehmensziele, welche in fünf Gruppen gegliedert sind. Die Verwaltungs-Objectives fallen in die Domäne “Evaluate, Direct and Monitor” (Bewerten, Lenken und Überwachen, EDM). Die Management-Objectives befinden sich in den Domänen “Align, Plan and Organize” (Ausrichten, Planen und Organisieren, APO), “Build, Acquire and Implement” (Aufbauen, Beschaffen und Implementieren, BAI), “Deliver, Service and Support” (Liefern, Warten und Unterstützen, DSS) sowie “Monitor, Evaluate and Assess” (Überwachen, Evaluieren und Bewerten, MEA). Für die Erreichung der Objectives beziehen sich diese immer auf einen Prozess und die zugehörigen Komponenten.[124]

Komponenten können unterschiedlichster Natur sein, wie[125]

- Prozesse, Organisationsstrukturen,
- Richtlinien, Prinzipien und Frameworks,
- Informationen,
- Kultur, Ethik und Verhalten,
- Menschen, Fähigkeiten und Kompetenzen, sowie
- Services, Infrastruktur und Anwendungen.

[122] Vgl. ISACA (2018), Online-Quelle [25.11.2021], S. 12 f.

[123] Vgl. ISACA (2018), Online-Quelle [25.11.2021], S. 19 f.

[124] Vgl. ISACA (2018), Online-Quelle [25.11.2021], S. 20.

[125] Vgl. ISACA (2018), Online-Quelle [25.11.2021], S. 21 f.

Die Objectives und Komponenten werden in den benötigten Kombinationen auf spezifische Schwerpunktbereiche angewendet. Schwerpunkte unterscheiden sich je nach Organisation und Anwendungsbereich und sind somit unlimitiert definierbar.[126]

Das Design von Verwaltungssystemen hängt von einigen Faktoren ab, die beliebig miteinander kombiniert werden können.[127] Welche das sind, ist in der folgenden Abbildung dargestellt:

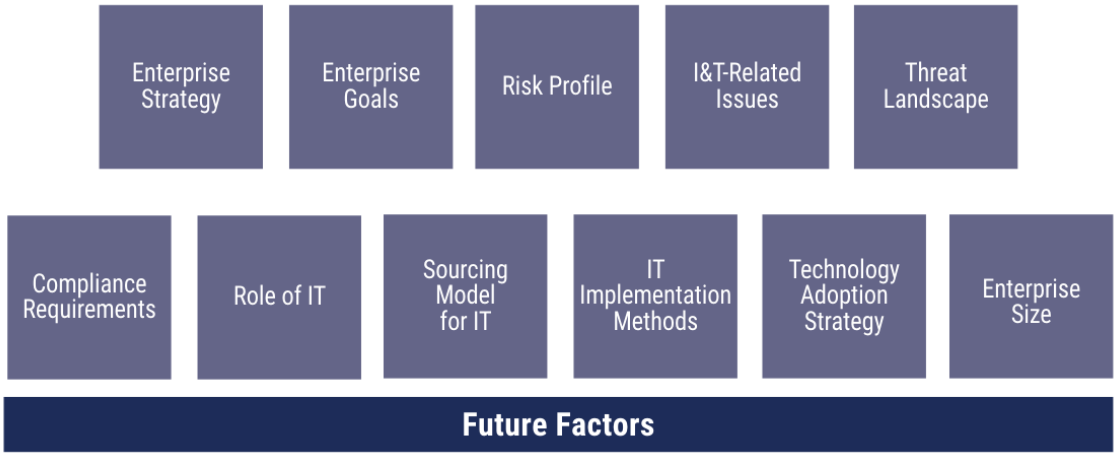

Abb. 13: Designfaktoren von COBIT 2019 (IT: Information Technology), Quelle: ISACA (2018), Online-Quelle [25.11.2021], S 23.

Diese Designfaktoren beeinflussen die Anpassung der Verwaltungssysteme an Unternehmen.[128]

4.9 CIS Controls

Die CIS Controls (Center of Internet Security Regeln) sind eine Kombination des Wissens von Experten mit unterschiedlichen Rollen aus verschiedenen Branchen. Diese stellen eine Sammlung von Aktionen für Unternehmen und Industrien dar. Für die Entwicklung werden die Kriterien der Anpassbarkeit an andere Normen und Richtlinien, die Messbarkeit, die Umsetzbarkeit, der Fokus auf das Wesentliche und das spezifische Wissen von Attacken angewendet. Die Version 8 der CIS Controls enthält 18 Controls, die je einen Überblick, eine Beschreibung der Kritikalität des Controls, Prozeduren und Tools für die benötigten Aktionen und die Beschreibungen der zugehörigen Schutzmaßnahmen beinhalten.[129]

[126] Vgl. ISACA (2018), Online-Quelle [25.11.2021], S. 22 f.

[127] Vgl. ISACA (2018), Online-Quelle [25.11.2021], S. 23.

[128] Vgl. ISACA (2018), Online-Quelle [25.11.2021], S. 45.

[129] Vgl. Center for Internet Security (2021), Online-Quelle [25.11.2021], S. 1 – 5.

Die Schutzmaßnahmen der Controls werden in drei sogenannte Implementation Groups (*IG*) kategorisiert.[130] Die einzelnen Gruppen sind folgendermaßen definiert:[131]

> **IG 1**: Betrifft Klein- und Mittelunternehmen (KMU), die mit minimalem Aufwand das Maximum an Cybersecurity erreichen wollen. Das Unternehmen soll möglichst einsatzbereit sein und Ausfallszeiten sollen möglichst vermieden werden. Die Sicherheitsmaßnahmen in dieser Gruppe sind simpel gehalten und werden somit typischerweise auf Standard-Hardware und -Software angewendet.
>
> **IG 2** (aufbauend auf IG 1): Diese Gruppe bezieht sich auf Unternehmen mit eigenen IT-Verantwortlichen und mehreren Abteilungen mit unterschiedlichen Risikoanforderungen. Oft sind dabei sensible Daten im Spiel. Kurze Ausfälle können verkraftet werden, jedoch ist der Verlust von Vertrauenswürdigkeit ein großes Problem. Sicherheitsmaßnahmen sollen Sicherheitsteams im Umgang mit der gesteigerten Komplexität unterstützen.
>
> **IG 3** (aufbauend auf IG 1 und IG 2): In diesen Unternehmen gibt es bereits Sicherheitsexperten, die sich auf die spezifischen Sicherheitsfacetten spezialisieren. Die sensiblen Funktionen und Informationen werden beaufsichtigt. Erfolgreiche Attacken können die öffentliche Sicherheit gefährden. Sicherheitsmaßnahmen betreffen die Abschwächung von gezielten Attacken und Zero-Day-Attacken.

Je nach Komplexität der Organisation werden die Gruppen in aufsteigender Reihenfolge angewendet. Dabei bezieht die darauffolgende Gruppe immer die vorherige mit ein. So wird eine Grundlage geschaffen, die standardmäßig implementiert sein soll und auf sämtliche Unternehmen zutrifft. Diese kann in den aufbauenden Gruppen auf jeweils ähnliche Risikoprofile angewendet werden.[132]

[130] Vgl. Center for Internet Security (2021), Online-Quelle [25.11.2021], S. 5.

[131] Vgl. Center for Internet Security (2021), Online-Quelle [25.11.2021], S. 6.

[132] Vgl. Center for Internet Security (2021), Online-Quelle [25.11.2021], S. 5.

5 INFORMATIONSSICHERHEIT VON TUNNELSTEUERUNGS-SYSTEMEN

Tunnelsteuerungssystemen stellen Systeme dar, die für die vollumfängliche Steuerung von Tunnelanlagen zuständig sind. Es handelt sich um das Zusammenspiel sämtlicher verteilter IT/OT-Komponenten innerhalb eines SCADA-Systems.

5.1 Aufbau von Tunnelsteuerungssystemen

Die Tunnelsteuerungssysteme sind in allen Anlagen ähnlich aufgebaut. Je nach Tunnellänge und Anforderungen des Auftraggebers unterscheiden sich die Anzahl der Komponenten, sowie die Schnittstellen zu Feldgeräten und Fremdgewerken. In der nachfolgenden Grafik ist beispielhaft eine reduzierte Topologie dargestellt:

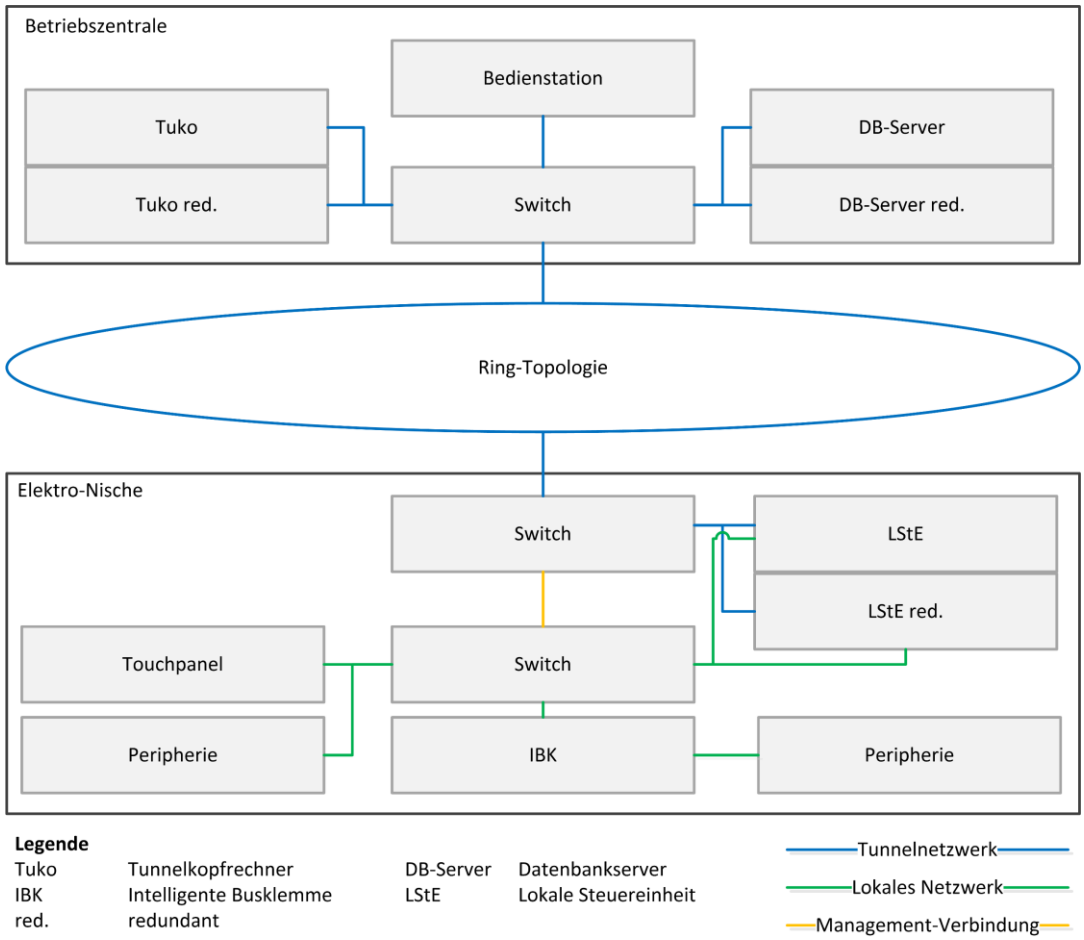

Abb. 14: Topologie eines beispielhaften Tunnelsteuerungssystems, Quelle: Eigene Darstellung.

Die Abbildung ist stark vereinfacht und dient rein dem Überblick der unterschiedlichen Komponenten und deren Verbindung zum Tunnelnetzwerk. Die einzelnen abgebildeten IT/OT-Komponenten werden im nachfolgenden Unterkapitel genauer erläutert.

Die Einteilung von Tunnelsteuerungssystemen in SCADA-Systeme basiert auf geografisch weitläufigen Anlagen mit vielen unterschiedlichen Örtlichkeiten, in denen IT/OT-Komponenten verteilt sind. Weiters wird ein zentraler Server, bzw. ein redundantes Server-Paar zur Überwachung und Steuerung verwendet.

Das Tunnelnetzwerk wird in Netzsegmente, abhängig von der Örtlichkeit, mit zugeordneten Virtual Local Area Networks (*VLAN*) gegliedert. Je nach Anlage befinden sich die angebundenen Feldgeräte in einem lokalen Netz der entsprechenden Örtlichkeit, oder im spezifischen Netzwerksegment des Standorts als Teil des Tunnelnetzwerks.

In Abb. 14 sind schematisch die Betriebszentrale (*BZ*) und eine Elektro-Nische (E-Nische, *EN*) abgebildet. Es gibt aber weitaus mehr Örtlichkeiten in Tunnelanlagen, die IT/OT-Komponenten beinhalten. Ein beispielhafter Aufbau mitsamt einer Anordnung der unterschiedlichen Standorte wird in folgender Abb. 15 präsentiert:

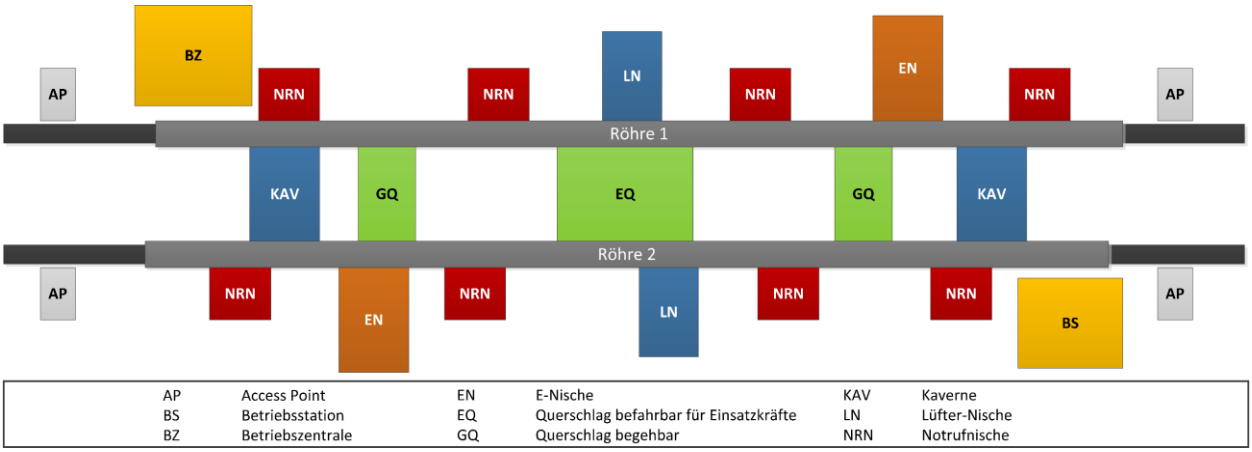

Abb. 15: Aufbau eines Beispieltunnels, Quelle: Eigene Darstellung.

Jeder Tunnel bzw. jede Tunnelkette besitzt eine Betriebszentrale, in der die zentralen Server, das sind Tunnelkopfrechner (*Tuko*) und Datenbankserver (*DB-Server*), verbaut sind. Zusätzlich befindet sich eine Bedienstation zur Bedienung des SCADA-Systems in der Zentrale. Ergänzend zur BZ liegt am anderen Tunnelende oder Ende der Tunnelkette eine Betriebsstation (*BS*). Diese entspricht meistens der Größe einer BZ. Der größte Unterschied zwischen diesen beiden Örtlichkeiten besteht darin, dass die BS keinen zentralen Server enthält.

In der Regel befinden sich in einem Tunnel mehrere E-Nischen, wobei die Anzahl je nach Tunnellänge variiert. Darin befinden sich lokale Steuereinheiten (*LStE*), die als Sub-Stationen der Tunnelkopfrechner Daten einsammeln und Aktionen steuern, Touchpanels zur lokalen Bedienung, sowie die Feldgeräte. Im Freifeld erfüllen diesen Zweck die Access-Points (*AP*). Im Wesentlichen verfolgen auch Lüfter-Nischen (*LN*) und Kavernen (*KAV*) denselben Zweck, nur, dass diese andere Gewerke umfassen.

Notruf-Nischen (*NRN*) beinhalten wiederum lediglich Notrufeinheiten und Hörer, die an intelligente Busklemmen (*IBK*) angebunden sind, deren Signale über die lokale(n) Steuereinheit(en) der nächstgelegenen E-Nische oder des nächstgelegenen Betriebsgebäudes verarbeitet werden.

Bei Tunneln mit mehr als einer Röhre, existiert zumindest ein begehbarer Durchgang mit der Bezeichnung Querschlag (*GQ*), um im Ereignisfall in die andere Röhre flüchten zu können. Die Anzahl der Querschläge ergibt sich durch die Tunnellänge. Bei langen Tunneln werden ebenfalls befahrbare Querschläge (*EQ*) errichtet, um Einsatzkräften einen Weg in die betroffene Röhre zu ermöglichen. Je nach Größe und Art des Durchgangs befinden sich darin IBKs oder ebenfalls lokale Steuereinheiten und Touchpanels.

Je nach Gegebenheiten kommen Hochbehälter zur Sammlung und Gewässerschutzanlagen zur Reinhaltung von Wasser zum Einsatz. Hierbei werden ebenfalls lokale Steuereinheiten, IBKs und Touchpanels eingesetzt, um die benötigten Ventile und Pumpen entsprechend den Wasserständen zu regulieren.

In jeder der Örtlichkeiten befinden sich üblicherweise zumindest ein oder mehrere Verteilerschränke, in denen die IT/OT-Komponenten eingebaut sind. Die Einrichtungen unterscheiden sich je nach Anlage aufgrund der Gegebenheiten und Anforderungen. Die beschriebenen Aspekte sollen nur einen Anhaltspunkt liefern und sind nicht als Standard anzusehen, da jede Tunnelanlage individuell geplant wird.

Die Leittechnik wird an die vorgegebenen Gewerke entsprechend angepasst. Folgende Gewerke sind in Tunneln unter anderem üblich:

- Lüftung
- Beleuchtung
- Verkehr
- Energie
- Funk
- Brand
- Notruf
- Akut
- Video
- Türen & Tore
- Gewässerschutz
- Löschwasser

Die Herausforderung besteht darin, die Gewerke, die teilweise oder vollumfänglich von Fremdfirmen geliefert werden, in das Leitsystem zu integrieren. Dabei sind die einzusetzenden Protokolle und Schnittstellen meistens vorgegeben.

5.2 Relevante IT/OT-Komponenten

Die relevanten IT/OT-Komponenten wurden zum Teil schon beim Aufbau der Tunnelanlagen erwähnt. In diesem Abschnitt wird genauer auf die einzelnen Typen und ihre Aufgaben eingegangen.

Sobald die Leittechnikkomponenten in Betrieb sind, wird darauf mit einer Fernverbindung über ein passwortgesichertes VPN zugegriffen. Der Fernwartungszugang wird vom Auftraggeber zur Verfügung gestellt und erfordert zwei Faktoren zur Anmeldung, und zwar ein komplexes Passwort und ein generierter Token. Die Benutzerkonten sind hierbei personalisiert und dürfen auch nur von der zugewiesenen Person benutzt werden, um Vorfälle direkt zuordnen zu können. Das ist durch die Aufzeichnung der Fernverbindungssitzungen möglich. Die Fernwartung bietet die Möglichkeit sich direkt auf die Serverebene zu verbinden. Weitergehend kann die Verbindung von den Servern auf die Steuerebene hergestellt werden. Der Datenaustausch, um Informationen von und zur Anlage zu transferieren, findet über eine separate, beigestellte Plattform statt. Sämtliche benötigte Daten müssen darauf hochgeladen und davon heruntergeladen werden. Damit finden erste Überprüfungen auf Malware statt.

5.2.1 Tunnelkopfrechner (Tuko)

Die Tunnelkopfrechner sind redundant ausgeführte, zentrale Server mit Windows-Betriebssystem, worauf die Prozessleitsoftware „XAMControl“ ausgeführt wird. Diese verwaltet die Logik und sämtliche Daten der untergeordneten lokalen Steuereinheiten und stellt sie diesen bereit. Die lokale Bedienung auf den Touchpanels wird ebenso über die Tukos gelenkt. Ein wesentlicher Aspekt ist die Überwachung der IT/OT-Komponenten und entsprechende Alarmgenerierung bei der Überschreitung von Grenzwerten. Gleichzeitig führen sie den notwendigen Datenaustausch mit den Datenbankservern und der darauf befindlichen Datenbank durch. Weiters dient einer der beiden Tunnelkopfrechner als Backup-Verzeichnis für die Backups. Zusätzlich verteilen beide die Systemzeit, die mit dem Zeitserver des Auftraggebers abgeglichen wird, über das Network Time Protocol (*NTP*) an die lokalen Steuereinheiten und Touchpanels. Somit sind die Tukos für das Zusammenspiel aller Komponenten verantwortlich. Daher müssen Ausfälle dieser Server unbedingt vermieden werden.

Die Tukos werden virtualisiert auf einem Hyperconverged-Infrastructure-Cluster, abgekürzt *HCI*-Cluster, des Auftraggebers betrieben. Daher liegen nur die Betriebssystemebene und die Applikationsebene in der Verantwortung der Dürr Austria GmbH. Die Hardware, in diesem Fall der HCI-Cluster, wird vom Auftraggeber verwaltet.

5.2.2 Datenbankserver (DB-Server)

Die benötigte Microsoft SQL-Datenbank-Instanz wird auf beiden redundant ausgeführten Datenbankservern installiert und gespiegelt. Dabei handelt es sich ebenso um virtuelle Maschinen mit Windows-Betriebssystem auf den HCI-Clustern. Die Instanz unterteilt sich in zwei Datenbanken, die für „XAMControl“ benötigt werden. Das ist zum einen die „XAMControlX4“- und zum anderen die „XAMRuntimeX4“-Datenbank. Diese Server dienen rein dem Datenerhalt. Daher werden täglich Datenbank-Backups erstellt, um im Ernstfall möglichst wenige Daten zu verlieren. Zusätzlich werden vom Auftraggeber regelmäßige Snapshots der virtuellen Maschinen erstellt.

5.2.3 Virtuelle Desktopinfrastruktur (VDI)

Die virtuelle Desktopinfrastruktur (*VDI*) wird ebenso, wie Tunnelkopfrechner und Datenbankserver, vom Auftraggeber virtualisiert beigestellt und basiert auf einem Windows-Betriebssystem. Sie dient vor allem der Installation von Debug- und Administrationssoftware, die Sicherheitslücken aufweisen könnte, und zum Aufbau von Remote-Verbindungen mit dem Leitsystem. Das hat den Hintergrund, dass die VDI nicht relevant für die Steuerung des Systems ist und somit ohne zu erwartende Ausfälle heruntergefahren oder formatiert werden kann.

5.2.4 Testsystem

Das Testsystem besteht aus virtuellen Maschinen, die ident zu den Tunnelkopfrechnern und Datenbankservern sind. Es ist ebenfalls im HCI-Cluster eingebettet. Die Möglichkeiten für die Durchführung von Tests sind sehr beschränkt, da sich das Testsystem im selben Netzwerk, wie das Produktivsystem befindet. Aufgrund der Tatsache, dass „XAMControl“ auf den Test-Tukos die selben IP-Adressen wie das Produktiv-Leitsystem anspricht, können maßgebliche Probleme entstehen. Daher wird das Testsystem nur für die Überprüfung von Patches, Updates und Einstellungen herangezogen.

5.2.5 Bedienstationen (BST)

Die Bedienstationen dienen der Steuerung des gesamten Systems. Das heißt, es wird eine Visualisierung des gesamten Tunnels dargestellt. Sie werden ebenso beigestellt und verfügen über ein Windows-Betriebssystem. In jeder Anlage wird grundsätzlich mindestens eine Bedienstation in wesentlichen Betriebsgebäuden, und zum Teil auch eine in Verkehrsmanagementzentralen, für die unmittelbare Bedienung des spezifischen Tunnels, verbaut. Durch den sogenannten „XAMIrisProxy“-Dienst öffnet sich nach dem Starten automatisch die „XAMIris“-Visualisierungssoftware. Dieser Dienst hat die Aufgabe, die „XAMIris“ zu starten, wenn sie nicht geöffnet ist. Standardmäßig wird sie mit einem Account mit Leserechten geöffnet. Danach können sich die Benutzer*innen individuell anmelden und erhalten die entsprechenden Berechtigungen. Weiterführend werden BST häufig für die Generierung von Excel-Reports verwendet, um die Aufzeichnungen von Trends darzustellen. Für die ordnungsgemäße Darstellung wird Excel auf den Bedienstationen benötigt.

5.2.6 Lokale Steuereinheiten (LStE)

Die lokalen Steuereinheiten werden als Industrie-PCs (*IPC*) mit einem Windows Betriebssystem und darauf installierten Software(-speicherprogrammierbaren-Steuerungen) ausgeführt. Sie sind für die Abläufe der Prozesse im örtlichen Umfeld verantwortlich und übermitteln die verarbeiteten Daten an die Tunnelkopfrechner. Je nach Bedeutsamkeit der angebundenen Gewerke werden sie redundant ausgeführt. Dabei wird vor allem die menschliche Sicherheit in Betracht gezogen. Bei einer Ausführung mit lokalen Netzwerken werden sie in dieses und ins Tunnelnetzwerk eingebunden. Das ist durch die zwei eingebauten Ethernet-Ports möglich, denen die geplanten IP-Adressen statisch und gemäß dem Netzwerk zugeordnet werden.

Die „XAMControl“-Soft-SPSen benötigen einen eigenen Dienst mit dem Namen „XAMPLC“. Dieser greift auf die lokale SQL-Datenbank zu. In dieser werden sämtliche Daten rund um die angebundenen Systeme der LStE verwaltet. Der Datenaustausch zum redundanten Gegenstück findet nicht direkt, sondern über die Tukos statt.

Zusätzlich sind die folgenden „XAMControl“-Dienste notwendig:

- Alarm Server
- Alerting Server
- Modbus TCP
- OPC UA (optional)
- IEC 104 (optional)

Außerdem wird auf den lokalen Steuereinheiten Administrations- und falls benötigt Debugsoftware installiert und ausgeführt, insofern diese nicht auf der VDI betrieben werden kann.

Für die Nutzung von Services des Auftraggebers ist eine Anbindung in den Windows-Verzeichnisdienst, Active Directory (*AD*), gefordert. Daher werden auch die vorgegebenen Host-Namenskonventionen verwendet. Somit stehen für das Aktuell-Halten der Tunnelanlagen die Windows Server Update Services (*WSUS*), ein Schwachstellenmanagementtool und eine Monitoring-Lösung zur Verfügung.

5.2.7 Touchpanels (TP)

Touchpanels bieten die Möglichkeit der lokalen Bedienung der angebundenen Feldkomponenten der Örtlichkeit, in der sie sich befinden. Das bedeutet, dass die Komponenten, die von der lokalen Steuereinheit an diesem Standort gesteuert werden, über das Touchpanel geregelt werden können.

Diese Komponenten sind wie die lokalen Steuereinheiten mit Windows ausgestattet und in die AD integriert. Sie haben nur „XAMControl“ und eine Software zum Abgleich der Systemzeit installiert. Gleich wie bei den Bedienstationen wird der „XAMIrisProxy“-Dienst für das automatische Öffnen der Visualisierung aktiviert.

5.2.8 Feldkomponenten

Jegliche Feldkomponenten werden von den lokalen Steuereinheiten gesteuert. Entweder werden diese direkt mit dem Switch oder über eine IBK mit dem Switch verbunden. Diese Komponenten befinden sich im selben Netzwerk wie die lokalen Steuereinheiten dieser Örtlichkeit. Das kann das Tunnelnetzwerk oder ein lokales Netzwerk sein, welches vom öffentlichen Tunnelnetzwerk abgekapselt ist. Komponenten, die nicht an den Bus angebunden sind, werden größtenteils über Ethernet verbunden. Dadurch kommen häufig proprietäre Protokolle zum Einsatz.

Folgende Feldkomponenten werden unter anderem eingesetzt:

- Doppelzählschleifen
- Wechselverkehrszeichen
- Medienkonverter
- Brandmeldezentrale
- Linienmeldezentrale
- Universalmessgeräte
- Unterbrechungsfreie Stromversorgung
- Intelligente Busklemmen
    - Ampeln
    - Höhenkontrolle
    - Leuchtdichtekameras
    - Leuchtstärkemessgeräte
    - Ventilatoren
    - Ventile
    - Pumpen
    - Beleuchtung

Die IBKs bieten digitale und analoge Ein- und Ausgänge. Bei den Analogwerten werden Strom- oder Spannungsbereiche an die angebundenen Geräte angepasst, um die Signale weiterverarbeiten zu können.

Die Feldkomponenten verfügen über eine Firmware, die nach Vorgaben des Auftraggebers bei der Inbetriebnahme aktuell sein muss. Bei Bekanntwerden von Schwachstellen muss sie ebenfalls aktualisiert werden.

5.2.9 Switches und Netzwerkkomponenten

Diese Geräte werden, so wie das gesamte Netzwerk, vom Auftraggeber geplant, konfiguriert und beigestellt. Das Tunnelnetzwerk wird in der Regel als Ringtopologie aufgebaut. Einige Anlagen verfügen über zusätzliche lokale Netzwerke innerhalb von Gebäuden und Nischen. Die IP-Adressen- und Portbelegungslisten werden vom AG übermittelt, um die Netzwerkeinstellungen der Komponenten auf Basis der Informationen dieser Listen einrichten zu können.

Bei Leittechnikkomponenten, die über eine lokale Firewall verfügen, wird diese aktiviert und nur die benötigten eingehenden Ports freigegeben. Aktuell handelt es sich dabei um die lokalen Steuereinheiten und Touchpanels. Die Firewall-Einstellungen von Tunnelkopfrechnern, Datenbankservern, der VDI, dem Testsystem und den Bedienstationen obliegen aufgrund deren Beistellung dem Auftraggeber.

5.2.10 Programmierlaptops

Programmierlaptops sind nicht anlagenrelevant. Sie sind das Werkzeug der Programmierer*innen und werden hauptsächlich im Firmengebäude betrieben. Bei Inbetriebnahmen muss, gleich wie bei der Fernwartung der Anlagen, die Verbindung über das VPN stattfinden. Daher kommen sie nicht direkt in Kontakt mit der Anlage.

Die Programmierung der Prozessleitsoftware findet im Unternehmen statt. Dafür wird eine virtuelle Maschine am firmeninternen Server aufgesetzt, auf der eine Datenbank und „XAMControl“ installiert wird. Damit besteht die Möglichkeit sich mit der „XAMIDE“, der Entwicklungsumgebung von „XAMControl“, über das Netzwerk darauf zu verbinden.

5.2.11 Betriebssystem

Als Betriebssystem von Tunnelkopfrechner, Datenbankservern, VDI, Testsystem, Bedienstationen, lokalen Steuereinheiten und Touchpanels kommt ein zur Errichtung aktuelles Windows-Betriebssystem zum Einsatz. Bei den vom AG beigestellten Komponenten wird zusätzlich zur Hardware auch das Betriebssystem zur Verfügung gestellt.

Lokale Steuereinheiten und Touchpanels werden auf Betriebssystemebene „gesichert“. Dafür werden folgenden Maßnahmen umgesetzt:

- Parametrierung der lokalen Firewall
- Deaktivierung von Schnittstellen
    - USB
    - Ethernet
- Nicht benötigte Aufgaben werden in der Aufgabenplanung deaktiviert

Das Betriebssystem wird über regelmäßige, manuell angestoßene Updates aktuell gehalten. Diese werden vom WSUS-Server, der vom AG beigestellt wird, bezogen.

5.2.12 Prozessleitsoftware

Im Unternehmen wird „XAMControl“ als Leit- und Visualisierungssoftware eingesetzt. Die Software dient der Entwicklung und dem Betrieb von SCADA- und Prozessleitsystemen. Dazu wird als Basis eine Datenbank benötigt, in der sämtliche Informationen gespeichert werden. Beim Erstellen eines neuen „XAMControl“-Projekts wird eine sogenannte „Solution“ erstellt. Diese bildet das Rahmenwerk für die Datenbank. Das bedeutet, dass jede Tunnelanlage eine eigene Solution abbildet, von der regelmäßige Datenbank-Sicherungen erstellt werden.

Folgende „XAMControl“-Anwendungen sind von Bedeutung:

> **„XAMControlIDE“**: Die *IDE* (Integrated Development Environment) ist die Entwicklungsumgebung von „XAMControl“. Darin wird die benötigte Logik für die Feldkomponenten in entsprechende Klassen implementiert. Zusätzlich werden in den Klassen visuelle Darstellungen der Geräte und deren Zustände, sowie Popups zur Steuerung ergänzt. Diese werden in der Visualisierung eingesetzt. Die Klassen werden in Soft-SPSen instanziiert und diese den entsprechenden Controllern, also lokalen Steuereinheiten, zugewiesen. Die grafischen Komponenten der Klassen werden in die Visualisierungsbilder gesetzt und mit der entsprechenden Instanz, die dargestellt werden soll, verknüpft. Weiters werden in der „XAMControlIDE“ die Clients, also Touchpanels und Bedienstationen konfiguriert, auf welchen die Visualisierung mithilfe des „XAMIrisProxy“-Dienstes automatisch geöffnet werden soll. Zusätzlich findet darauf die Benutzerverwaltung für die gesamte Solution statt.

Diese Möglichkeiten ergeben sich vor allem, wenn sich die IDE mit dem übergeordneten PLC-Dienst des Tukos verbindet, da darauf sämtliche Daten verwaltet werden.

„XAMIris“: Die „XAMIris“ dient der Visualisierung des Leitsystems. Sie stellt die berechtigungsspezifische Steuerung und Überwachung der Tunnelanlagen zur Verfügung. Die anzuzeigenden Prozessbilder werden in der IDE erstellt. Darin befinden sich die grafischen Elemente der Feldkomponenten. Der Aufbau ist gewerkspezifisch, sodass jedes Gewerk in einem eigenen Bild dargestellt wird. Bei der Öffnung der „XAMIris“ mittels der „XAMIrisProxy“ können die anzuzeigenden Bilder limitiert werden, sodass zum Beispiel auf Touchpanels nur die benötigte Örtlichkeit angezeigt wird.

„XAMTraceViewer“: Diese Applikation liefert eine Darstellung über die Laufzeitmeldungen der „XAMControl“-Dienste und -Anwendungen. Zusätzlich können in der Programmlogik erforderliche Ausgaben programmiert werden, um relevante Ereignisse zu dokumentieren oder Debug-Informationen anzuzeigen. Die Meldungen werden mit der aktuellen Systemzeit gesichert.

Zusätzlich zu den Applikationen sind für den aufrechten Betrieb der Solution und des Leitsystems bestimmte Dienste notwendig. Diese werden auf den Komponenten folgendermaßen benötigt:

	Tuko	**LStE**	**TP**	**BST**
XAMPLC	X	X		
XAMAlarmServer	X			
XAMArchiver	X			
XAMIrisProxy			X	X
XAMIEC104Server	X			
XAMIEC104Client	X			
XAMOpcUaIOClient	X			
XAMOpcUaIOServer	X			
XAMSnmp	X	X	X	X
XAMProfibus		X		
XAMModbusTCPClient		X		
XAMUpdateService		X	X	X

Tab. 4: Angewendete „XAMControl“-Dienste (Tuko: Tunnelkopfrechner, LStE: Lokale Steuereinheit, TP: Touchpanel, BST: Bedienstation), Quelle: Eigene Darstellung.

Die „XAMPLC“ ist der Dienst, der für den Datenaustausch und somit das Aufrechterhalten der Solution verantwortlich ist. Der „XAMAlarmServer“ dient der Darstellung der Alarme. Dazu werden sämtliche Variablen, die als Alarm deklariert und aktiv sind, in der Alarm-Zeile ausgegeben und das betroffene Feldgerät in der Visualisierung entsprechend markiert. Für die Aufzeichnung von Trenddaten und historischen Daten wird der „XAMArchiver“ aktiviert.

Diese Informationen werden in die „XAMRuntimeX4“-Datenbank geschrieben. Der „XAMIrisProxy“-Dienst wird für die automatische Initialisierung der „XAMIris“ verwendet. Mithilfe dieses Dienstes werden nur die für den Client freigegebenen Prozessbilder angezeigt. „XAMIEC104Server“ und „XAMOpcUaIOServer“ werden für die Verbindung und den Datenaustausch zur Verkehrsmanagementzentrale verwendet. Je nachdem welches Protokoll im Einsatz ist, wird der entsprechende Dienst verwendet. Die Client-Services dieser Protokolle werden unter anderem für die Anbindung zu Servern von Fremdgewerken, wie Video oder Brand angewendet. „XAMSnmp“ ist dafür verantwortlich, dass die Prozessorauslastung und Arbeitsspeicherbelegung der Hosts mit aktiviertem Dienst über die Logik ausgelesen und zentral angezeigt werden. Der „XAMModbusTCPClient“ wird auf Komponenten aktiviert, an denen IBKs oder anderweitige Geräte mittels Modbus TCP angebunden sind. Werden Geräte mit Profibus angebunden, das sind bei einigen Anlagen IBKs, wird dafür der „XAMProfibus“-Dienst aktiviert. Der „XAMUpdateService“ wird benötigt um „XAMControl“-Updates auf den Client-Komponenten, auf welchen der Dienst aktiviert ist, automatisch auszurollen.

Weiters bietet „XAMControl“ die Möglichkeit Benutzeraccounts über die Domäne abzugleichen. Dadurch werden die komplexen Passwörter bereits im Vorhinein vergeben und so muss auch nur ein Kennwort regelmäßig geändert werden. Damit wird die Offenlegung der Passwörter durch Notieren minimiert. Die Benutzerkonten werden über die Benutzergruppen abgefragt und in „XAMControl“ den gleich benannten Gruppen zugeordnet, wobei die Berechtigungen stufenweise und gruppenspezifisch vergeben werden. Somit bekommt jeder die minimalen Rechte, die benötigt werden: Administratoren IDE-Berechtigungen, Operatoren Steuerungsrechte und temporäre Benutzer*innen eigene Gruppen.

Updates von „XAMControl“ sind nur innerhalb desselben Releases möglich, da bei großen Versions-Sprüngen Inkompatibilitäten auftreten können.

5.2.13 Software

Bei der Verwendung von Software von Drittherstellern wird auf das Minimalprinzip geachtet. Nur die tatsächlich benötigten Applikationen werden verwendet. Weiters wird beachtet, auf welchen Leittechnikkomponenten ein möglicher Schaden durch Schwachstellen in Dritthersteller-Software das geringste Übel wäre.

Die Softwareprodukte werden entsprechend der nachfolgenden Tabelle in die Anlage eingebracht:

	Tuko	**DB-Server**	**VDI**	**LStE**	**TP**	**BST**
Datenbank		O		X		
Datenbank-Administration			O			
IBK-Administration			X	X		
Zählschleifen-Administration			X	X		
Medienkonverter-Administration			X	X		
Schnittstellentreiber				X	X	
Sicherungssoftware				X	X	
Internetbrowser			O			
Zeitsynchronisierungssoftware	X			X	X	
Datenverarbeitung			O			O
O … Beistellung Auftraggeber			X … Beistellung Dürr Austria GmbH			

Tab. 5: Zuordnung der Dritthersteller-Software zu den Komponentenarten (Tuko: Tunnelkopfrechner, DB-Server: Datenbankserver, VDI: Virtuelle Desktopinfrastruktur, LStE: Lokale Steuereinheit, TP: Touchpanel, BST: Bedienstation), Quelle: Eigene Darstellung.

Die mit „O“ markierten Zellen bedeuten eine Beistellung des Auftraggebers, wobei das Patchen dieser Software im Verantwortungsbereich der Dürr Austria GmbH liegt.

Als Datenbank wird der „Microsoft SQL Server“ verwendet. Auf den Datenbankservern kommt die Standard- und auf den lokalen Steuereinheiten die Express-Version zum Einsatz. Die Datenbanken auf den beiden Datenbankservern sind bezüglich der Ausfallsicherheit gespiegelt. Die eingerichtete „XAMControl“-Datenbank-Instanz unterteilt sich in die zwei Datenbanken „XAMControlX4“ und „XAMRuntimeX4“. Beide werden täglich gesichert. Die Datenbankverwaltung findet über das SQL Management Studio auf der VDI statt.

Für die Verwaltung der intelligenten Busklemmen, Zählschleifen und Medienkonverter wird Administrationssoftware benötigt, um diese zu parametrieren oder Fehlercodes auszulesen. Falls die Hardware über die VDI erreichbar ist, wird die Software auch darauf installiert, da Schwachstellen und/oder Schadsoftware darauf den geringsten Einfluss haben. Andernfalls werden diese Softwareprodukte auf den lokalen Steuereinheiten derselben Örtlichkeit installiert.

Für Schnittstellen, wie zum Beispiel die Touch-Funktionalität der Touchpanels oder die Überwachung mittels *SNMP* (Simple Network Management Protocol) der lokalen Steuereinheiten, werden separate Treiber benötigt.

Da Touchpanels und lokale Steuereinheiten von der Dürr Austria GmbH beigestellt werden, befindet sich auf diesen auch eine Sicherungssoftware, um Backups des aktuellen Systemabbildes der Komponenten im Fall eines Ausfalls zur Verfügung zu haben. Mithilfe dieses Programms werden nach Änderungen des Systems Sicherungen erstellt und im Backup-Verzeichnis am Tuko abgelegt.

Für den Datenaustausch über die Datendrehscheibe und das Aufrufen von Webinterfaces von Feldkomponenten wird ein Internetbrowser benötigt. Dabei wird „Microsoft Edge Chromium“ verwendet und mit Windows-Updates aktualisiert.

Die Zeitsynchronisierung ist für die Ereignisaufzeichnung von Relevanz, um Rückschlüsse auf Auffälligkeiten unterschiedlicher Komponenten ziehen zu können. Daher wird eine Software für den Abgleich der Systemzeit der IT/OT-Komponenten mit dem NTP-Server des Auftraggebers verwendet.

Für die Erstellung von Reports, der über einen gewissen Zeitraum aufgezeichneten Trend-Daten von Datenpunkten, wird Excel benötigt. Die Berichte werden im Excel-Dateiformat gespeichert.

5.2.14 Protokolle

Die meisten angewendeten Protokolle wurden bereits bei den „XAMControl“-Diensten erwähnt. Jedoch bleiben noch einige offen, die für die Kommunikation der IT/OT-Komponenten zusätzlich notwendig sind. Hierbei werden nur IP-Protokolle betrachtet. Serielle Schnittstellen werden nicht berücksichtigt.

Dabei wird Modbus TCP ausgehend für die Ansteuerung von intelligenten Busklemmen, Wechselverkehrszeichen und Infotafeln benötigt. SNMP wird bidirektional auf den Tukos, die diese Daten auswerten, sowie den lokalen Steuereinheiten und Touchpanels, die ihren Status übermitteln, freigegeben. Dieses Protokoll wird ebenso für die Überwachung der unterbrechungsfreien Stromversorgung benötigt. Für den Abgleich der Systemzeit wird NTP benötigt. Dieses Protokoll wird von der Dürr Austria GmbH auf den Tunnelkopfrechnern, lokalen Steuereinheiten und Touchpanels verwendet. Der Zeitabgleich auf den übrigen Komponenten obliegt dem Auftraggeber. Sollte eine Querkommunikation zwischen den lokalen Steuereinheiten und Tunnelkopfrechnern für den Datenabgleich benötigt werden, wird dafür OPC UA verwendet. Dieses Protokoll wird ebenso für die Verbindung zur Verkehrsmanagementzentrale und zu den Servern für Brand- oder Videosysteme eingesetzt. Für diese Anwendungsbereiche wird mitunter auch IEC 60870-5-104 zur Anwendung gebracht. Weiters kommen auch proprietäre Protokolle für die Zählschleifen zum Einsatz. Für das Aufrufen von Webinterfaces von Feldkomponenten wird ausgehend *HTTP* (Hypertext Transfer Protocol) verwendet, da diese die verschlüsselte Version *HTTPS* (Hypertext Transfer Protocol Secure) häufig nicht unterstützen.

Für die Verwaltung der Datenbank und den Datenabgleich zwischen den beiden gespiegelten Datenbanken auf den Datenbankservern werden SQL-Protokolle für die SQL-Spiegelung, den SQL-Browser und die SQL-Server-Instanz benötigt. „XAMControl“-Protokolle sind ebenfalls proprietär. Sie umfassen die Abwicklung der Redundanz, der Kommunikation, sowie der Treiber. Für den Transfer von Datenbank- und Imagesicherungen auf das Backup-Verzeichnis wird das Protokoll Server Message Block (*SMB*) eingesetzt.

Die verwendeten Protokolle werden anlagenspezifisch dokumentiert, um die Parametrierung der lokalen Firewalls daran anzupassen.

5.3 Angewendete Security-Maßnahmen

Viele der von der Dürr Austria GmbH angewendeten Security-Maßnahmen wurden bereits erwähnt. In diesem Kapitel erfolgt eine strukturelle Darstellung der Maßnahmen.

Führen von Asset-Listen

Es werden Asset-Listen geführt, die sämtliche IP-Komponenten beinhalten. Darin sind Hostnamen, Gerätetypen, Seriennummern, Standorte, Ortstypen und Funktion der Assets verzeichnet. Zusätzlich liefern die Listen Informationen über installierte Software und Software-Versionen, deren Hersteller, sowie Daten der letzten Patches.

Datensicherung und Wiederherstellung

Die Datensicherung und Wiederherstellung ist für den Fall von unvorhersehbaren Ausfällen oder Defekten von Komponenten relevant. Daher werden die Häufigkeit und Art, sowie der Ablageort der Image- und Datenbank-Sicherungen definiert. Dazu werden Wiederherstellungstests durchgeführt um sicherzustellen, dass die Backups voll funktionsfähig sind.

Desaster-Recovery

Desaster-Recovery beschreibt die Aktionen, die nach einem unvorhersehbaren Ereignis getroffen werden. Darin wird definiert, wie lange die Ausfallsspanne maximal betragen darf und wie unter anderem der Tausch von Komponenten, oder das Neu-Aufsetzen und Backup-Einspielen mit entsprechenden Tests durchgeführt werden.

Malwareschutz

Die Verwendung einer Malwareschutz-Software für lokale Steuereinheiten und Touchpanels wurde geprüft. Es wird jedoch davon abgesehen, um die Performance der Komponenten und somit die Verfügbarkeit nicht einzuschränken.

Logging

Logging beschreibt die Ereignis- und Aktionsaufzeichnung bei einer anlagenweiten, gleichbleibenden Systemzeit. Das bezieht sich vor allem auf die Windows-Ereignisaufzeichnung und die „XAMControl“-Journalaufzeichnungen.

Patch Management

Die Software wird einem halbjährlichen Patch-Prozess unterzogen. Sofern kritische Schwachstellen oder Sicherheitslücken bekannt werden, wird die Software gepatcht, oder andernfalls alternative Lösungen angewendet.

Härtung

Härtung bedeutet die Erhöhung der Widerstandsfähigkeit von Assets. Die lokalen Steuereinheiten und Touchpanels werden vor der Auslieferung mit den nachfolgend beschriebenen Maßnahmen gehärtet:

Passwortsicherung

Überall auf Server- und Steuerungsebene, wo eine Passwortsicherung möglich ist, werden komplexe Passwörter mit Mindestlänge vergeben. Diese werden halbjährlich geändert.

BIOS- und Datenbank-Passwörter werden einmalig komplex vergeben. Eine Änderung findet nur statt, wenn sie kompromittiert werden.

Minimalprinzip

Bei der Errichtung der Systeme wird auf das Minimalprinzip geachtet, daher werden nicht benötigte Ethernet- und sämtliche USB-Schnittstellen auf Betriebssystemebene deaktiviert. Die USB-Schnittstellen werden zusätzlich im BIOS blockiert.

Dasselbe Prinzip gilt für die Software. Es wird auf jeder Komponente nur das Mindestmaß an benötigten Programmen für den stabilen Betrieb der Tunnelanlage installiert.

Lokale Firewall

Die lokalen Firewalls werden auf den lokalen Steuereinheiten und Touchpanels entsprechend der benötigten Protokolle und Ports aktiviert, konfiguriert und für jede Komponente dokumentiert.

Berechtigungen

Die Berechtigungen werden anhand der Anbindung an die Domäne gruppenspezifisch vergeben. Die Rechte der Betriebssystem-Benutzerkonten werden dadurch vom Auftraggeber verteilt. Die Berechtigungen in „XAMControl“ werden ebenfalls gruppenspezifisch vergeben, wobei ein Abgleich der Benutzergruppen über die Active Directory stattfindet. Dadurch werden neu erstellte AD-Benutzeraccounts ebenfalls in „XAMControl“ angelegt und mit den entsprechenden Berechtigungen versehen, sowie gelöschte Benutzeraccounts automatisch deaktiviert.

Schwachstellenmanagement

Das Schwachstellenmanagement wird mit einem vom Auftraggeber beigestellten Tool durchgeführt. Dieses bewertet die Schwachstellen nach ihrer Kritikalität. Die Ergebnisse sind maßgeblich für das Patch Management. Dafür wird die entsprechende Client-Software auf den lokalen Steuereinheiten und Touchpanels installiert und diese in die Server-Lösung integriert. Bei Inkompatibilitäten mit dem Tool wird eine anlagenweite abgeschwächte und manuelle Analyse durchgeführt.

Mit der Durchführung der halbjährlichen IT-Betriebsleistungen werden die Einstellungen überprüft, die aufgrund der Patches geändert werden könnten. Darunter fallen zum Beispiel die Firewall-Regeln.

Bei den IT-Betriebsleistungen sind folgende Aspekte von Relevanz und müssen angepasst sowie auf Aktualität geprüft werden:

	Tuko	DB-Server	VDI	LStE	TP	BST
Hardware				X	X	
Windows	X	X	X	X	X	X
XAMControl	X		X	X	X	X
Datenbank		X		X		
Drittherstellersoftware	X	X	X	X	X	X
Firewall				X	X	

Tab. 6: Relevante Teilbereiche der Komponenten (Tuko: Tunnelkopfrechner, DB-Server: Datenbankserver, VDI: Virtuelle Desktopinfrastruktur, LStE: Lokale Steuereinheit, TP: Touchpanel, BST: Bedienstation), Quelle: Eigene Darstellung.

Die Tabelle liefert zusätzlich einen Überblick, welche Teilbereiche von der Dürr Austria GmbH, auf welchen Komponenten eingerichtet werden. Bei den Tunnelkopfrechnern und Datenbankservern treffen diese Informationen ebenso auf das Testsystem zu.

5.4 Abgrenzung von OT und IT

Die zuvor beschriebenen IT/OT-Komponenten werden auf Basis der Tab. 1 in der nachfolgenden Tabelle der IT und der OT zugeordnet, um einen Überblick für die weiteren Vorgehensweisen zu schaffen:

	IT	OT
Hardware	Switches HCI-Cluster Bedienstationen Programmierlaptops	Intelligente Busklemme Feldkomponenten
	Lokale Steuereinheiten Touchpanels	
Software	Windows Zeitsynchronisierungssoftware Administrationssoftware XAMControl Virtuelle Maschinen	Prozessleitsoftware
Daten	Betriebssystemereignisse Logs	Trends Journal Anlagenbuch

Tab. 7: Zuordnung der Assets zu Information Technology (IT) und Operational Technology (OT) (HCI: Hyperconverged Infrastructure), Quelle: Eigene Darstellung.

Tab. 7 zeigt klar auf, dass in den Tunnelanlagen IT- mit OT-Systemen stark vermischt sind. Eine konkrete Zuordnung kann in anderen Industriebereichen zutreffend sein, bei Tunnelsteuerungssystemen ist sie aber nur begrenzt möglich. Werden Hardware, Software und Daten getrennt voneinander betrachtet, ist eine eindeutige Zuteilung, abgesehen von lokalen Steuereinheiten und Touchpanels, möglich. Das Gesamtsystem eines Gerätes kann keinem Bereich definitiv zugeordnet werden, da auf IT-Hardware OT-Software installiert wird. Lokale Steuereinheiten und Touchpanels können nicht eindeutig zugeordnet werden, da sie den rauen Umgebungsbedingungen der Industrie angepasst werden, es sich dabei im Wesentlichen aber um IT-Hardware handelt. Bei der Prozessleitsoftware handelt es sich in diesem Kontext um die anwendungsfallspezifische Logik, die in „XAMControl“ entwickelt wird, um die Tunnelanlagen zu steuern. Die OT-Daten „Trends“, „Journal“ und „Anlagenbuch“ sind Teile der „XAMControl“-Applikation, um Wartungstickets, Ereignisse und Wertänderungen einzusehen. Die „Logs“, die in den IT-Daten vermerkt sind, sind Teil der Datenbanken.

Beim Einsatz von IT-Komponenten in der OT muss darauf geachtet werden, dass sämtliche nicht benötigte Plugins und Features, deaktiviert sind. Zusätzlich müssen die Sicherheitsvorgaben der beiden Sparten, unter Berücksichtigung der wesentlichen Funktionen und ständigen Verfügbarkeit, bestmöglich angewendet werden.

Im Wesentlichen sind Tunnelanlagen große OT-Systeme mit einem abgekapselten OT-Netzwerk, in denen IT-Assets eingesetzt werden. Die Anforderungen an die IT-Komponenten sind daher dieselben wie an jene der OT. Da die Assets nicht eindeutig zur IT oder OT zugeordnet werden können, treffen die Begriffe IT-Komponenten und OT-Komponenten nicht zu. Im Folgenden wird das Gesamtsystem von Tunnelkopfrechnern, lokalen Steuereinheiten, Touchpanels oder Bedienstationen als IT/OT-Systeme bezeichnet.

Die IT/OT-Konvergenz ist in Bezug auf die Assets stark ausgeprägt. Auf das Netzwerk bezogen herrscht eine strikte Trennung von dem OT-Tunnelnetzwerk und dem IT-Unternehmensnetzwerk. Da eine Abgrenzung der Systeme in jeweils einen Bereich nicht möglich ist, müssen IT und OT gesamtheitlich betrachtet und die OT-Security auch auf die IT-Komponenten angewendet werden.

5.5 Angriffsmöglichkeiten

In diesem Abschnitt werden die Angriffsmöglichkeiten erörtert. Das bedeutet, dass sowohl die potenziellen Angriffsarten, sowie Angreifer*innen evaluiert werden, um ein Bewusstsein zu schaffen, wovor der Schutz besonders wichtig ist und worauf Wert gelegt werden muss.

Mögliche Arten von Angriffen, die mit großer Wahrscheinlichkeit passieren können, sind:

- **Network Hacking**
  - **DDoS**

    Sollte es gelingen auf eine der IT/OT-Komponenten Zugriff zu erlangen, wird eine DDoS-Attacke auf das gesamte Netzwerk möglich. Es sind zwar nur die benötigten Ports der lokalen Firewalls freigegeben, es ist aber trotzdem wahrscheinlich, dass einer dieser Ports herausgefunden und missbraucht werden kann.

  - **Eavesdropping**
    Da teilweise unverschlüsselte Kommunikation zur Feldebene stattfindet, kann dieser gelauscht werden. Zu diesem Zweck müsste zuerst der Zugriff geschaffen werden. Sensible Daten werden auf der Feldebene zwar nicht kommuniziert, eine Manipulation der Daten wäre aber fatal.

- **Malware, Viren**
  Durch den Download von infizierten Patches für Dritthersteller-Software von unsicheren Websites könnten Malware und Viren in Tunnelanlagen unbeabsichtigt eingebracht werden.
- **Social Engineering**
  Mit der Erteilung von Berechtigungen für Tunnelanlagen an „falsche“ Personen, wäre ein solcher Angriff möglich. Die Meldung der benötigten Benutzer*innen wird vom Auftragnehmer auf einer Vertrauensbasis an den Auftraggeber übermittelt. Da beidseitig davon ausgegangen, dass die Daten korrekt sind, könnten solche Angriffe beide Parteien betreffen.
- **Angriffe von innen**
  Gelangweilte Operatoren, oder Angestellte des Betriebs, welche die Systemgrenzen austesten, oder denken, dass die Handlungen keine Auswirkungen haben, sind die wahrscheinlichste Ursache eines Angriffs von innen. Administratoren mit bösartigen Absichten sind nicht auszuschließen.

Im Gegensatz zu den vorhin beschriebenen, wahrscheinlichen Angriffsarten sind die Folgenden mögliche, aber unwahrscheinliche, Szenarien:

- **Gestohlene/Verlorene Smartphones oder Notebooks**
  Da eine Zwei-Faktor-Authentifizierung gefordert ist, stellen verlorene oder gestohlene Smartphones oder Notebooks keine extreme Situation dar, für welche gesonderte Maßnahmen getroffen werden müssen. Zusätzlich sind Smartphones und Notebooks passwort- oder biometrisch-geschützt, wodurch ein Zugriff weiter erschwert wird.
- **Zugriff auf Firmengeräte außerhalb des Unternehmens**
  Auf Firmengeräte kann außerhalb des Unternehmens nur mittels VPN zugegriffen werden. Das Gleiche gilt für Verbindungen zu Tunnelanlagen.
- **Manipulierte Hardware**
  Ein Angriff mit manipulierter Hardware ist unwahrscheinlich, da sämtliche Räume und Örtlichkeiten der Tunnelanlagen versperrt und mit einem Zonenkonzept versehen sind. Die Programmierlaptops könnten manipuliert werden, diese haben aber keine Auswirkung auf die Tunnelanlage, da damit keine direkte Verbindung hergestellt wird.
- **Angriffe auf die Cloud**
  Eine Cloud wird per se nicht eingesetzt, daher sind Angriffe darauf nicht möglich. Lediglich die Datendrehscheibe beinhaltet Informationen im Internet. Darauf befinden sich aber keine relevanten Daten. Diese wird rein für den kurzfristigen Datenaustausch zwischen Anlage und Unternehmen genutzt.

- **Phishing**
  Sollte das Passwort für die Fernverbindungsplattform „gephisht“ werden, wird immer noch der zweite Faktor für die Authentifizierung benötigt. Für den Zugriff auf die Tunnelkomponenten muss zuerst immer die Verbindung über das VPN und die Fernverbindungsplattform geschaffen werden. Daher hat das Bekanntwerden des Passworts oder der Passwörter keine große Auswirkung. Bei Bekanntwerden eines Phishing-Angriffs sollten die Kennwörter dennoch geändert werden.
- **Physischer Zugang**
  Ein unautorisierter physischer Zugang ist unwahrscheinlich, da die Örtlichkeiten dem Zonenkonzept des Auftraggebers unterliegen. Sämtliche Räume sind versperrt und die Autorisierung erfolgt erst durch Bekanntgabe des benötigten Zugangs. Es werden dabei nur die gebrauchten Zonen freigeschalten. Für Außenstehende ist ein Zugang somit beinahe unmöglich.
- **Backdoors**
  Mit Backdoors ist kaum zu rechnen, da es sich um abgekapselte Systeme handelt, die aus dem Internet nicht erreicht werden können.

Hinter den Angriffen stecken in der Regel Personen, die bestimmte Absichten verfolgen. Mögliche Profile sind:

- Erfahrene **Hacker*innen** mit dem Hintergrund Erpressungsgeld zu verlangen.
- **Systemadministrator*innen** mit der Absicht dem Unternehmen zu schaden. Als Motiv könnte unter anderem Rache im Vordergrund stehen.
- **Bediener*innen** bzw. **Operator*innen** aus Langeweile oder weil diese etwas ohne böse Absichten testen.
- Der Begriff **Lieferanten** muss in diesem Kontext abgegrenzt werden, da die Dürr Austria GmbH auch die Rolle des Lieferanten übernimmt und somit eigene Komponenten hacken oder Backdoors einbauen könnte. Daher führt der Auftraggeber einen Sicherheitscheck zumindest auf Cluster-Ebene durch.
- **Sicherheitsforscher*innen** die unter anderem vom Auftraggeber beauftragt werden, um die Sicherheit der Systeme zu prüfen. Dies findet mit der Durchführung von Penetrationstests statt.
- **Terrororganisationen** oder **Cyberangriffe**, um möglichst großen Schaden anzurichten und die Infrastruktur lahmzulegen.

Zu den unwahrscheinlichen Arten von Angreifer*innen zählen die folgend beschriebenen:

- Für **Script Kiddies** ist es nicht so einfach auf die Tunnelanlagen zu stoßen. Dazu müsste eine gewisse Motivation und Wissen vorhanden sein.
- **Staatlich gelenktes Hacking** ist ebenfalls unwahrscheinlich, da Tunnelanlagen keine Ertragsausfälle, abgesehen von der Tunnelmaut von ausgewählten Anlagen, verursachen und somit keine bedeutende Wirtschaftsschädigung hervorrufen.
- Bei **Mitbewerbern** der Dürr Austria GmbH und des Auftraggebers ist kein Motiv ersichtlich, um Angriffe durchzuführen oder Anlagen stillzulegen.

6 ANWENDUNG DER IEC 62443

Für die Anwendung der IEC 62443 ist zunächst wichtig zu wissen, welche Rolle die Dürr Austria GmbH dabei einnimmt, um die entsprechenden Teile der Normenreihe anwenden zu können. Kurzgefasst umfassen die Tätigkeiten

- die Entwicklung der Prozessleitsoftware,
- das Aufsetzen der IT/OT-Systeme,
- die Inbetriebnahme der Prozessleitsoftware und IT/OT-Systeme, sowie
- deren Wartung und Instandhaltung.

Mit der Entwicklung der Prozessleitsoftware in „XAMControl“ wird die Rolle des Produktlieferanten eingenommen. Die Dürr Austria GmbH ist aber auch Dienstleister. Das begründet sich durch die Implementierung der Prozessleitsoftware und der Drittherstellersoftware auf den beigestellten und zugekauften IT/OT-Systemen, sowie das Aufsetzen dieser Systeme, um danach eine gesamtheitliche Integration in die Anlage durchzuführen. Zusätzlich bietet das Unternehmen die Dienstleistung der Wartung und Instandhaltung an. Die bestehenden Informationssicherheitskonzepte vereinen dadurch die Blickwinkel dieser beiden Rollen.

Die Grundsätze der IEC 62443 werden im Folgenden evaluiert, um eine Basis für die Erarbeitung der zutreffenden Normen zu schaffen.

Zonen und Conduits

Das Prinzip der Zonen und Conduits wird vom Auftraggeber umgesetzt. Dieser hat bereits ein entsprechendes Zonenkonzept entwickelt und in Anwendung. Die Zonen werden aufgrund von Sicherheitsebenen unterteilt. Räume, in denen sich die Tunnelkopfrechner befinden, haben sehr strenge Zutrittsvorschriften. Beinahe gleich relevant sind Räume oder Verteilerschränke mit lokalen Steuereinheiten und Touchpanels. Weniger relevant sind einfache Verteilerschränke, wobei selbst diese versperrt und in verschlossenen Räumen verbaut sind. Somit wird funktional und nach Sicherheitsrelevanz unterschieden. Die Conduits sind dabei das Netzwerk, welches die Zonen miteinander verbindet. Dieses wird mit den lokalen Firewalls seitens Dürr Austria GmbH bestmöglich geschützt.

Secure by Design

Secure by Design wird beim Einrichten der IT/OT-Komponenten bereits zu Beginn berücksichtigt. Die Sicherheitsvorgaben werden dabei vor der Auslieferung parametriert.

Minimalprinzip

Das Minimalprinzip wird in Bezug auf Software, Schnittstellen und Netzwerkprotokolle angewendet.

Wesentliche Funktionen

Die wesentlichen Funktionen müssen immer gegeben sein und dürfen durch Security-Maßnahmen nicht eingeschränkt werden. Zu den wesentlichen Funktionen von Tunnelsteuerungssystemen gehören:

- Steuerung der Leittechnikkomponenten
- Visualisierung des Leitsystems
- Datenaustausch
- Standard-Benutzerkonto für das automatische Öffnen der Visualisierung
- Anmeldung auf IT/OT-Systeme
- Systemauslastung innerhalb von Toleranzgrenzen

Security-Levels und Reifegrade

Da es vom Auftraggeber keine Vorgaben für zu erreichende Security-Levels (SL-T) gibt, wird die Norm als Hilfsmittel zur Einschätzung der bisherigen Sicherheitslevels und Reifegrade, sowie für die Verbesserung und Erweiterung von Security-Maßnahmen angewendet.

Sollten diesbezüglich konkrete Vorgaben des Auftraggebers bekannt werden, besteht eine Grundlage der Security-Levels und Reifegrade, auf die aufgebaut werden kann.

Defense in Depth

Durch die Umsetzung zusätzlicher Maßnahmen soll die Defense-in-Depth-Strategie weiterentwickelt und verbessert werden.

Folgende Normen der Normenreihe werden im Weiteren genauer untersucht und die Reifegrade und Security-Levels zugeordnet, da sie für Produktlieferanten und Dienstleister ausgelegt sind. Gleichzeitig wird aus diesen das Verbesserungspotential evaluiert:

- Teil 2-4: Security Program Requirements for IACS Service Providers
  (Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme)
- Teil 3-3: System Security Requirements and Security Levels
  (Systemanforderung zur IT-Sicherheit und Security-Level)
- Teil 4-1: Product Security Development Lifecycle Requirements
  (Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung)
- Teil 4-2: Technical Security Requirements for IACS Components
  (Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme)

6.1 Teil 2-4: Security Program Requirements for IACS Service Providers

Dieser Teil stellt Anforderungen an IT-Sicherheitsprogramme für Dienstleister und behandelt das Reifegradmodell. Dabei werden Prozesse und keine technischen Aspekte bewertet. Die Norm ist generisch gehalten und kann auf entsprechende Profile zugeschnitten werden. Daher treffen für die Dürr Austria GmbH nicht alle Anforderungen zu.

Die Norm liefert einen Anhang mit einer Auflistung von 124 Anforderungen. Diese sind anhand der dargestellten Parameter in der nachfolgenden Tabelle beschrieben:

Anford.-ID	**BR/RE**	**Bereich**	**Oberbegriff**	**Unterbegriff**	**Doku?**	**Beschreibung der Anforderung**	**Begründung**

Tab. 8: Aufbau der Anforderungen aus der IEC 62443-2-4, Quelle: OVE EN IEC 62443-2-4 (2020), S. 25 ff (leicht modifiziert).

Die Anforderungs-ID ist die jeweilige Kurzbezeichnung. Die nächste Spalte BR/RE zeigt, ob es sich um eine Basisanforderung oder um eine weitergehende Anforderung handelt. Mithilfe der Spalte Bereich werden die Anforderungen direkt zu Kategorien wie zum Beispiel „Schutz vor Schadsoftware“ oder „Mitarbeiter“ zugeordnet. Durch den Oberbegriff werden die Bereiche unterteilt, wobei diese Begriffe sich wiederholen können. Dazu zählen unter anderem „Passwörter“ oder „Sicherheitslücken“. In der Spalte Unterbegriff werden die technischen Elemente innerhalb des Oberbegriffs, wie unter anderem die „Änderung“ oder „Zusammensetzung“ von Passwörtern, definiert. Ob der Prozess dokumentiert sein muss, gibt die Spalte Doku? an. Diese enthält ein „Ja“ für eine geforderte Dokumentation und andernfalls ein „Nein“. Die „Beschreibung der Anforderung“ enthält eine textuelle Erklärung der Anforderung, die mit der Begründung mit zusätzlichen Informationen ergänzt wird.[133]

[133] Vgl. OVE EN IEC 62443-2-4 (2020), S. 18 – 24.

6.1.1 Anwendung

Auf die Anforderungen der Norm wird einzeln eingegangen, indem die bisherige Umsetzung beschrieben und das Verbesserungspotential, das sich daraus ergibt, ergänzt wird. Zusätzlich wird der abgeschätzte Reifegrad ergänzt. Ebenso wird festgehalten, welche Punkte in der Verantwortung des Auftraggebers liegen und daher nicht von der Dürr Austria GmbH berücksichtigt werden.

Die Norm liefert ein Excel-Template, in dem die Anforderungen aufgelistet sind. Dieses wird als Basis für die Ausarbeitung verwendet und mit den Spalten Anmerkung zur Umsetzung und Reifegrad ergänzt.

Dazu ist eine Anforderung aus dem Teil 2-4 dargestellt, um ein Beispiel darzustellen:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?
SP.01.01	RE(1)	Mitarbeiter	Unterwei-sung	IT-Sicherheits-anforderungen – IEC 62443-2-4	Nein

Beschreibung der Anforderung	Begründung
Der Dienstleister muss die Fähigkeit besitzen, sicherzustellen, dass er ausschließlich Personal des Unterauftragnehmers oder des Beraters „Automatisierungslösungs“-bezogene Tätigkeiten zuweist, das in den in dieser Spezifikation geforderten Verantwortlichkeiten, Leitlinien und Vorgehensweisen unterwiesen wurde und diese erfüllt.	Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser sicherheitsbewusstes Personal des Unterauftragnehmers, sicherheitsbewusste Berater und Vertreter zur Arbeit an der „Automatisierungslösung“ bereitstellen kann. Siehe ISO/IEC 27036-3 für weitergehende organisatorische Anforderungen an die Lieferkette.

Tab. 9: Anforderung aus der IEC 62443-2-4 (SP: IT-Sicherheitsprogramm, BR: Basisanforderung, RE: Weitergehende Anforderung), Quelle: OVE EN IEC 62443-2-4 (2020), S. 26 (leicht modifiziert).

Da Unterauftragnehmer das bestehende Informationssicherheitskonzept vorab bekommen und sich an die darin beschriebenen Maßnahmen halten müssen, werden sie damit unterwiesen. Der Nachweis besteht in der nach der Inbetriebnahme erstellten Informationssicherheitsdokumentation, welche die erfüllten Maßnahmen beschreibt. Der Reifegrad wird mit „3“ bewertet, da es sich um einen wiederholbar nachweisbaren Prozess handelt, welcher keiner ständigen Verbesserung unterliegt.

Diese Erkenntnisse werden folgendermaßen dokumentiert:

Anmerkung zur Umsetzung	Reifegrad
Unterauftragnehmer müssen sich an vorgegebenes ISMS-Konzept halten	3

Tab. 10: Evaluierung des Reifegrads einer Anforderung aus der IEC 62443-2-4 (ISMS: Informationssicherheitsmanagementsystem), Quelle: Eigene Darstellung.

Nach diesem Schema werden die 124 Anforderungen bearbeitet und evaluiert.

6.1.2 Verbesserungspotential

Durch die Evaluierung der Norm ergeben sich die nachfolgend beschriebenen Verbesserungsmöglichkeiten der Prozesse und Dokumentationen:

- Überprüfung des Informationssicherheitskonzeptes von Dritten, um weitere Möglichkeiten oder Fehlerquellen zu erkennen.
- Awareness-Schulung der Mitarbeitenden, um die Notwendigkeit von Security-Maßnahmen sichtbar zu machen.
- Verschlüsselte Ablage des Passworts des Backup-Users, welcher für die Übertragung der Backups in das Backup-Verzeichnis verwendet wird.
- Verschlüsselte Ablage der lokalen Passwortlisten am Firmenserver.
- Abklärung der internen Verantwortung für die An- und Abmeldung von Benutzer*innen beim Auftraggeber.
- Durchführung von Penetrationstests bei lokalen Steuereinheiten, Touchpanels und „XAMControl“.
- Grafikkarten-Schnittstellen von lokalen Steuereinheiten und Touchpanels sperren, sofern dadurch der Zugriff bei Ausfällen der Remote-Verbindungen weiterhin möglich ist.
- Limitierung der Zugriffe auf Verzeichnisse von lokalen Steuereinheiten und Touchpanels nach Benutzergruppen.
- Erweiterung der Unterscheidung von Berechtigungen der Benutzergruppen in Windows bei lokalen Steuereinheiten und Touchpanels.
- Beschreibung des Prozesses, dass Dateneingaben validiert, von autorisierten Benutzer*innen und nur innerhalb der Anlage geändert werden.
- Passwortschutz von Backups oder Limitierung der Benutzergruppen mit Zugriff auf Backup-Ordner.
- Anwendung von kryptografischen Maßnahmen.
- Ergänzung von USB- und Ethernet-Schnittstellen im Kommunikationsschema.
- Erstellung der Prozessdefinition für die Prüfung auf IT-Sicherheitsvorfälle und der weiteren Vorgehensweise während den IT-Betriebsleistungen.
- Definition und Parametrierung der Protokollierung von Windows An- und Abmeldungen für eine bestimmte Anzahl von Tagen.
- Überprüfung und Definition von Belastungsproben im Sinne von Ereignisstürmen auf lokale Steuereinheiten, Touchpanels und gezielt „XAMControl“.
- Regelmäßige Überprüfung auf entbehrliche Benutzerkonten in „XAMControl“.
- Erstellung einer Beschreibung für den Umgang mit mobilen Datenträgern (unter anderem USB-Sticks und externe Festplatten) im Anlagenumfeld.
- Erstellung von Installationsanleitungen für Patches.
- Erstellung einer konkreten Anleitung für den Backup-&-Restore-Prozess.
- Beschreibung von der Erstellung und der Erkennung von erfolgreichen Backups.

Die beschriebenen Verbesserungsmöglichkeiten bieten Anhaltspunkte, um über Optimierungen zu diskutieren.

6.2 Teil 3-3: System Security Requirements and Security Levels

Der Teil 3-3 der IEC 62443 behandelt die Sicherheitsanforderungen und Security-Levels der industriellen Steuerungssysteme. Die Systemanforderungen und die weitergehenden Anforderungen sind hierbei den entsprechenden grundlegenden Anforderungen der Norm zugeordnet. Dieser Teil der Normenreihe ist für Systemintegratoren, Produktlieferanten und Dienstleister ausgelegt.[134]

Da vom Auftraggeber keine separaten Anforderungen der IEC 62443 vorgegeben werden, wird der Standardkatalog angewendet.

Die Norm gibt die erreichbaren Security-Levels (SL-C) vor. Die vorgegebenen SL-C entsprechen in diesem Fall den erreichten Security-Levels (SL-A), da die möglichen überprüften Maßnahmen der Anforderungen durchführbar und gleichzeitig umgesetzt sind. Anhand der erreichbaren Security-Levels ergibt sich der SL-C-Vektor, der die Security-Levels der grundlegenden Anforderungen darstellt.

Jede der 51 Systemanforderungen definiert die Ansprüche für das Erreichen der einzelnen Security-Levels. Dabei werden die Prinzipien der wesentlichen Funktionen, Ausgleichsmaßnahmen und minimal erforderlichen Rechte berücksichtigt.

6.2.1 Anwendung

Der Teil wird auf das beigestellte Automatisierungssystem, welches integriert wird, gesamtheitlich angewendet. Dazu gehören lokale Steuereinheiten, Touchpanels, „XAMControl“ und Feldgeräte. Dabei werden die Anforderungen der Norm bearbeitet und die Security-Levels evaluiert. Diese werden folgendermaßen vorgegeben:

SL-C(IAC, Automatisierungssystem) 1: SR 1.1;
SL-C(IAC, Automatisierungssystem) 2: SR 1.1 (1);
SL-C(IAC, Automatisierungssystem) 3: SR 1.1 (1) (2);
SL-C(IAC, Automatisierungssystem) 4: SR 1.1 (1) (2) (3).

Abb. 16: Vorgegebene Security-Levels einer Anforderung aus der IEC 62443-3-3 (SL-C: Erreichbarer Security-Level, IAC: Identifizierung und Authentifizierung, SR: Systemanforderung), Quelle: OVE EN IEC 62443-3-3 (2020), S. 30.

Die Abbildung zeigt, dass für die Stufe eins der Systemanforderung (SR) 1.1 die Erfüllung dieser Anforderung wesentlich ist. Diese ist textuell in der Norm beschrieben. Für die Erreichung des zweiten Levels muss die weitergehende Anforderung eins, für das dritte die weitergehenden Anforderungen eins und zwei und für das vierte die weitergehenden Anforderungen eins, zwei und drei erfüllt werden. Die weitergehenden Anforderungen sind innerhalb der Klammern vermerkt.

Auf dieser Grundlage werden sämtliche Anforderungen in einer Excel-Tabelle zusammengefasst, bearbeitet und die entsprechenden Anmerkungen ergänzt.

[134] Vgl. OVE EN IEC 62443-3-3 (2020), S. 14.

Die nachfolgende Tabelle zeigt die Ausarbeitung der „SR 1.1 – Identifizierung und Authentifizierung von Nutzer*innen“:

Grundlegende Anforderung	**Anforderung**	**Weitergehende Anforderung**	**SL-C**	**Anmerkung**
FR 1 – Identifizierung und Authentifizierung	SR 1.1 – Identifizierung und Authentifizierung von Nutzer*innen		2	Benutzer*innen können eindeutig authentifiziert werden
FR 1 – Identifizierung und Authentifizierung	SR 1.1 – Identifizierung und Authentifizierung von Nutzer*innen	SR 1.1 RE 1 – Eindeutige Identifizierung und Authentifizierung	-	ja
FR 1 – Identifizierung und Authentifizierung	SR 1.1 – Identifizierung und Authentifizierung von Nutzer*innen	SR 1.1 RE 2 – Multifaktor-Authentifizierung für nicht vertrauenswürdige Netze	-	XAMControl bietet keine Multifaktor-Authentifizierung
FR 1 – Identifizierung und Authentifizierung	SR 1.1 – Identifizierung und Authentifizierung von Nutzer*innen	SR 1.1 RE 3 – Multifaktor-Authentifizierung für alle Netze	-	XAMControl bietet keine Multifaktor-Authentifizierung

Tab. 11: Zuordnung des Security-Levels zu einer Anforderung aus der IEC 62443-3-3 (FR: Grundlegende Anforderung, SR: Systemanforderung, RE: Weitergehende Anforderung, SL-C: Erreichbarer Security-Level), Quelle: Eigene Darstellung.

Die grundlegende Anforderung ist in der ersten Spalte beschrieben. Danach befinden sich die Anforderung und die weitergehende Anforderung. Die Beschreibung der Anforderungen wird direkt aus der Norm entnommen und nicht separat in die Tabelle eingefügt. Jeder Zeile wird eine Anmerkung beigefügt, um die bisherige Umsetzung und/oder mögliches Verbesserungspotential zu ergänzen. Anhand dieser Evaluierung findet die Zuordnung der Security-Levels (SL-C) zu den Systemanforderung statt.

Im Fall der darüber ausgearbeiteten Anforderung ist der SL-C 2, da die weitergehende Anforderung 1 erfüllt wird und die weitergehenden Anforderungen 2 und 3 nicht umgesetzt werden können. Das entspricht der Auflistung aus Abb. 16, bzw. der Norm. Die weitergehenden Anforderungen bekommen keinen Security-Level zugeordnet, da diese ein Teil der übergeordneten Systemanforderung sind.

Werden sämtliche Anforderungen ausgearbeitet, ergibt sich der SL-C Vektor der grundlegenden Anforderungen. Für die Automatisierungssysteme in der Tunnelumgebung ist dieser folgendermaßen:

SL-C(Automatisierungssystem) = { 0 0 1 0 / 1 0 }

Im Vektorformat scheinen die Security-Levels sehr niedrig. Das resultiert daher, dass immer der niedrigste Wert der gesamten Anforderungen innerhalb der grundlegenden Anforderung zur Bewertung herangezogen wird. Würden die durchschnittlichen Levels betrachtet werden, wäre der Wert weitaus höher. Die grundlegende Anforderung „FR 5 – Eingeschränkter Datenfluss“ liegt in der Verantwortung des Auftraggebers und wird daher nicht bewertet.

6.2.2 Verbesserungspotential

Aufgrund der Evaluierung der Systemanforderungen ergeben sich nachfolgend beschriebene Aspekte zur Verbesserung und Überprüfung von Möglichkeiten der OT-Security:

- Überprüfung, ob Möglichkeiten für eine eindeutige Identifizierung und Authentifizierung von Softwareprozessen und Geräten vorhanden sind.
- Löschen von initialen Konten und Vergabe von minimalen Rechten bei Systemkonten.
- Überprüfung auf Authentifizierer (Passwörter) von Feldkomponenten und Anpassung an Security-Vorgaben.
- Überprüfung ob Schlüsselzertifikate angewendet werden und diese von der *PKI* (Public Key Infrastructure) bezogen werden.
- Überprüfung ob öffentliche Schlüssel angewendet werden und Vertrauenswürdigkeit gegeben ist.
- Ergänzung von Nutzungshinweisen, um auf Rechte und Pflichten bei der Benutzung des Systems aufmerksam zu machen.
- Limitierung der freigegebenen Ports der lokalen Firewalls auf das Tunnelnetzwerk oder Netzwerksegment.
- Überprüfung der Sinnhaftigkeit von Sitzungssperren bei lokalen Steuereinheiten.
- Überprüfung auf weitere Möglichkeiten zur Ereignisaufzeichnung, wie zum Beispiel bei Vorfällen während der Sicherung oder der Wiederherstellung von Daten.
- Überprüfung der Einstellungen von Warnungen für Limits der Speicherkapazität von Ereignissen.
- Ausgabe von Informationen an Bedienpersonal, wenn die Verarbeitung von Ereignisdaten ausfällt.
- Erarbeitung des Einsatzes von Blacklisting oder Whitelisting für lokale Steuereinheiten und Touchpanels.
- Erarbeitung des Prozesses für die Überprüfung von IT-Sicherheitsfunktionen, die im laufenden Betrieb durchgeführt werden können.
- Limitierung der Berechtigungen für das Ausführen von Administrationssoftware.
- Definition des sicheren Zustands von „XAMControl“-Variablen bei Ausfällen.
- Überprüfung und Einführung von Schutzmaßnahmen für Prüfinformationen, wie Ereignisdaten.
- Implementierung von Windows-(Lese-)Berechtigungen, je nach AD-Gruppe bei lokalen Steuereinheiten und Touchpanels.
- Überprüfung der Verwendung von Verschlüsselung und ob diese ggf. verbessert werden kann.
- Überprüfung, ob die Steuerung der Netzbelastung vom Auftraggeber umgesetzt wird.
- Umfangreiche Tests zur Wiederherstellung des Automatisierungssystems.
- Anwendung der geringsten Funktionalität und Überprüfung der Möglichkeiten in „XAMControl“ und bei Windows-Diensten und -Bibliotheken.

Die beschriebenen Verbesserungsmöglichkeiten und Ansätze für Überprüfungen liefern viel Potenzial für die Optimierung der OT-Security in Tunnelsteuerungssystemen.

6.3 Teil 4-1: Product Security Development Lifecycle Requirements

Dieser Teil behandelt die organisatorische Bewertung von Prozessen, die für die Produktentwicklung oder Instandhaltung von Bedeutung sind. Für die Prozessbewertung findet das Reifegradmodell Einsatz.

Die Norm liefert Sicherheitsanforderungen für Entwickler*innen und/oder Produktlieferanten und ist daher nicht für Integratoren und Produktanwender*innen ausgelegt. Sie legt den Entwicklungslebenszyklus für Produkte fest, um von einer sicheren Entwicklung und Instandhaltung ausgehen zu können, mit dem Wissen, dass die vergebenen SL-C entsprechend umgesetzt werden. Zusätzlich werden mit der Anwendung das Secure-by-Design- und das Defense-in-Depth-Prinzip gestärkt. Die sorgfältige Planung der IT-Sicherheitsprozesse dient vor allem der beständigen Ausführung der Aktivitäten, auch bei Ressourcenmangel, unzureichender Zeit oder Prozessschwächen.[135]

Im Gegensatz zum Teil 2-4 bezieht sich dieser Teil direkt auf das Produkt und nicht auf das gesamte System. In diesem Fall ist das der Code, der in „XAMControl“ entwickelt wird. Der konkrete Anwendungsbereich für diese Norm ist schwierig abzugrenzen, da das eingesetzte System eine Kombination aus bestehenden Produkten ist, die großteils von der Dürr Austria GmbH installiert, aber nicht entwickelt werden. Dennoch wird das gesamte System betrachtet, da dieses das Produkt darstellt, das implementiert wird.

Der Teil 4-1 enthält 47 Anforderungen, die den folgenden acht Ansätzen zugeordnet sind:[136]

- Ansatz 1 – Verwaltung der IT-Sicherheit
- Ansatz 2 – Spezifikation der IT-Sicherheitsanforderungen
- Ansatz 3 – IT-Sicherheit durch den Entwurf
- Ansatz 4 – Gesicherte Implementierung
- Ansatz 5 – Verifikations- und Validierungsprüfungen der IT-Sicherheit
- Ansatz 6 – Behandlung sicherheitsbezogener Probleme
- Ansatz 7 – Verwaltung von IT-Sicherheits-Updates
- Ansatz 8 – IT-Sicherheitsrichtlinien

Alle Anforderungen sind in der Norm ausführlich beschrieben und bieten Ansätze für die Anwendung und Verbesserung der Prozesse.

[135] Vgl. OVE EN IEC 62443-4-1 (2018), S. 8 – 22.

[136] Vgl. OVE EN IEC 62443-4-1 (2018), S. 22 – 51.

6.3.1 Anwendung

Für die Anwendung werden sämtliche Anforderungen in einer Excel-Tabelle gesammelt. Zu jedem Eintrag wird der geschätzte Reifegrad ergänzt und eine Anmerkung hinzugefügt, welche die bisherige Umsetzung oder eventuelles Verbesserungspotential aufzeigt.

Ein Beispiel für die Erarbeitung einer Anforderung ist in der folgenden Tabelle dargestellt:

Ansatz	**Anforderung**	**Beschreibung**	**Reife-grad**	**Anmerkung**
Ansatz 1 – Verwaltung der IT-Sicherheit	SM-7: IT-Sicherheit der Entwicklungs-umgebung	Es muss ein Prozess mit Ablaufsteuerungen und technischen Maßnahmen angewendet werden, um das Produkt während der Entwicklung, der Fertigung und der Lieferung zu schützen. Dies umfasst den Schutz des Produkts oder eines Produkt-Updates (Patch) während Entwurf, Implementierung und Freigabe.	4/5	Im Unternehmen werden Informations-sicherheitsmaß-nahmen angewendet und laufend verbessert

Tab. 12: Anwendung der IEC 62443-4-1, Quelle: Eigene Darstellung.

Der Ansatz, die Anforderung und die Beschreibung stammen direkt aus der Norm. Anhand des Auszugs ist ersichtlich, dass die siebte Anforderung des ersten Ansatzes dargestellt wird. Sämtliche Anforderungen eines Ansatzes werden mit demselben Kürzel versehen, welches in diesem Fall „SM“ ist. Für die Anforderung der Sicherheit der Entwicklungsumgebung wird der Reifegrad 4/5 gewählt, da dieser Prozess mittlerweile automatisch, wie im Informationssicherheitskonzept beschrieben, durchgeführt wird, und ständigen Verbesserungen unterliegt, die unmittelbar dokumentiert werden. Die Informationen zu der Umsetzung der Anforderungen werden in der Anmerkung ergänzt.

6.3.2 Verbesserungspotential

Aus der Erarbeitung der Norm ergeben sich folgende Möglichkeiten zur Verbesserung der Prozesse:

- Erstellung eines Prozesses für die Kennzeichnung der Verantwortungen der geforderten Prozesse mithilfe einer RACI-Matrix.
- Überprüfung der Anwendung von Kryptografie und privaten Schlüsseln.
- Erstellung eines Bedrohungsmodells für den „XAMControl“-Individualcode.
- Ergänzung des erreichbaren Security-Levels (SL-C) im Informationssicherheitskonzept.
- Erweiterung der Genauigkeit der Dokumentation von Schnittstellen, Speicherressourcen, Dateien und Verzeichnisse, sowie der „XAMControl“-Konfigurationsdateien.
- Erarbeitung von Sicherheitsmaßnahmen bei der Entwicklung von Individualcode in „XAMControl“.
- Evaluierung von Codierungsnormen und gegebenfalls Anpassung des firmeninternen Coding-Standards.
- Definition der Strategien zur Bedrohungsabschwächung, indem potenzielle Schwachstellen während des Aufsetzens der Komponenten bzw. der Implementierung des Codes und somit vor Inbetriebnahme berücksichtigt werden.
- Definition eines Prozesses für die Überprüfung der Software-Versionen nach Common-Vulnerabilities-and-Exposures-Einträgen (*CVE*-Einträgen), welche dann gesammelt zur Verfügung gestellt werden, sowie der möglichen Compiler-Einstellungen und der verknüpfbaren Bibliotheken in „XAMControl“.
- Erstellung einer Vorlage für eine Risikoanalyse zur Bewertung von Schwachstellen und Maßnahmen.
- Erstellung von genauen Anweisungen für die Anwendung und Installation von Patches.
- Ergänzung der Beschreibung von Bedrohungen vor denen geschützt wird, mit Berücksichtigung des Defense-in-Depth-Prinzipes im Informationssicherheitskonzept.
- Ergänzung einer Beschreibung des sicheren Ausbringens von Anlagen und der Entsorgung von Produkten im Informationssicherheitskonzept.
- Erstellung einer ausführlichen Beschreibung bezüglich der Authentifikationsmechanismen und Unterscheidung zwischen normalen Anwender*innen und Administrator*innen.
- Evaluierung potenzieller Fehler, die auftreten können und dürfen.

Die beschriebenen Verbesserungsmöglichkeiten liefern einen Fortschritt für das Informationssicherheits-konzept und für das Verständnis zur Umsetzung der Maßnahmen.

6.4 Teil 4-2: Technical Security Requirements for IACS Components

Die IEC62443-4-2 ist der Teil der Normenreihe, der die erreichbaren Security-Levels (SL-C) für die Produktbewertung liefert und daher für die Hersteller ausgelegt ist. Dabei handelt es sich um eine technische Bewertung der umgesetzten Sicherheitsmaßnahmen.[137]

In Summe umfasst die Norm 58 Anforderungen, wobei nicht alle von Relevanz für die eingesetzten Komponenten sind. Einige Forderungen werden nur für spezifische Komponentenarten beschrieben, da sich der Anwendungsbereich unterscheidet.

Die Komponenten werden wie folgt unterteilt:[138]

- Anforderungen an Softwareanwendungen (SAR)
- Anforderungen an eingebettete Geräte (EDR)
- Anforderungen an Host-Geräte (HDR)
- Anforderungen an Netzwerkkomponenten (NDR)

Grundsätzlich wird nur der Individualcode, der in „XAMControl“ implementiert wird, von der Dürr Austria GmbH erstellt. Jedoch werden auch die eingesetzten Hardware-Komponenten beurteilt, da diese einen Bestandteil des gesamten Produkts bilden. Somit können Lücken in der Bewertung ausgeschlossen werden. Die Komponenten werden, wie in der Tab. 13 definiert, zugeordnet:

Bezeichnung	**Komponenten**
SAR	XAMControl, Individualcode
DER	Lokale Steuereinheiten, Touchpanels
HDR	Bedienplatzrechner (AG), Tukos (AG), DB-Server (AG)
NDR	Switches (AG), VPN-Terminator (AG)

Tab. 13: Zuordnung der Komponenten zu den Komponentenarten der IEC 62443-4-2 (SAR: Anforderungen an Softwareanwendungen, EDR: Anforderungen an eingebettete Geräte, HDR: Anforderungen an Host-Geräte, NDR: Anforderungen an Netzwerkkomponenten, AG: Auftraggeber, VPN: Virtual Private Network), Quelle: Eigene Darstellung.

Die Tunnelkopfrechner und Datenbankserver sind ein Sonderfall, da sie Host-Geräte mit den Anforderungen von eingebetteten Geräten bezüglich Echtzeit, Verfügbarkeit und Integrität sind.

Die Anforderungen sind ähnlich zu denen vom Teil 3-3. Sie bauen auf den sieben funktionalen Anforderungen auf und werden zum Teil mit weitergehenden Anforderungen ergänzt. Je nach Erfüllungsgrad der Basis-Anforderung oder der weitergehenden Anforderungen werden die Security-Levels vergeben.

[137] Vgl. OVE EN IEC 62443-4-2 (2020), S. 16 f.

[138] Vgl. OVE EN IEC 62443-4-2 (2020), S. 17.

6.4.1 Anwendung

Die Anwendung dieses Teiles ist beinahe analog zum Teil 3-3, bis auf den Aspekt, dass der Anwendungsbereich auf spezifische Komponententypen gelegt wird.

Bei der Bewertung der Komponenten werden diese von der Umgebung abgekapselt, und somit ohne jegliche Möglichkeiten außerhalb des Systems, betrachtet. Es wird Bezug auf die Anforderungen an Softwareanwendungen (SAR) und damit dem Individualcode und der „XAMControl"-Applikation, sowie die Anwendungen an eingebettete Geräte (DER), also lokale Steuereinheiten und Touchpanels, genommen. Die Geräte, die den Anforderungen an Host-Geräte (HDR) und Anforderungen an Netzwerkkomponenten (NDR) zugeordnet werden, liegen im Verantwortungsbereich des Auftraggebers und werden daher nicht beurteilt.

Die nachfolgende Abb. 17 stellt die Definition des Security-Levels für die Anforderung „CR 1.1 – Identifizierung und Authentifikation von Nutzer*innen" dar. Die Eins und Zwei in Klammer stellen die Nummerierung der weitergehenden Anforderungen dar.

- SL-C(IAC,Komponente) 1: CR 1.1;
- SL-C(IAC,Komponente) 2: CR 1.1 (1);
- SL-C(IAC,Komponente) 3: CR 1.1 (1) (2);
- SL-C(IAC,Komponente) 4: CR 1.1 (1) (2).

Abb. 17: Vorgegebene Security-Levels einer Anforderung aus der IEC 62443-4-2 (SL-C: Erreichbarer Security-Level, IAC: Identifizierung und Authentifizierung, CR: Komponentenanforderung), Quelle: OVE EN IEC 62443-4-2 (2020), S. 32.

Weiters ist die Norm auf die Unterstützung der wesentlichen Funktionen, die Anwendung von Ausgleichsmaßnahmen, falls eine Anforderung nicht erzielt werden kann, auf das Prinzip der minimal erforderlichen Rechte und auf die Anwendung eines sicheren Softwareentwicklungsprozesses nach dem Teil 4-1 ausgelegt.[139]

Die Security-Levels für Softwareanwendungen und eingebettete Geräte werden nach dem folgenden Schema in einem Excel-Dokument zugeordnet:

Grundlegende Anforderung	**Anforderung**	**SL-C SAR**	**SL-C DER**	**SL-C HDR**	**SL-C NDR**	**Anmerkung**
FR 1 – Identifizierung und Authentifikation	CR 1.1 – Identifizierung und Authentifikation von Nutzer*innen	4	4	-	-	Personalisierte Konten, mit denen sich alle Nutzer*innen authentifizieren müssen.

Tab. 14: Anwendung der IEC 62443-4-2 (SL-C: Erreichbarer Security-Level, SAR: Anforderungen an Softwareanwendungen, EDR: Anforderungen an eingebettete Geräte, HDR: Anforderungen an Host-Geräte, NDR: Anforderungen an Netzwerkkomponenten, FR: Grundlegende Anforderung, CR: Komponentenanforderung), Quelle: Eigene Darstellung.

[139] Vgl. OVE EN IEC 62443-4-2 (2020), S. 30 f.

Die weitergehenden Anforderungen und Anforderungsbeschreibungen werden bei diesem Normenteil direkt aus der Norm entnommen und evaluiert und nicht separat in der Liste aufgeführt. Bei Anforderungen, die nicht von weitergehenden Anforderungen ergänzt werden, wird der erreichbare Security-Level bestmöglich abgeschätzt. Durch die Anwendung der Norm wird der erreichbare als auch der aktuell standardmäßige eingestellte Status dokumentiert.

Nachdem die Security-Levels für jede einzelne Anforderung konkret definiert werden, ergeben sich die Security-Level-Vektoren für die Anforderungen an Softwareprozesse (SAR) und die Anforderungen an eingebettete Geräte (DER), wie nachfolgend dargestellt:

SL-C (SAR) = { 0 1 1 0 4 1 1 }

SL-C (DER) = { 0 1 0 0 4 1 1 }

Die Werte der Vektoren weisen schlechtere Werte auf, als die Security tatsächlich durchschnittlich erreicht, da für jede funktionale Anforderung der schlechteste Wert der zugeordneten Anforderungen angenommen wird. Die Anforderung mit dem niedrigsten Security-Level in der Gruppe kann oft nicht erfüllt werden, da wesentliche Funktionen damit eingeschränkt werden würden. Dafür können Ersatzmaßnahmen getroffen werden.

6.4.2 Verbesserungspotential

Aus der Evaluierung der Norm ergeben sich folgende Aspekte, die den OT-Security-Maßnahmen der Dürr Austria GmbH hinzugefügt werden können:

- Überprüfung von möglichen Hardwaremechanismen für Authentifizierer (Passwörter) und gegebenfalls die Integration solcher.
- Überprüfung, ob PKI-Zertifikate für einen Einsatzbereich von Relevanz sind.
- Überprüfung, ob öffentliche oder symmetrische Schlüssel für einen Einsatzbereich von Relevanz sind.
- Überprüfung, ob Maßnahmen oder automatische Meldungen an das Monitoring-System für erfolglose Anmeldeversuche zu treffen sind.
- Ergänzung von Nutzungshinweisen in „XAMControl“-Visualisierung und bei lokalen Steuereinheiten und Touchpanels als Desktop-Hintergrund.
- Überprüfung der Anwendung von mobilem Code, bzw. Limitierung der Berechtigungen auf bestimmte Benutzer*innen.
- Rollenspezifische Zuweisung der Sitzungssperrung nach gewissen Parametern für Windows und „XAMControl“.
- Überprüfung, ob Verfügbarkeitseinschränkungen durch eine rollenspezifische Abmeldung von Remote-Desktop-Sessions von lokalen Steuereinheiten und Touchpanels auftreten.
- Anpassung der Ereignisdatenkapazität von Windows und Überprüfung des Schwellwerts für die Ausgabe von Warnungen bzgl. des Speicherlimits.
- Überprüfung und ggf. Anpassung des Log-Managements mithilfe der NIST SP 800-92, dem Guide für das Computersicherheits-Log-Management.

- Überprüfung der Erkennung von nicht autorisierten Änderungen der Systemzeit mit NTP.
- Überprüfung der möglichen Anwendung von diversen Mechanismen zum Schutz vor Schadcodes.
- Einführung der Überprüfung der Informationssicherheitsfunktionalität mit einem Verifikationsprozess.
- Überprüfung der Möglichkeit der Verifikation von Software- und Informationsintegrität.
- Überprüfung der Möglichkeit von Authentizität und Integrität der Windows- und Drittherstellersoftware-Updates.
- Überprüfung der Relevanz von physikalischem Manipulationsschutz bzw. -erkennung zusätzlich zum Blockieren der Firewall-, USB- und Ethernet-Ports von lokalen Steuereinheiten und Touchpanels.
- Überprüfung, ob Vertrauensanker (vertrauenswürdige Datenquelle mit Schutz von Hardwaremechanismen) von Bedeutung und implementiert sind.
- Überprüfung der Möglichkeiten für Integritätsmaßnahmen für den Boot-Prozess auf Windows-Ebene.
- Überprüfung, ob Verschlüsselungsschutz notwendig und möglich ist.
- Limitierung der Zugriffsmöglichkeit auf Ereignisprotokolle, indem diese nur lesend ausgegeben und die Schreibrechte bzw. die Möglichkeit des Löschens nur für bestimmte Rollen vergeben werden.
- Überprüfung der Beistellung des Auftraggebers oder des möglichen Einsatzes von IDS (Intrusion Detection System) oder IPS (Intrusion Prevention System).
- Überprüfung von Möglichkeiten zum Schutz vor DDoS-Attacken in Windows.
- Limitierung der Bandbreite und Prozesspriorität für Windows- und „XAMControl“-Prozesse.
- Evaluierung und Parametrierung von Integritätsprüfungen bei Backups.
- Überwachung von Netzwerk- und IT-Sicherheitseinstellungen.
- Evaluierung der minimal benötigten Funktionalität von Diensten, Funktionen und Bibliotheken in Windows.

Die Punkte, bei denen nicht konkret auf lokale Steuereinheiten und Touchpanels bzw. Windows oder „XAMControl“ eingegangen wird, betreffen Softwareprozesse und eingebettete Geräte.

Vom Verbesserungspotential werden technische Maßnahmen für die Optimierung der OT-Security abgeleitet.

7 ANWENDBARKEIT ERGÄNZENDER NORMEN UND RICHTLINIEN

In diesem Kapitel werden die Normen und Richtlinien, die im Kapitel 4 Ergänzende Normen und Richtlinien behandelt wurden, auf ihre Anwendbarkeit evaluiert.

Das NIS-Gesetz wird bereits vom Auftraggeber vorgegeben, und ist daher in dessen Anforderungen berücksichtigt. Es wird somit bereits angewendet und nicht separat betrachtet.

Die Verwendung der weiteren Normen und Richtlinien ist in der nachfolgenden Tabelle erörtert:

	Evaluiert	Anwendbar	Nicht relevant
ISO/IEC 27001		X	
BDEW Whitepaper	X		
ISO/IEC 15408		X	
BSI IT-Grundschutz-Kompendium		X	
NIST SP 800-82 Rev. 2		X	
NIST Cybersecurity Framework	X		
ITIL V4			X
COBIT 2019			X
CIS Controls	X		

Tab. 15: Anwendbarkeit ergänzender Normen und Richtlinien, Quelle: Eigene Darstellung.

Bei der Anwendbarkeit wird zwischen diesen drei Möglichkeiten unterschieden:

- **Evaluiert**: werden in diesem Kapitel bearbeitet
- **Anwendbar**: sind anwendbar, werden aber nicht bearbeitet
- **Nicht relevant**: werden nicht angewendet, sind nicht relevant

Sämtliche Standards, die evaluiert werden, werden auf Verbesserungspotential untersucht. Daher wird beschrieben, wie die Überprüfung stattfindet und welche Optimierungsmaßnahmen sich daraus ergeben.

COBIT 2019 und ITIL V4 sind nicht relevant, da sich diese nicht explizit mit der Umsetzung von der IT- oder OT-Security befassen.

Die Verwendung der als anwendbar gekennzeichneten Standards für die Evaluierung der OT-Security von Tunnelsteuerungssystemen ist möglich. Diese werden aber in dieser Arbeit nicht weiterverfolgt, da sie zu umfangreich für eine detaillierte Betrachtung sind.

Darunter fällt zum einen die ISO/IEC 27001:2013. Diese Norm ist bereits in den Informationssicherheitsprozess für die Tunnelsteuerungssysteme integriert, da darauf die bestehenden Security-Konzepte aufbauen. Das betrachtete Whitepaper des BDEW ist aber eine Ableitung davon, die zusätzliche Ansätze für industrielle Umgebungen bietet.

Zum anderen ist das BSI IT-Grundschutz-Kompendium anwendbar. Die darin enthaltene Schicht „IND: Sicherheitsaspekte industrieller IT“ ist für die industrielle Umgebung von Bedeutung. Bei der weiteren Betrachtung ist ersichtlich, dass die darin enthaltenen Anforderungen bereits mit den übrigen Normen abgedeckt werden. Daher liefert die Erarbeitung kaum Ergänzungsmaßnahmen.

Die Evaluationskriterien für die Informationssicherheit, die in der ISO/IEC 15408 definiert sind, liefern weitere interessante Ansätze, die auf die OT-Security bezogen werden können. Da diese dreiteilige Norm einen weitläufigen Umfang hat, kann diese nicht genauer betrachtet werden.

Der Standard NIST SP 800-82 Rev. 2, der die Security von industriellen Steuerungssystemen behandelt, liefert wesentliche Hilfestellungen. Da das Overlay für die Beurteilung der OT-Security auf einen weiteren Standard aufbaut, ist die Bearbeitung in Bezug auf die Zeit unwirtschaftlich, da sich die Inhalte mit denen der evaluierten Normen überschneiden.

Evaluiert werden folglich

- das NIST Cybersecurity Framework, als Basis für die Betrachtung weiterer Standards,
- die CIS Controls und
- das BDEW Whitepaper.

7.1 NIST Cybersecurity Framework

Das NIST Cybersecurity Framework enthält 23 Kategorien und 108 granulare Subkategorien, die den Kategorien zugeordnet sind. Sie beschreiben die Anforderungen, welche in weiteren Standards behandelt werden. Daher befinden sich im Excel-Template zu jeder Subkategorie Referenzen auf die entsprechenden Normen. Das Framework referenziert auf die folgenden Standards:

- CIS CSC
- COBIT 5
- ISA 62443-2-1:2009
- ISA 62443-3-3:2013
- ISO/IEC 27001:13
- NIST SP 800-53 Rev. 4

Die Kategorien im Cybersecurity Framework sind generisch gehalten und dafür in den weiterführenden Normen spezifischer gestaltet. Daher können diese in den Standards unterschiedlich definiert sein. Um mehrere Ansätze zu verfolgen, werden einige dieser Normen betrachtet. Die folgende Abbildung stellt die Anwendung der referenzierten Standards dar:

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5

Abb. 18: Verwendete Referenzen einer Anforderung des NIST Cybersecurity Frameworks, Quelle: NIST Cybersecurity Framework (2018) (leicht modifziert).

Die Referenzen, die betrachtet werden, sind grün markiert, jene die nicht betrachtet werden in rot und teilweise überprüfte in orange eingefärbt. In diesem Fall ist die Referenz auf die ISO/IEC 27001:2013 orange eingefärbt, da diese mithilfe des BDEW Whitepaper betrachtet wird und darin nur die Anforderung A.8.1.1 beschrieben wird, aber nicht A.8.1.2. Durch die Einfärbung wird ersichtlich, welche Aspekte tiefgründiger behandelt werden. Wären sämtliche Referenzen rot eingefärbt, würde das bedeuten, das Thema wäre noch nicht behandelt worden. Das trifft nach der gesamtheitlichen Evaluierung aber nicht zu, da jegliche Aspekte darin berücksichtigt werden.

Die Anwendung der Referenzen wird als vollumfängliche Betrachtung der Normen durchgeführt, abgesehen von der ISO/IEC 27001:2013. Bei dieser werden die Anforderungen vom BDEW Whitepaper herangezogen, da diese bereits zu einem früheren Zeitpunkt betrachtet wurden. Die komplette Betrachtung der Standards ergibt sich, weil die aktuelle Version des NIST Cybersecurity Framework aus dem Jahr 2018 stammt und auf veraltete Standards verweist. Eine Neuauflage besteht bei den CIS Controls und COBIT zu. Von der NIST SP 800-53 gibt es ebenfalls bereits eine fünfte Revision.

Diese wird aber nicht verwendet, da stattdessen das NIST SP 800-82 in Betracht gezogen wird, welches wiederum auf die NIST SP 800-53 Revision 4 verweist. Da sich die Subkategorien in den einzelnen Normen wiederfinden, wird auf diese nicht explizit eingegangen. Aus dem Framework ergibt sich daher kein direktes Verbesserungspotential für die OT-Security in Tunnelsteuerungssystemen.

7.2 CIS Controls

Für die CIS Controls wird ebenfalls ein Excel-Dokument mit der Auflistung der Anforderungen beigestellt. Dieses wird als Basis für die Erarbeitung verwendet. Darin sind alle Controls aufgelistet und je nach Komplexität mit den entsprechenden Implementation Groups versehen. Da die Controls für die IT und nicht für Industrieanlagen ausgelegt sind, können sie nicht vollumfänglich angewendet werden. Die zutreffenden Anforderungen werden betrachtet und dem Anwendungsfall entsprechend evaluiert.

Zunächst werden nur die Anforderungen, die für die Implementation Group 1 markiert sind, behandelt, da die Dürr Austria GmbH kein Sicherheits- bzw. Experten-Teams für die Security beschäftigt. Der Scope wird zwar auf die Industrieanlagen und nicht das Unternehmen gelegt, die ressourcentechnischen Anforderungen sind aber die gleichen.

Zukünftig kann auf die Erarbeitung der IG 1 aufgebaut und die beiden zusätzlichen Gruppen IG 2 und IG 3 ergänzt werden.

Für die Ausarbeitung der Controls werden zunächst die Anforderungen, die nur auf IG 2 und IG 3 zutreffen, ausgeblendet. Daraus resultieren 44 Anforderungen, die von Relevanz für die Implementation Group 1 sind.

Die einzelnen Controls werden folgendermaßen tabellarisch dargestellt:

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3
1	1,2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	x	x	x

Tab. 16: Darstellung eines CIS Controls (CIS: Center of Internet Security, IG: Implementation Group), Quelle: Center for Internet Security (2021), Online-Quelle [25.11.2021] (leicht modifiziert).

Mithilfe der Vorlage werden die Anforderungen auf ihre bisherige Umsetzung, bzw. mögliches Verbesserungspotential geprüft.

Durch die Evaluierung der Controls ergeben sich folgende Ansätze und Verbesserungsmöglichkeiten für die OT-Security im Bereich der Tunnelsteuerungssysteme:

- Überprüfung der möglichen Umsetzung für Verteilungsmechanismen für Software bzw. Patches.
- Überprüfung von unautorisierter Software, die dann ersetzt oder entfernt wird.
- Definition eines Datenmanagementprozesses, in dem Datensensibilität, Dateneigentümer*innen, sowie die Behaltedauer und der Umgang damit definiert bzw. dokumentiert sind.
- Bestimmung der Sensibilität von Daten.
- Evaluierung einer geeigneten Technologie für die Verschlüsselung von sensiblen Daten.
- Überprüfung von automatischen Session-Sperren bei Inaktivität.
- Überprüfung der Anmelde-Accounts auf Feldkomponenten auf initiale Anmeldenamen und Passwörter.
- Definition von Intervall und Dokumentierung für die Überprüfung von Accounts und User*innen.
- Anwendung und Überprüfung von Application Whitelisting.
- Konkrete Definition der Daten, die mit dem Logging genauer untersucht bzw. ausgewertet und an den zentralen Server übermittelt werden.
- Adäquate Anpassung der Speicherkapazität für Logs.
- Berücksichtigung der Security von Backups im Datenwiederherstellungsprozess.
- Anwendung von Verschlüsselungsreferenzen bei Backup-Daten, die ähnlich der Verschlüsselung der Originaldaten sind.
- Durchführung von Awareness-Schulungen für Mitarbeitende zur Erkennung von Social-Engineering-Attacken, das Aufzeigen von Authentisierungs-Best-Practices, wie die Wahl von Passwörtern, für die Erkennung und Meldung von Sicherheitsvorfällen, sowie die Meldung von fehlenden Sicherheitsupdates für Assets.

Diese Aspekte werden überprüft und wenn möglich in den Informationssicherheitsprozess, vor allem betreffend der OT-Security, eingepflegt.

7.3 BDEW Whitepaper

Das BDEW Whitepaper ist ein Excel-Dokument mit 37 Anforderungen betreffend sicheren Steuerungs- und Telekommunikationssystemen. Diese referenzieren auf die ISO/IEC 27002:2013, den Anwendungsleitfaden für das Informationssicherheitsmanagement aus der ISO/IEC 27001, und die ISO/IEC 27009:2017, die Anforderungen für sektorspezifische Anwendungen aus der ISO/IEC 27001 enthält. Die Anforderungen sind mit konkreteren Maßnahmen und Umsetzungsvorschlägen als die Normen versehen.

Jedes Element ist mit der Sicherheitsanforderung und den entsprechenden Referenzen auf die Normen versehen. Dazu sind Ergänzungen und Anmerkungen mit weiterführenden Informationen beigefügt. Zusätzlich sind mögliche Maßnahmen für Betriebsführungs- und Leitsysteme, Systembetrieb, Übertragungstechnik und Sprachkommunikation, sowie Sekundär-, Automatisierungs- und Fernwirktechnik ergänzt.

Die folgende Abbildung zeigt einen Auszug aus dem BDEW Whitepaper, der eine Anforderung mit den Zusatzinformationen darstellt:

Nummer	Norm-Referenzen	Beschreibung
4.2.1 Ansprechpartner		
Sicherheitsanforderungen	ISO/IEC 27002:2013 / 27019:2017: 6.1.1, 6.1.5, 15.1.2	Der Auftragnehmer muss einen Ansprechpartner definieren, der während der Angebotsphase, der System-Entwicklung und während des geplanten Betriebs- und Wartungszeitraumes für den Bereich der ITSicherheit verantwortlich ist.
Ergänzungen und Anmerkungen		Bei entsprechender Unternehmensgröße sollten die Aufgaben in den verschiedenen Bereichen und Projektphasen von mehreren Mitarbeitern wahrgenommen werden. Auf Projektebene sollte allerdings ein einzelner Verantwortlicher benannt werden, der dem Auftraggeber als primärer Ansprechpartner dient. Für den Fall der Abwesenheit sollte eine Vertretung vorgesehen werden.
Betriebsführungs- und Leitsysteme, Systembetrieb		**./.**
Übertragungstechnik und Sprachkommunikation		**./.**
Sekundär-, Automatisierungs- und Fernwirktechnik		**./.**

Abb. 19: Anforderung aus dem BDEW Whitepaper, Quelle: Österreichs Energie/BDEW (2018), Online-Quelle [25.11.2021], S. 26.

Zu den Anforderungen stehen ergänzende Spalten für die Risikoklassen zur Verfügung. Diese werden für die Betrachtung aber nicht beansprucht, da es sich um eine generelle Evaluierung der Optimierungsmöglichkeiten handelt.

Der Reifegrad der Umsetzung der einzelnen Controls wird qualitativ in einer weiteren Spalte bewertet. Dafür stehen die folgenden Werte zur Auswahl:

- unbearbeitet
- nicht umgesetzt
- teilweise umgesetzt
- weitgehend umgesetzt
- vollständig umgesetzt
- vollständig umgesetzt, geprüft und bewertet
- entbehrlich

Das Whitepaper liefert keine genaue Definition der Beurteilungsgrade, daher werden diese wie folgt beschrieben, angewendet:

- **unbearbeitet**: von Relevanz, wurde aber noch nicht betrachtet
- **nicht umgesetzt**: von Relevanz und im Bewusstsein, wird aber noch nicht umgesetzt
- **teilweise umgesetzt**: Teile der Anforderung werden bereits umgesetzt
- **weitgehend umgesetzt**: Anforderung bis auf Kleinigkeiten umgesetzt
- **vollständig umgesetzt**: Anforderung wird bereits komplett umgesetzt
- **vollständig umgesetzt, geprüft und bewertet**: *Diese Bewertung wird nicht verwendet*
- **entbehrlich**: Anforderung nicht anwendbar oder nicht gefordert

Weiters liefert die Vorlage eine Hilfestellung für die Bewertung der Anforderungen bei internen und externen Audits mit den entsprechenden Parametern aus den beiden referenzierten Normen.

Sofern eine Verbesserung der Anforderungen möglich ist, wird das Verbesserungspotential evaluiert. Dadurch ergeben sich weitere Ansätze zur Verbesserung der OT-Security, die einen direkten Bezug zu Industrieanlagen besitzen. Dazu zählen:

- Evaluierung der Anwendung von internen Audits.
- Implementierung von Laufzeitüberwachungs-Mechanismen.
- Deaktivierung von nicht benötigten Diensten.
- Überprüfung der Konsistenz von Daten an den Außenschnittstellen von Anwendungen, als auch bei der Übergabe zwischen verschiedenen Systemmodulen innerhalb von Applikationen.
- Überprüfung von Kommunikationen auf Applikations-Ebene mit Hilfe von Kommunikations-Gateways mit Prüffunktionen.

Da im OT-Security-Prozess die ISO/IEC 27001:2013 bereits berücksichtigt ist, ergeben sich aus dem BDEW Whitepaper nur wenige Verbesserungsmaßnahmen. Dafür liefert es Erkenntnisse für Optimierungen der bereits angewendeten Maßnahmen.

7.4 NIST SP 800-82 Rev. 2

Ursprünglich war geplant die NIST Special Publication 800-82 in der zweiten Revision in die Verbesserung der OT-Security von Tunnelsteuerungssystemen miteinzubinden. Bei der genauen Evaluierung stellte sich heraus, dass das Overlay mit den Controls auf die NIST SP 800-53 Rev. 4 verlinkt. Daher müssen beide Standards parallel betrachtet werden. Somit ist die Schnittmenge der Overlays der beiden Standards auf Verbesserungspotential zu evaluieren. Das ergibt einen zeitlich zu umfangreichen Aufwand für die Evaluierung eines ergänzenden Standards. Dieser wäre analog zu den betrachteten Teilen der IEC 62443 zu sehen. Daher wird dieser Standard in dieser Arbeit nicht weiter betrachtet.

Eine zukünftige Erarbeitung dieses Standards und Einpflegen in den OT-Security-Prozess ist aber geplant.

8 OPTIMIERUNG DER OT-SECURITY IN TUNNELSTEUERUNGSSYSTEMEN

In diesem Kapitel werden die Anpassungen für die Umsetzung der Informationssicherheit betreffend die OT-Security in Tunnelsteuerungssystemen evaluiert. Das betrifft sowohl die Dokumentation, sowie prozessuale und technische Verbesserungen.

Die Anpassungen ergeben sich aus den erarbeiteten Verbesserungspotentialen, die als Ergebnis der Ausarbeitungen der Normen resultieren. Die möglichen Verbesserungen der diversen Normen werden zusammengefasst und die unterschiedlichen Ansätze zu den Themen vereint. Daraus ergibt sich ein einheitliches Gesamtbild für die verschiedenen Anpassungen.

Zusätzlich werden in diesem Kapitel gefundene Verbesserungsmöglichkeiten, die nicht von den Standards behandelt werden, ergänzt.

Diese werden in

- prozessuale Anpassungen und
- technische Anpassungen aufgeteilt.

Die prozessualen Anpassungen beschreiben die benötigten Anpassungen diverser Prozesse, die für die OT-Security von Relevanz sind. Mit diesen werden die Abläufe zur Umsetzung von Maßnahmen definiert. Die technischen Anpassungen enthalten konkrete technische und umsetzbare Maßnahmen, wobei die technischen Anpassungen ebenso in die Prozesse und die Dokumentation, integriert werden müssen.

Ergänzend wird am Ende des Kapitels das Defense-in-Depth-Modell für die OT-Security in Tunnelsteuerungssystemen evaluiert.

8.1 Prozessuale Anpassungen

Die prozessualen Anpassungen betreffen sowohl die Ergänzung von komplett neuen Inhalten, die auch technisch noch umgesetzt werden müssen, als auch Teile der Prozesse, die noch dokumentiert werden müssen. Die Ergebnisse werden in das Informationssicherheitskonzept der Dürr Austria GmbH integriert. Daher erfolgt eine Gliederung nach den Kapiteln des Konzepts. Es ist zu beachten, dass für die Vermeidung von Redundanzen die Zuordnung der Verbesserungsmaßnahmen nur bei dem zutreffendsten Thema stattfindet.

Allgemein

Eine Überprüfung von Dritten für die Erkennung von weiteren Möglichkeiten oder potenziellen Fehlerquellen im Informationssicherheitsprozess sollte stattfinden. Dazu wäre ein internes oder auch externes Audit anzudenken.

Als nächster Schritt ist eine Awareness-Schulung der Mitarbeitenden durchzuführen, um die OT-Security sichtbar zu machen. Damit soll Bewusstsein für die Erkennung von Social-Engineering-Attacken, die Anwendung von Authentifizierungs-Best-Practices, welche zum Beispiel die Wahl von Passwörtern betreffen, für Erkennung und Meldung von Sicherheitsvorfällen, sowie die Meldung von fehlenden Sicherheitsupdates für Assets geschaffen werden. Die Überprüfung auf IT-Sicherheitsvorfälle und der Umgang damit müssen noch definiert werden. Bei Auffälligkeiten, die auf einen Vorfall hindeuten, müssen Anpassungen der Sicherheitsmaßnahmen, wie zum Beispiel die Änderung der Passwörter von Standard-Benutzerkonten oder der Datenbank, stattfinden. Weiters ist ein Prozess zu definieren, wie mit bekannt gewordenen Sicherheitslücken umgegangen werden muss.

Die Grundkonfiguration der Security sollte automatisiert überprüfbar sein. Dazu muss die sichere Standard-Konfiguration genauer beschrieben werden. Dieser ist beizulegen, welche Schritte nach dem Einbau der Komponenten in die Tunnelanlage noch durchzuführen sind, um die Grundkonfiguration zu vervollständigen. Zusätzlich sind Maßnahmen für die Überprüfung der IT-Sicherheitsfunktionen im laufenden Betrieb zu evaluieren. Ergänzend muss ein durchführbarer Prozess für die Überprüfung der Informationssicherheitsfunktionalität mit einem Verifikationsprozess erstellt werden. Dazu werden als Hilfestellung Testarten definiert, wie zum Beispiel Funktionstests, Stresstests und Penetrationstests, die vor und nach der Auslieferung der Komponenten regelmäßig durchgeführt werden.

Es muss ein Datenmanagementprozess definiert werden, in dem die Datensensibilität, die Dateneigentümer*innen, sowie die Behaltedauer und der Umgang mit den Daten erläutert und dokumentiert sind. Dazu muss zusätzlich die Bestimmung der Sensibilität von Daten durchgeführt werden. Auch muss die Dokumentation in Bezug auf die Genauigkeit von Schnittstellen, Speicherressourcen, Dateien und Verzeichnisse, sowie der „XAMControl“-Konfigurationsdateien erweitert werden.

Das Informationssicherheitskonzept muss um weitere Aspekte, welche in dieser Arbeit evaluiert wurden, erweitert werden. Das ist zum einen die Beschreibung der Bedrohungen vor denen geschützt werden soll, unter Berücksichtigung des Defense-in-Depth-Prinzips. Weiters müssen potenzielle Fehler, die im Laufe des Betriebs zu erwarten sind, niedergeschrieben werden. Ebenso von Relevanz ist das sichere Ausbringen der Komponenten aus den Anlagen, sowie deren sichere Entsorgung. Zusätzlich ist eine Ergänzung des erreichbaren Security-Levels (SL-C) umzusetzen. Für das Patchen der Firmware-Stände besteht die Notwendigkeit diese davor anlagenspezifisch zu dokumentieren, um die verwendeten Versionen überprüfen zu können. Daher müssen diese in den Asset-Listen erfasst werden.

Für Änderungen der Systeme muss ein Prozess dokumentiert werden, der beschreibt, wie damit umgegangen und inwiefern die Dokumentation angepasst wird. Ergänzend müssen sämtliche beschriebene Maßnahmen, die umgesetzt werden, mit einer Kennzeichnung der verantwortlichen Person/Position dokumentiert werden. Die Verantwortungen müssen dazu mittels einer RACI-Matrix evaluiert werden. Die Matrix kann in das Informationssicherheitskonzept integriert werden.

Zugriffschutz und Berechtigungsvergabe

Ein wesentlicher Aspekt des Zugriffsschutzes und der Berechtigungsvergabe ist der Abruf der benötigten Benutzeraccounts mit den entsprechenden Berechtigungen beim Auftraggeber. Dazu muss noch die interne Verantwortung für die Durchführung abgeklärt und dokumentiert werden.

Weiters muss der Prozess für die Validierung von Dateneingaben in „XAMControl“, entsprechend den festgesetzten Grenzwerten und der Möglichkeit der Änderung nur von autorisierten Benutzer*innen innerhalb der Anlage, definiert werden.

Es muss dokumentiert werden, in welchem Intervall die Überprüfung auf entbehrliche Benutzerkonten in „XAMControl“ und Windows stattfindet und wie damit weiterführend verfahren wird. Weiters muss eine berechtigungsspezifische Darstellung der Zugriffsmöglichkeiten auf Windows, sowie die generellen Möglichkeiten der Benutzergruppen ergänzt werden. Ergänzend werden die Authentifikationsmechanismen und die Unterscheidung von normalen Anwender*innen und Administrator*innen ausführlich beschrieben. Zusätzlich muss eine konkrete Auflistung und Begründung der Standard-Benutzerkonten beigelegt werden.

Weiters muss evaluiert werden, ob eine maximale Anzahl gleichzeitig angemeldeter Nutzer*innen die OT-Security erheblich verbessert. Die Erkenntnisse werden im Informationssicherheitskonzept ergänzt. Die wahrscheinlichsten Arten von einzutretenden Sicherheitsvorfällen werden ebenfalls im Konzept niedergeschrieben.

Kryptografische Maßnahmen

Die kryptografischen Maßnahmen müssen evaluiert und im Informationssicherheitskonzept prozessual definiert werden.

Logging / Ereignisaufzeichnung

Für das Logging muss die entsprechende Behaltedauer der Daten definiert werden. Zusätzlich müssen die betrachteten Informationen konkret beschrieben und eine Abgrenzung der für das zentrale Monitoring bereitgestellten Daten stattfinden.

Softwareentwicklung

Für die sichere Softwareentwicklung ist ein Bedrohungsmodell für den „XAMControl“-Individualcode zu erstellen. Dazu müssen Codierungsnormen und gegebenfalls Anpassungen des firmeninternen Coding-Standards durchgeführt und Sicherheitsmaßnahmen bei der Entwicklung des Codes definiert werden.

Zusätzlich müssen die sicheren Zustände der „XAMControl“-Variablen, die vor allem bezüglich Ausfallsszenarien von Relevanz sind, im Informationssicherheitskonzept beschrieben werden.

Schwachstellenmanagement

Die Definition des Prozesses zur Bedrohungsabschwächung, in dem potenzielle Schwachstellen während des Aufsetzens der Komponenten bzw. der Implementierung des Codes vor Inbetriebnahme berücksichtigt werden, muss durchgeführt werden. Zusätzlich ist ein Prozess für die Überprüfung der eingesetzten Software nach CVE-Einträgen umzusetzen. Auf dieser Basis soll die Software gesammelt für die Installation zur Verfügung gestellt werden.

Weiters muss eine Vorlage für eine Risikoanalyse zur Bewertung von Schwachstellen und deren Maßnahmen erstellt werden.

Härtung / Netzwerk / Schutz vor Schadsoftware

Das Kommunikationsschema, das die benötigten Protokolle und aktivierten Firewall-Ports auflistet, wird zukünftig mit aktivierten bzw. deaktivierten USB-Ports und Ethernet-Schnittstellen ergänzt. Zusätzlich werden eventuell gesperrte Grafikkarten-Schnittstellen in diesem und im Informationssicherheitskonzept dokumentiert. Zur Darstellung der verwendeten „XAMControl“-Dienste werden diese anlagenspezifisch aus der Tab. 4 in das Informationssicherheitskonzept übernommen.

Der Umgang mit mobilen Datenträgern im Anlagenumfeld muss definiert werden. Das bedeutet, dass konkretisiert wird, ob diese eingesetzt werden dürfen.

Es soll eine Definition von Penetrationstests und Ereignisstürmen für lokale Steuereinheiten, Touchpanels und „XAMControl“ stattfinden und eine mögliche Anwendung evaluiert werden. Falls nicht, muss die Begründung im Informationssicherheitskonzept ergänzt werden.

Backup & Restore

Es muss eine konkrete und schrittweise Anleitung für die Durchführung des Backup-&-Restore-Prozesses erstellt werden. Zurzeit ist die Beschreibung im Informationssicherheitskonzept oberflächlich gehalten. Dazu muss ergänzt werden, wie erfolgreiche Backups erstellt und erkannt werden. Dasselbe gilt für die Wiederherstellung der Sicherungen. Weiters muss die Security von Backups über deren Lifecycle berücksichtigt werden. Zusätzlich muss eine ausführliche Testroutine betreffend der Wiederherstellung des Automatisierungssystems definiert werden.

Patch Management

Die Prozessanpassungen beim Patch Management finden durch die Erstellung von detaillierten Installationsanleitungen für Patches statt. Die Anleitungen müssen genaue Anweisungen für die Anwendung und Installation von Patches beinhalten.

Zumindest bei der Umsetzung des Patch Managements müssen Überprüfungen von unautorisierter Software durchgeführt werden. Die Software wird entweder ersetzt oder entfernt.

Zukünftig müssen auch Patches von der Firmware von Feldgeräten berücksichtigt werden. Die Möglichkeit des Einspielens der Firmwareupdates muss definiert und Verfügbarkeitseinschränkungen berücksichtigt werden. Dazu muss ein konkreter Ablauf definiert, sowie Möglichkeiten zur Integrationsprüfung evaluiert werden.

8.2 Technische Anpassungen

Die technischen Anpassungen sind jene, die direkt auf den Komponenten, ergänzend zu den bisherigen Maßnahmen, umgesetzt werden. Sie werden entsprechend des Aufbaus des Informationssicherheitskonzeptes gegliedert, um diese im Informationssicherheitskonzept angemessen ergänzen zu können. Einige der Maßnahmen können inhaltlich mehreren Überbegriffen zugeordnet werden. Dabei wurde immer der passendste gewählt, um Redundanzen zu vermeiden.

Allgemein

Die Ergänzung von Nutzungshinweisen, um auf Rechte und Pflichten bei der Benutzung des Systems aufmerksam zu machen, ist anzustreben. Diese werden in Windows simpel als Desktophintergrund dargestellt. Bei „XAMControl“ findet eine Integration in die Visualisierung statt.

Zugriffschutz und Berechtigungsvergabe

Eine verschlüsselte bzw. passwortgeschützte Ablage der Passwortlisten mit Informationen zu den einzelnen Tunnelanlagen ist am Firmenserver vorgesehen. Darin sind Datenbankpasswörter, Feldgerätpasswörter, sowie das Passwort für den Standard-Useraccount mit Zugriff auf das Sicherungsverzeichnis, gespeichert. Aus diesem Grund ist ein entsprechender Schutz anzuwenden.

Für das anlagenspezifische Backup-Verzeichnis muss eine konkrete Limitierung der Benutzergruppen mit Zugriffsrecht angewendet werden. Das Dateisystem in Windows muss bei lokalen Steuereinheiten und Touchpanels berechtigungsspezifisch geschützt werden. Das heißt, dass unter anderem nur Administrator*innen Zugriffsberechtigungen für die Programmverzeichnisse bekommen und Standard-Benutzer*innen nur den Zugriff auf deren persönliche Daten haben. Zusätzlich müssen die Berechtigungen auf die Windows-Administrationsprogramme streng reglementiert sein, sodass nur noch User*innen aus der Administratorengruppe darauf zugreifen können. Dasselbe gilt für das Ausführen von Softwareprozessen, sowie mobilem Code, wie zum Beispiel portabler Software. Bei Prüfinformationen wie Ereignisdaten ist darauf zu achten, dass Standard-User*innen maximal Lese- aber keine Schreibrechte bekommen.

Systemkonten müssen mit den minimal benötigten Rechten ausgestattet werden. Hinzu kommt, dass sämtliche initiale Konten, die keine wesentliche Funktion erbringen, gelöscht werden müssen. Der lokale Backup-Benutzeraccount, der als Windows-Konto für Notfälle bei den lokalen Steuereinheiten und Touchpanels besteht, sollte weitestgehend niedrigprivilegiert parametriert werden, um bei einem Missbrauch dieses Kontos keine weitreichenden Folgen zu erzielen. Die Einführung einer eindeutigen Identifizierung und Authentifizierung von Softwareprozessen muss evaluiert werden.

Es muss eine Evaluierung durchgeführt werden, welche Feldkomponenten Authentifizierungsmechanismen, wie zum Beispiel Passwörter, unterstützen. Für diese werden komplexe Passwörter vergeben. Weiters werden mögliche Hardwaremechanismen und deren Anwendungsmöglichkeiten für Authentifizierer überprüft.

Automatische Sitzungssperren für lokale Steuereinheiten und Touchpanels müssen evaluiert werden. Vor allem bei lokalen Steuereinheiten, die lokal nur bedient werden, um diese für die Inbetriebnahme entsprechend einzurichten, ist die Sinnhaftigkeit zu hinterfragen. Daher ist eine benutzergruppenspezifische Abmeldung, vor allem niedrigprivilegierter Benutzerkonten, anzustreben. Das Gleiche gilt für die Sperren von Remote-Desktop-Sessions. Sitzungssperren in „XAMControl“ sind nicht möglich, da eine ständige Bedienbarkeit gefordert ist und diese damit behindert werden würde.

Kryptografische Maßnahmen

Die Anwendung von kryptografischen Maßnahmen bzw. eines Verschlüsselungsschutzes ist zu prüfen. Dabei müssen die Anwendungsmöglichkeiten von Kryptografie und somit privaten, öffentlichen und symmetrischen Schlüsseln auf ihre Relevanz für den Einsatzbereich geprüft werden. Zusätzlich muss die Vertrauenswürdigkeit der Schlüssel berücksichtigt werden. Sofern Schlüsselzertifikate angewendet werden, müssen diese von einem Vertrauensanker, bzw. der PKI bezogen werden.

Beim Umgang mit sensiblen Daten müssen diese mit einer geeigneten Technologie verschlüsselt werden.

Logging

Die Protokollierung der An- und Abmeldungen in Windows muss für eine bestimmte Anzahl von Tagen definiert und parametriert werden. In „XAMControl“ muss die Zeitspanne nicht separat definiert werden, da darin die An- und Abmeldeinformationen ohnehin länger (entsprechend des Ringspeichers) gespeichert sind.

Zusätzlich soll die Überprüfung auf weitere Möglichkeiten zur Ereignisaufzeichnung stattfinden, um sämtliche relevante Ereignisse sicherstellen zu können. Dazu zählen unter anderem erfolglose Anmeldeversuche und relevante Daten, die mit der Übermittlung an das zentrale Monitoring-System einen schnellen Überblick über Informationssicherheitsvorfälle liefern. Sollten weitere aufzuzeichnende Ereignisse in Betracht kommen, kann der Standard NIST SP 800-92, der Guide für das Computersicherheits-Log-Management, als Hilfestellung verwendet werden.

Damit die Ereignisse über einen längeren Zeitraum gespeichert werden, muss eine Anpassung der Ereignisdatenkapazität stattfinden. Bei der Überschreitung eines definierten Schwellwerts soll eine Warnung bezüglich des Speicherlimits ausgegeben werden.

Weiters ist eine Ausgabe von Informationen an das Bedienpersonal, wenn die Verarbeitung von Ereignisdaten ausfällt, sowie eine Implementierung von Laufzeitüberwachungs-Mechanismen, wie zum Beispiel Watch Dogs, zu prüfen.

Softwareentwicklung

Der Einsatz von Sicherheitsmaßnahmen für die Entwicklung von Individualcode in „XAMControl“ muss überprüft und umgesetzt werden.

Schwachstellenmanagement

Die Berücksichtigung von potenziellen Schwachstellen während des Aufsetzens der Komponenten bzw. der Implementierung des Codes muss vor der Inbetriebnahme umgesetzt werden.

Härtung / Netzwerk / Schutz vor Schadsoftware

Das Blockieren von Grafikkarten-Schnittstellen von lokalen Steuereinheiten und Touchpanels soll überprüft werden. Dabei muss der etwaige Zugriff bei Ausfällen von Remote-Verbindungen berücksichtigt werden, da ansonsten keine weitere Möglichkeit der visuellen Darstellung besteht. Ergänzend ist die Anwendung eines physischen Manipulationsschutzes auf Wirtschaftlichkeit und Notwendigkeit zu prüfen.

Zusätzlich zur Limitierung der freigegebenen Ports der lokalen Firewalls müssen diese auf das Tunnelnetzwerk bzw. die entsprechenden Netzsegmente beschränkt werden, um Zugriffe von einem anderen Netzwerk zu verhindern.

Eine ausführliche Härtung der Datenbanken muss zukünftig realisiert werden. Dazu werden die Vorgaben von Microsoft umgesetzt. Bei den Datenbanken auf den lokalen Steuereinheiten wird gegebenfalls der „Mixed Mode“ aktiviert, damit eine Anmeldung mit den Windows- bzw. Active-Directory-Benutzerkonten möglich ist.

Da keine Software zum Schutz vor Schadsoftware verwendet wird, um jegliche Probleme mit der Performance und somit Beschränkungen der Verfügbarkeit zu vermeiden, ist die Umsetzung von Application Whitelisting zu prüfen. Damit soll der Einsatz von Schadsoftware verhindert werden. Zusätzlich muss eine Überprüfung der möglichen Anwendung von Mechanismen zum Schutz vor Schadcodes, auch was den Individualcode in „XAMControl“ betrifft, geprüft werden.

Zur Vervollständigung des Prinzips der geringsten Funktionalität müssen sämtliche Dienste und Bibliotheken in Windows auf ihre Notwendigkeit überprüft werden und nicht benötigte deaktiviert oder deinstalliert werden.

Zum Schutz vor DDoS-Attacken müssen die Datenübertragungsraten mit Berücksichtigung der einzelnen Protokolle limitiert, sowie weitere Maßnahmen evaluiert werden. Zusätzlich zu der Limitierung der Bandbreite müssen Prozessprioritäten für Windows- und „XAMControl“-Prozesse vergeben werden, damit die wesentlichen Funktionen am längsten verfügbar sind.

Eine Abklärung der Beistellung des Auftraggebers oder des möglichen Einsatzes von IDS (Intrusion Detection System) oder IPS (Intrusion Prevention System) ist durchzuführen und abzuwägen, ob ein solches System einen wirtschaftlich vertretbaren Vorteil mit sich bringt.

Es sind Überprüfungen von Möglichkeiten für Integritätsmaßnahmen vom Boot-Prozess auf Windows-Ebene durchzuführen und zu ergänzen. Weiters müssen Verfahren zur Verifikation von Software- und Informationsintegrität evaluiert werden.

Eine automatische Überprüfung zur Erkennung von nicht autorisierten Änderungen der Systemzeit über NTP muss stattfinden, da ansonsten die Zeitstempel der Ereignisdaten manipuliert werden könnten.

Mechanismen zur Überwachung von Netzwerk- und IT-Sicherheitseinstellungen müssen evaluiert und eingeführt werden, um veränderte Parameter zu erkennen. Die Durchführung von Penetrationstests bei lokalen Steuereinheiten, Touchpanels und „XAMControl“ vor Inbetriebnahme ist anzudenken, um die Sicherheitsmaßnahmen zu bewerten.

Backup & Restore

Die Backup-Daten müssen ähnlich gut wie die Originaldaten verschlüsselt werden. Das kann damit erzielt werden, dass der Ablageordner für Backups im Dateisystem nach denselben Berechtigungen Zugriff gewährt, wie sie im Originalsystem umgesetzt sind.

Die Möglichkeit zur Parametrierung von Integritätsprüfungen bei Backups muss in „XAMControl“, bzw. der Microsoft SQL-Datenbank, sowie im Backup-Programm für die Erstellung der Sicherungen von lokalen Steuereinheiten und Touchpanels geprüft werden.

Bei der Sicherung der Daten werden Einträge erstellt, welche die Durchführung dokumentieren. Für die Wiederherstellung muss das noch geprüft werden.

Patch Management

Für die Verteilung von Patches und Software auf lokale Steuereinheiten und Touchpanels sollen zukünftig Verteilungsmechanismen zum Einsatz kommen, welche die entsprechenden Daten aussenden. Die Umsetzungsmöglichkeiten müssen evaluiert und die beste Lösung angewendet werden.

Bei Windows- und Drittherstellersoftware-Updates muss überprüft werden, wie die Sicherstellung der Authentizität und Integrität möglich ist und diese dann entsprechend umgesetzt werden.

8.3 Defense-in-Depth-Modell

Sämtliche bereits umgesetzte, als auch evaluierte Maßnahmen, welche die OT-Security in Tunnelsteuerungssystemen betreffen, werden für die Erstellung des Modells berücksichtigt. Daraus lassen sich die Schichten für das Defense-in-Depth-Modell ableiten. Dieses ist für die lokalen Steuereinheiten und Touchpanels gesamtheitlich definiert. „XAMControl“ ist als Applikation integriert und wird nicht gesondert betrachtet.

Die Abb. 20 zeigt das erstellte Defense-in-Depth-Modell:

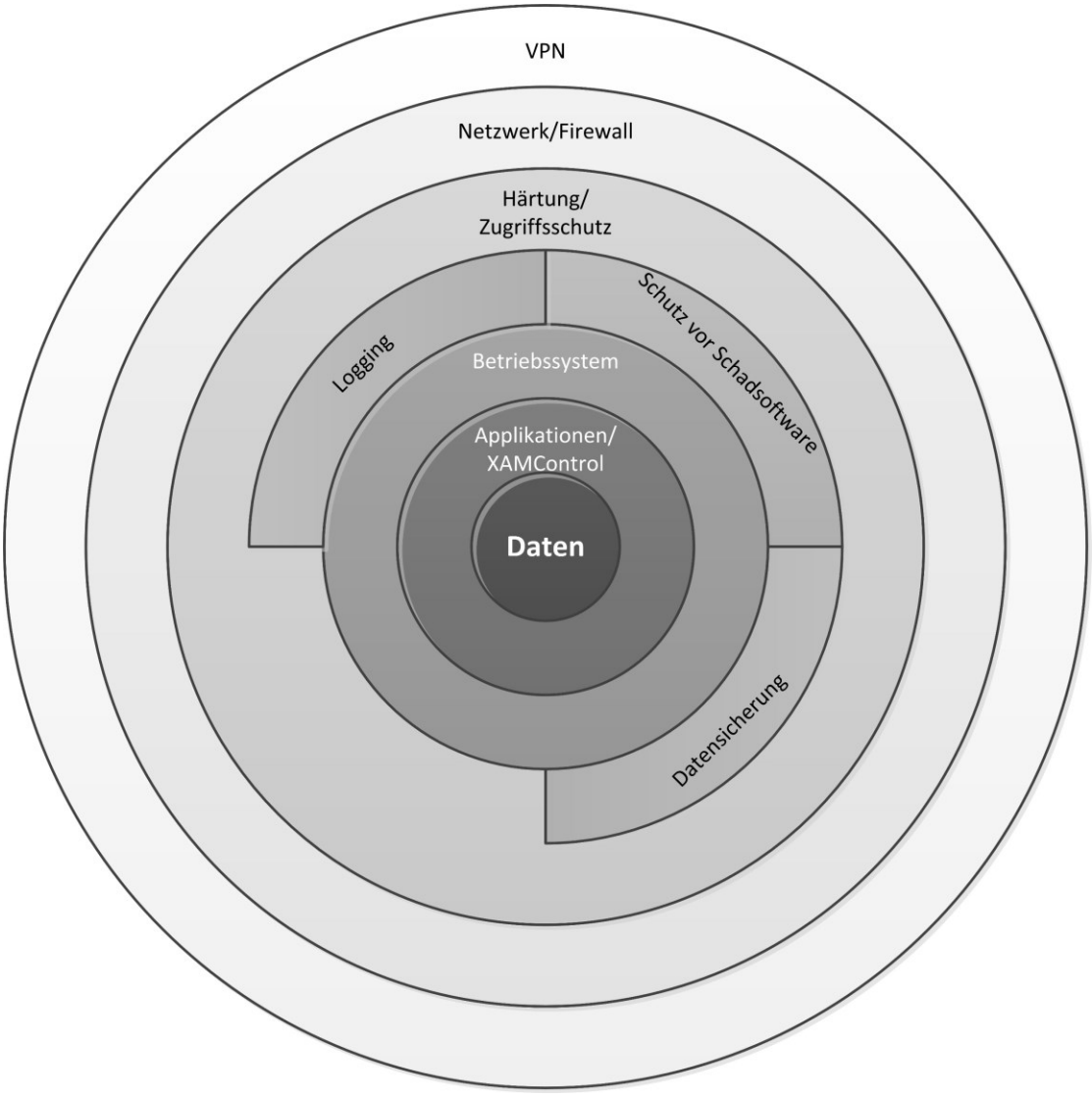

Abb. 20: Defense-in-Depth-Modell der OT-Security in Tunnelsteuerungssystemen (VPN: Virtual Private Network), Quelle: Eigene Darstellung.

Anhand der Abbildung ist ersichtlich, welche Schichten durchdrungen werden müssen, um einen erfolgreichen Angriff durchzuführen. Weiters ist ablesbar, wie die Schichten zur Aufrechterhaltung der Security beitragen.

Die äußerste Schicht ist das VPN, welches vom Auftraggeber beigestellt wird. Dieses umfasst den gesamten Zugriff zu den Tunnelanlagen. Sollte ein Durchdringen gelingen, besteht zumindest ein Zugriff zu den Tunnelnetzwerken.

Die Netzwerk/Firewall-Schicht dient dem Erkennen von Eindringlingen und der Limitierung der Netzwerk-Ports und Netzwerkzuordnung der Kommunikationspartner. Somit wird der Zugriff auf weitere Komponenten erschwert.

Im Fall eines Übergehens der Firewall bzw. des Netzwerkschutzes, kommen Härtung und Zugriffsschutz zum Tragen. Dabei wird unter anderem dafür gesorgt, dass Authentifizierungsmechanismen, komplexe Passwörter, sowie Blockierungen von Ethernet- und USB-Schnittstellen umgesetzt werden.

Als Zwischenschicht zum Eindringen in das Betriebssystem werden drei parallele Layer definiert. Dabei handelt es sich um den Schutz vor Schadsoftware. Das sind Maßnahmen für die Verhinderung des Einbringens von Schadsoftware in die Systeme. Dazu wird nebenher geloggt, um Eindringversuche aufzuzeichnen. Das ist vor allem bei häufigen hintereinander fehlgeschlagenen Zugriffsversuchen, sowie zu untypischen Zeiten genauer zu beobachten. Drittens wird die Datensicherung betrieben. Sollte es zu einem Eindringen und Einbringen von Schadsoftware oder zur Manipulation von Daten kommen, kann mithilfe von Backups der letzte einwandfreie Stand eingespielt werden. Dabei ist zu beachten, dass die Sicherheitsmaßnahmen angepasst werden, um ein neuerliches Eindringen zu verhindern.

Um eine erfolgreiche Invasion in das Betriebssystem zu erschweren, werden weitere Maßnahmen getroffen. So werden im Dateisystem Limitierungen der Zugriffe je nach Berechtigung durchgeführt und Windows-Administrationstools, wie die Eingabeaufforderung und die Gruppenrichtlinie für User*innen ohne Administratorenberechtigungen gesperrt.

Falls bis zu den Applikationen durchgedrungen wird, werden sämtliche Applikationen, bei denen ein Passwortschutz möglich ist, sowie „XAMControl“, mit komplexen Passwörtern bzw. den Active-Directory-Authentifizierungsdaten geschützt. Das Durchbrechen dieser Schicht bietet den Weg zum Kern des Modells.

Sämtliche Schichten werden zum Schutz der Informationen umgesetzt. Dabei handelt es sich um die Daten von Tunnelanlagen, die vor allem vor Manipulation geschützt werden müssen.

Dieses Defense-in-Depth-Modell wird im Informationssicherheitskonzept eingepflegt, um die unterschiedlichen Verteidigungsschichten übersichtlich darzustellen.

9 RESÜMEE

In diesem Kapitel werden die Ergebnisse und Erkenntnisse dieser Arbeit zusammengefasst, der Ausblick der zukünftigen Tätigkeiten beschrieben, sowie die Erreichung der Ziele evaluiert.

Eine konkrete Zuordnung der Komponenten in die Sparten IT oder OT ist in den Tunnelanlagen beinahe unmöglich. Das kommt daher, dass die Geräte der Steuerungsebene, die in OT-Anlagen verbaut werden, größtenteils IT-Komponenten sind. Daher ist eine ausgeprägte IT/OT-Konvergenz vorzufinden. Weiters ist die Evaluierung der Angreifer*innen und möglichen Attacken eine aufschlussreiche Information. Dieses Wissen macht Angriffe trotzdem nicht unmöglich und es können unvorhersehbare Ereignisse eintreten. Da die evaluierten Normen sich nicht speziell auf diese Parameter beziehen und einen gesamtheitlichen Schutz der Komponenten vorsehen, ist die Definition von Angreifer*innen und Angriffsarten dafür obsolet.

Aus der IEC 62443 lassen sich viele Aspekte der unterschiedlichen Teile entnehmen. Konkret anwendbar sind die Teile 2-4, 3-3, 4-1 und 4-2, da diese für Systemintegratoren und Produktentwickler ausgelegt sind. Das sind die beiden Rollen, welche die Dürr Austria GmbH bezüglich der Tunnelsteuerungssysteme einnimmt. Jedoch überschneiden sich die Inhalte der Normen, da der Umfang für die Evaluierung für sämtliche Teile beinahe gleich angenommen wurde.

Es finden sich unzählige weitere zutreffende Normen. Daher wurde in dieser Arbeit eingegrenzt, welche Normen oberflächlich betrachtet und welche genauer evaluiert werden. Daraus ergibt sich, dass viele Standards unterschiedliche Terminologien für dieselben Bedeutungen verwenden. Im Wesentlichen sind die Inhalte oft sehr ähnlich und häufig auf bestimmte Anwendungsbereiche zugeschnitten. Selbst wenn IT-Normen und -Richtlinien angewendet werden, müssen die wesentlichen Funktionen ständig im Vordergrund stehen und berücksichtigt werden. Eine Anwendung von IT-Standards ist aber besser möglich als anfänglich angenommen. Das kommt daher, dass diese bessere Möglichkeiten für die eingesetzten IT-Komponenten aufweisen, als die Normen die rein für die OT-Security ausgelegt sind. Der Vorteil der OT-Security-Normen ist, dass diese die uneingeschränkten wesentlichen Funktionen umfänglicher behandeln und das industrielle Umfeld berücksichtigen. Es hätten noch weitaus mehr Normen genauer betrachtet werden können. Um den Umfang nicht zu sprengen, wurden nur die CIS Controls, das BDEW Whitepaper und das NIST Cybersecurity Framework umfänglich behandelt.

Das behandelte Thema in allen Aspekten zu beschreiben ist kaum möglich, da dadurch der Rahmen gesprengt worden wäre. Dafür sind die Optimierungsmöglichkeiten der einzelnen Standards ausführlich beschrieben und zusammengefasst, damit diese einheitlich in den Unternehmensstandard zurückgeführt werden können. Durch den Vergleich des Ist-Zustands mit den Normen ist ersichtlich, dass das Unternehmen bezüglich der OT-Security gut aufgestellt ist. Es gibt trotzdem noch einiges zu verbessern, wobei berücksichtigt werden muss, dass die Security ein kontinuierlicher Prozess ist, der ständig angepasst werden muss.

Zukünftige Anpassungen können mit den technischen Beschreibungen der IEC 62443 erreicht werden. Diese wurden in dieser Arbeit nicht berücksichtigt, da sie nicht zugänglich sind. Dabei wären konkret die Teile 2-3 „Patch Management in the IACS Environment“ und 3-1 „Security Technologies for IACS“ von Interesse. Diese beinhalten technische Umsetzungsmaßnahmen, die als Ergänzung zu den Normen, welche lediglich die Umsetzung der Security bewerten, angewendet werden können. Als weiteren Schritt können die Teile, die noch nicht veröffentlicht wurden, auf Anwendbarkeit und Verbesserungspotential überprüft werden. Dabei handelt es sich um die Teile 1-3 „System Security Compliance Metrics“, 1-4 „IACS Security Lifecycle and Use-Cases“, welcher sich noch im Entwurfsstatus befindet, und 2-2 „Implementation Guidance for an IACS Security Management System“. Es muss aber angemerkt werden, dass die wesentlichen Aspekte bereits mit den bisher evaluierten Teilen abgedeckt sind, da diese vor allem für Produktentwickler und Systemintegratoren, die Rollen welche die Dürr Austria GmbH einnimmt, von Bedeutung sind.

Weiters können noch einige ergänzenden Normen betrachtet werden. Zum einen ist die ISO/IEC 15408 für den Anwendungsbereich von Interesse, zum anderen ist eine vollumfängliche Evaluierung der NIST SP 800-82 eine Bereicherung. Mit diesen kann das von der Dürr Austria GmbH verwendete Security-Konzept erweitert und die OT-Security-Maßnahmen weiter ausgebaut werden.

Zur Finalisierung der Ergebnisse müssen diese noch in den Unternehmensstandard integriert werden. Dafür wurde bereits die notwendige Struktur geschaffen.

Abschließend bleibt zu erwähnen, dass die relevanten Teile der IEC 62443 evaluiert, ergänzende Normen gefunden und mit den definierten Umsetzungsmöglichkeiten die OT-Security optimiert wurde. Damit wurde die Zielsetzung eines einheitlichen Gesamtbildes zur OT-Security in Tunnelsteuerungssystemen erreicht. Der Handlungsbedarf bezüglich der Cybersecurity und generell der OT-Security in Tunnelsteuerungssystemen ist derzeit somit gedeckt.

LITERATURVERZEICHNIS

Gedruckte Werke (9)

Bundesamt für Sicherheit in der Informationstechnik (2021b): *Schichtenmodell und Modellierung*, in: (Hrsg.): *IT-Grundschutz-Kompendium*, Reguvis Fachmedien GmbH, Bundesamt für Sicherheit in der Informationstechnik, Bonn, S. 1 – 6

Bundesamt für Sicherheit in der Informationstechnik (2021a): *IT-Grundschutz – Basis für Informationssicherheit*, in: (Hrsg.): *IT-Grundschutz-Kompendium*, Reguvis Fachmedien GmbH, Bundesamt für Sicherheit in der Informationstechnik, Bonn, S. 1 – 8

ClydeBank Technology (Hrsg.) (2016): *ITIL For Beginners – The Complete Beginner's Guide to ITIL*, 2. Auflage, ClydeBank Media LLC, Albany, NY

Agutter, Claire (2020): *ITIL 4 Essentials – Your essential guide for the ITIL 4 Foundation exam and beyond*, 2. Auflage, IT Governance Publishing, Cambridgeshire, UK

Andelfinger, Volker; Hänisch, Till (2017): *Industrie 4.0 – Wie cyber-physische Systeme die Arbeitswelt verändern*, Springer Gabler, Wiesbaden

Awad, Ali; Fairhurst, Michael (2018): *Information Security: Foundations, technologies and applications*, London, UK

Eigner, Martin; Gilz, Torsten; Gerhardt, Florian; Nem, Fabrice (2012): *Informationstechnologie für Ingenieure*, Springer, Berlin Heidelberg

Hanschke, Inge (2020): *Informationssicherheit und Datenschutz – einfach & effektiv*, Hanser Verlag, München

Kofler, Michael; Zingsheim, André; Gebeshuber, Klaus; Kania, Stefan; Widl, Markus; Kloep, Peter; Aigner, Roland; Hackner, Thomas; Neugebauer, Frank (2020): *Hacking & Security – Das umfassende Handbuch*, 2. Auflage, Rheinwerk Verlag, Bonn

Matt, Dominik; Modrák, Vladimír; Zsifkovits, Helmut (2020): *Industry 4.0 for SMEs – Challenges, Opportunities and Requirements*, Springer Nature Switzerland AG, Cham

Reiss, Manuela; Reiss, Georg (2019): *Praxisbuch IT-Dokumentation*, 3 Auflage, Hanser Verlag, München

Wissenschaftliche Artikel (7)

Dolan, Bob (2018): *Cyber Security & Its Impact on Operational Technologies*, in: Network Security, 48/2018, BNP Media, S. 83 – 86

Euchner, Jim (2018): *The Internet of Things*, in: Research-Technology Management, 61/2018, S. 10 – 11

Fretty, Peter (2020): *IT/OT Convergence is Here, But Are You SECURE?*, in: Industry week, 269/2020, Penton Media, Inc., Penton Business Media, Inc. and their subsidiarie, S. 21 – 23

Gershenfeld, Neil; Euchner, Jim (2015): *Atoms and Bits: Rethinking Manufacturing*, in: Research-Technology Management, 58/2015, S. 16 – 23

Ku, Jesse (2021): *How to ensure OT cybersecurity: Despite advances, operational technology network cybersecurity still lags information technology cybersecurity*, in: Plant engineering, 75/2021, CFE Media LLC, S. 26 – 28

Seetharaman, A.; Patwa, Nitin; Saravanan, A.S.; Sharma, Abhishek (2019): *Customer expectation from Industrial Internet of Things (IIOT)*, in: Journal of Manufacturing Technology Management, 30/2019, Emerald Publishing Limited, S. 1161 – 1178

Seiden, Steven; Johnson, Leighton; Barber, Tony; Campara, Djenana (2020): *Cybersecurity, IT and OT: Information technology strategies can help combat new cybersecurity vulnerabilities and deploy a solid cybersecurity program for operational technology use for industrial control systems, RTUs and SCADA, as IIoT deployments incre*, in: Control Engineering, 67/2020, CFE Media LLL, S. 22 – 24

Online-Quellen (33)

Center for Internet Security (2021): *CIS Controls Version 8*
https://www.cisecurity.org/controls/v8/ [Stand: 25.11.2021]

ISACA (2018): *COBIT 2019 Framework – Introduction and Methodology*
https://www.isaca.org/resources/cobit [Stand: 25.11.2021]

Dürr Austria GmbH 1 (2021): *Dürr Austria GmbH*
https://www.duerr-gruppe.at/de/ [Stand: 25.11.2021]

Dürr Austria GmbH 2 (2021): *Dürr Austria GmbH – Firmenphilosophie*
https://www.duerr-gruppe.at/de/firmenphilosophie.html [Stand: 25.11.2021]

Republik Österreich – Parlamentsdirektion (2018): *Erläuterungen NISG*
https://www.bundeskanzleramt.gv.at/dam/jcr:24b93885-8b30-4770-8782-c20453591f7d/Erlaueterungen-NISG.pdf [Stand: 25.11.2021]

ComputerWeekly.de (2020): *ICS Security (Industrial Control System Security)*
https://www.computerweekly.com/de/definition/ICS-Security-Industrial-Control-System-Security [Stand: 25.11.2021]

IEC (2021): *IEC TR 62443-3-1:2009*
https://webstore.iec.ch/publication/7031 [Stand: 25.11.2021]

Indu-Sol GmbH (2021): *IIT – Industrial Information Technology*
https://www.indu-sol.com/support/glossar/iit-industrial-information-technology/ [Stand: 25.11.2021]

Frontier Computer Corp. (2021): *Industrial Internet of Things*
https://www.frontiercomputercorp.com/industrial-iot/ [Stand: 25.11.2021]

Logicalis Group (2021): *Industrial Internet of Things (IIoT) – Was ist das?*
https://www.de.logicalis.com/iiot-was-ist-das/ [Stand: 25.11.2021]

Gartner, Inc. (2021): *Operational Technology (OT)*
https://www.gartner.com/en/information-technology/glossary/operational-technology-ot [Stand: 25.11.2021]

ISA Global Cybersecurity Alliance (2020): *Quick Start Guide: An Overview of ISA/IEC 62443 Standards* https://gca.isa.org/isagca-quick-start-guide-62443-standards [Stand: 25.11.2021]

IEC (2021): *Understanding IEC 62443* https://www.iec.ch/blog/understanding-iec-62443 [Stand: 25.11.2021]

TKmag (2021): *Was ist OT? – OT-Netzwerke in der Praxis* https://www.thomas-krenn.com/de/tkmag/expertentipps/was-ist-ot/ [Stand: 25.11.2021]

Infradata Inc. (2019): *What is OT Security? Operational Technology Security explained and explored* https://www.infradata.com/resources/what-is-ot-security/ [Stand: 25.11.2021]

Securicon Team (2019): *What's the Difference Between OT, ICS, SCADA and DCS?* https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/ [Stand: 25.11.2021]

Abercrombie, Katherine (2019): *ICS Security – IT vs OT* https://www.contextis.com/en/blog/ics-security-it-vs-ot [Stand: 25.11.2021]

Antova, Galina (2021): *IT/OT-Konvergenz: Es wächst zusammen, was (nicht) zusammengehört* https://www.it-daily.net/it-sicherheit/cloud-security/28429-it-ot-konvergenz-es-waechst-zusammen-was-nicht-zusammengehoert [Stand: 25.11.2021]

Beeson, Richard (2020): *Die Kluft zwischen IT und OT* https://www.computerweekly.com/de/meinung/Die-Kluft-zwischen-IT-und-OT [Stand: 25.11.2021]

Bendel, Oliver (2021): *Cyberphysische Systeme – Definition: Was ist "Cyberphysische Systeme"?* https://wirtschaftslexikon.gabler.de/definition/cyber-physische-systeme-54077/version-384624 [Stand: 25.11.2021]

Breuss, Thomas; Lukac, Drazen; Tonweber, Gottfried; Weissmann, Benjamin (2021): *Wird die coronabedingt Digitalisierung zum Brandbeschleuniger für Cyberkriminalität?* https://www.ey.com/de_at/cybersecurity/wird-die-coronabedingte-digitalisierung-zum-brandbeschleuniger-fur-cyberkriminalitat [Stand: 25.11.2021]

Buchy, Jackie (2016): *Cyber Security vs IT Security: Is There a Difference?* https://business.gmu.edu/blog/tech/2016/06/30/cyber-securit-it-security-difference/ [Stand: 25.11.2021]

Huber, Walter (2021): *Industrie 4.0 – So unterscheiden sich IT und OT* https://www.channelpartner.de/a/so-unterscheiden-sich-it-und-ot,3335362 [Stand: 25.11.2021]

Lachenmaier, Jens; Kemper, Hans-Georg (2020): *Informationstechnologie (IT)* https://www.gabler-banklexikon.de/definition/informationstechnologie-it-58827/version-377520 [Stand: 25.11.2021]

Luber, Stefan; Litzel, Nico (2017): *Was ist das Industrial Internet of Things (IIoT)?* https://www.bigdata-insider.de/was-ist-das-industrial-internet-of-things-iiot-a-654986/ [Stand: 25.11.2021]

Mullane, Michael (2021): *Schutz der IT- und OT-Versorgungsketten mit internationalen Normen und Konformitätsbewertung* https://www.dke.de/de/arbeitsfelder/industry/news/schutz-der-it-und-ot-versorgungsketten [Stand: 25.11.2021]

Nolle, Tom (2019): *IT/OT-Konvergenz: Die besten Strategien im Detail* https://www.computerweekly.com/de/ratgeber/IT-OT-Konvergenz-Die-besten-Strategien-im-Detail [Stand: 25.11.2021]

Österreichs Energie; BDEW (2018): *Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme* https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf [Stand: 25.11.2021]

Ramos, Jaime (2021): *What is the Internet of Things or IOT? Definition and Examples* https://tomorrow.city/a/what-is-the-internet-of-things-or-iot-definition-and-examples [Stand: 25.11.2021]

Rohr, Sebastian; Juschkat, Katharina (2021): *Grundlagen Industrial IT Security – Aufbau, Definitionen, Umsetzung* https://www.elektrotechnik.vogel.de/grundlagen-industrial-it-security-aufbau-definitionen-umsetzung-a-838961/?r=ext [Stand: 25.11.2021]

Siriu, Stefanie (2021): *Was ist Informationssicherheit – eine Definition* https://www.haufe.de/compliance/management-praxis/informationssicherheit/was-ist-informationssicherheit-eine-defintion_230130_483132.html [Stand: 25.11.2021]

Springer, Matthias (2016): *Was ist der Unterschied zwischen Safety und Security?* https://www.tuev-nord.de/explore/de/erklaert/was-ist-der-unterschied-zwischen-safety-und-security/ [Stand: 25.11.2021]

Wege, Oliver; Porwitzki, Doris (2020): *Industrial Control System* https://www.secupedia.info/wiki/Industrial_Control_System [Stand: 25.11.2021]

Normen, Gesetze und Sonstiges (16)

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2020): *EN ISO/IEC 15408-1: Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 1: Einführung und allgemeines Modell*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2020): *EN ISO/IEC 15408-2: Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 2: Sicherheitsfunktionskomponenten*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2021): *EN ISO/IEC 15408-3: Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 3: Komponenten zur Sicherheitskontrolle*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2020): *EN ISO/IEC 27000: Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2017): *EN ISO/IEC 27001: Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2017): *EN ISO/IEC 27002: Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen*

Limes Security (Hrsg.) (2021): *ICS.201: OT Security Foundation Training*

Bundeskanzleramt Österreich (Hrsg.) (2021): *Netz- und Informationssystemsicherheitsgesetz – NISG: Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen*

National Institute of Standards and Technology (Hrsg.) (2018): *NIST Cybersecurity Framework: Framework for Improving Critical Infrastructure Cybersecurity*

National Institute of Standards and Technology (Hrsg.) (2015): *NIST SP 800.82 Rev. 2: Guide To Industrial Control Systems (ICS) Security*

National Institute of Standards and Technology (Hrsg.) (2018): *NIST SP 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2019): *OVE EN IEC 62443-2-1: Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2020): *OVE EN IEC 62443-2-4: IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2020): *OVE EN IEC 62443-3-3: Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2018): *OVE EN IEC 62443-4-1: IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*

OVE Österreichischer Verband für Elektrotechnik (Hrsg.) (2020): *OVE EN IEC 62443-4-2: IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

AD	Active Directory
AG	Auftraggeber
AP	Access-Point
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BS	Betriebsstation
BSI	Bundesamt für Sicherheit in der Informationstechnik
BST	Bedienstation
BZ	Betriebszentrale
CIS	Center for Internet Security
CMMI	Capability Maturity Model Integration
CPS	Cyber Physical Systems, Cyberphysische Systeme
CVE	Common Vulnerabilities and Exposures
DB-Server	Datenbankserver
DC	Data Confidentiality, Vertraulichkeit der Daten
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service
DoS	Denial of Service
EGIT	Enterprise Governance of Information and Technology
EN	Elektro-Nische, E-Nische
EQ	Befahrbarer Querschlag
FR	Foundational Requirements, Basisanforderungen, Grundlegende Anforderungen
GQ	Begehbarer Querschlag
HCI	Hyperconverged Infrastructure
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAC	Identification and Access Control, Identifizierung und Authentifizierung
IACS	Industrial Automation and Control Systems

IBK	Intelligente Busklemme
ICS	Industrial Control Systems, Industrielle Steuerungssysteme
IDE	Integrated Development Environment
IG	Implementation Group
IIoT	Industrial Internet of Things, Industrielles Internet der Dinge
IIT	Industrial Information Technology, Industrial IT, Industrielle IT, Industrielle Informationstechnologie, Industrielle IT
IoT	Internet of Things, Internet der Dinge
IPC	Industrie-PC
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
IT	Information Technology, Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITSM	IT-Service-Management
KAV	Kaverne
LN	Lüfter-Nische
LStE	Lokale Steuereinheit
NISG	Netz- und Informationssystemsicherheits-Gesetz, NIS-Gesetz
NIST	National Institute of Standards and Technology
NRN	Notruf-Nische
NTP	Network Time Protocol
OT	Operational Technology, Betriebstechnologie
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller, Speicherprogrammierbare Steuerung
PP	Protection Profile, Schutzprofile
RA	Resource Availability, Verfügbarkeit der Ressourcen
RDF	Restricted Data Flow, Eingeschränkter Datenfluss
RE	Requirement Enhancements, Weitergehende Anforderungen
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SI	System Integrity, Systemintegrität

SL	Security Level, Security-Level, Sicherheitslevel
SL-A	Achieved Security Levels, Tatsächlich erreichte Security-Levels
SL-C	Capability Security Levels, Erreichbare Security-Levels
SL-T	Target Security Levels, Zu erreichende Security-Levels
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SPS	Speicherprogrammierbare Steuerung, Programmable Logic Controller
SR	System Requirements, Systemanforderungen
ST	Security Target, Sicherheitsvorgaben
TOE	Target of Evaluation, Evaluierungsgegenstand
TP	Touchpanel
TRE	Timely Response to Events, Rechtzeitige Reaktion auf Ereignisse
Tuko	Tunnelkopfrechner
UC	Use Control, Nutzungskontrolle
VDI	Virtuelle Desktopinfrastruktur
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WSUS	Windows Server Update Services