Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) für die Fernwärme- und Fernkälteversorgung

F1001 d Ausgabe Februar 2023

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
Bundesamt für wirtschaftliche Landesversorgung BWL

Thermische Netze
Réseaux Thermiques
Reti Termiche

SVGW
SSIGE

Zusammenfassung

Die zunehmende Durchdringung und Vernetzung der Informations- und Kommunikationstechnologie (IKT) eröffnet unverzichtbare ökonomische wie auch gesellschaftliche Potenziale. Durch die fortschreitende Digitalisierung entstehen jedoch neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss. Die Cyber-Sicherheit der kritischen Infrastrukturen eines Landes ist von höchster Wichtigkeit. Daher müssen diese Infrastrukturen angemessen geschützt werden, wobei es den entsprechenden IKT-Systemen besondere Beachtung zu schenken gilt.

In der Branche der thermischen Netze[1], die die Fernwärme- und Fernkälteversorgung umfasst, werden die meisten operativen Vorgänge durch ein industrielles Kontrollsystem (ICS)[2] gesteuert. Es besteht aus mehreren Steuerkomponenten, die zur Erreichung eines gemeinsamen Ziels zusammenwirken. Aufgabe dieses Systems ist es, Daten von variablen Prozessen oder den Zustand von Industriemaschinen zu erfassen und diese Maschinen vor Ort oder aus der Ferne zu steuern und zu überwachen. Somit kommt diesem System eine zentrale Bedeutung zu. Es erlaubt, alle Aufgaben von Industrieanlagen zu steuern, weshalb es unbedingt gegen Cyber-Bedrohungen und Datendiebstahl geschützt werden muss.

Eine wirksame Bewältigung der Cyber-Sicherheitsprobleme erfordert ein klares Verständnis der aktuellen Sicherheitsherausforderungen sowie der verfügbaren Gegenmassnahmen. Der vorliegende IKT-Minimalstandard bietet ein Rahmenwerk, dank dem sich die Organisationen in der Branche der thermischen Netze nicht nur gegen Angriffe sowie Fehlmanipulationen schützen können, sondern der es ihnen auch erlaubt, sich nach einem Vorfall möglichst rasch wieder zu erholen. Innerhalb dieses Sicherheitsrahmens stufen Unternehmen ihr Risiko selbstständig ein und setzen geeignete Massnahmen um.

Der IKT-Minimalstandard stützt sich hauptsächlich auf das Cyber-Sicherheitsprogramm NIST Framework Core.[3] Dies garantiert ein wirksames Schutzverfahren und ermöglicht den verschiedenen Wirtschaftsbranchen den Einsatz eines Cyber-Sicherheitsprogramms mit vergleichbaren, kohärenten Ergebnissen. Damit beruhen der IKT-Minimalstandard des Bundesamtes für wirtschaftliche Landesversorgung BWL und die verschiedenen branchenspezifischen Versionen davon auf denselben Massnahmen. Dank dieses einheitlichen Vorgehens können Unternehmen, die in verschiedenen Bereichen (z. B. Strom[4], Trinkwasser[5], Erdgas[6], thermische Netze) tätig sind, ein gemeinsames Cyber-Sicherheitsprogramm verwenden.

Das vorliegende Dokument ist in sieben Kapitel unterteilt. Kapitel 1 enthält eine Einführung in den Minimalstandard und die Branche der thermischen Netze als kritische Infrastruktur für die Landesversorgung. In Kapitel 2, das sich auf die Branche der thermischen Netze konzentriert, werden die Struktur der Branche sowie deren IKT-Prozesse erläutert und kritische Aktivitäten evaluiert. Kapitel 3 befasst sich mit den besonderen Bedürfnissen und Anforderungen eines ICS. In den Kapiteln 4 und 5 werden die verschiedenen Teile des Cyber-Sicherheitsprogramms des IKT-Minimalstandards im Einzelnen aufgeführt, darunter das Risikomanagement, die Defense-in-depth-Strategie und die Cyber-Sicherheitsmassnahmen des NIST Framework Core. Den Abschluss bilden die Kapitel 6 und 7 mit den Schlussfolgerungen und den Anhängen.

[1] In diesem Dokument bezieht sich der Begriff «thermische Netze» stets auf die Fernwärme- und Fernkälteversorgung.

[2] ICS: Industrial Control System (industrielles Kontrollsystem). Weitere Informationen hierzu in Kapitel 3.1.

[3] In den USA entwickelter Verfahrensrahmen zur Unterstützung öffentlicher und privater Organisationen bei der Verbesserung ihrer Cyber-Sicherheit. Der Rahmen umfasst fünf Funktionen: Identifizieren (Identify), Schützen (Protect), Erkennen (Detect), Reagieren (Respond) und Wiederherstellen (Recover). Weitere Informationen hierzu in den Kapiteln 4 und 5.

[4] Handbuch Grundschutz für «Operational Technology» in der Stromversorgung. Verband der Schweizer Elektrizitätsunternehmen (VSE), Aarau 2018.

[5] Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Wasserversorgung. Schweizerischer Verein des Gas- und Wasserfaches (SVGW), Zürich 2019.

[6] Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Gasversorgung. Schweizerischer Verein des Gas- und Wasserfaches (SVGW), Zürich 2020.

Inhaltsverzeichnis

1 Einführung

1.1 Hintergrund und Überblick

Die Wirtschaftliche Landesversorgung (WL) bzw. das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat sich im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)[7] mit der Verwundbarkeit der IKT-Systeme befasst, die zur Sicherstellung der Versorgung thermischer Netze erforderlich sind. Ziel war die Einführung eines Minimalstandards für die IKT-Sicherheit, dank dem sich die Organisationen dieser Branche angemessen gegen mögliche Cyber-Risiken schützen können.

In der Schweiz besteht die Hauptaufgabe der Branche der thermischen Netze (Fernwärme- und Fernkälteversorgung) in der Beheizung von Gebäuden, der Bereitstellung von Brauchwarmwasser sowie der Wärmeerzeugung für die Industriesektoren. Die Branche ist sehr heterogen. Sie setzt sich aus einer Vielzahl von Akteuren zusammen, die zur Wärmeerzeugung unter schiedliche Energiequellen und industrielle Prozesse nutzen. Diverse Expertenberichte[8] kommen zum Schluss, dass die Branche von den neuen energiepolitischen Entscheiden des Landes profitieren wird. Es darf daher von einer Erhöhung der Produktion und einer Ausweitung der thermischen Netze ausgegangen werden. Sollte die Branche in den nächsten Jahren tatsächlich expandieren, wäre eine Störung mit negativen Auswirkungen auf die entsprechenden Infrastrukturen für die Landesversorgung umso bedenklicher. Daher muss die Branche angemessen gegen entsprechende Risiken geschützt werden.

Unternehmen, die im Bereich der thermischen Netze tätig sind, verwenden täglich IKT-Systeme, um ihre Aufgaben zu erfüllen. Zur Steuerung ihrer industriellen Aktivitäten bedienen sie sich eines industriellen Kontrollsystems (Industrial Control System, ICS). Das wichtigste ICS ist das Leitsystem, das ein zentrales Element der Automatisierungspyramide darstellt (siehe Kapitel 2.4.2). Das Leitsystem ermöglicht die Zentralisierung der Erfassung, Überwachung, Kontrolle und Verarbeitung von Daten und stellt eine wesentliche Komponente im Betriebsablauf eines Unternehmens dar, da es ihm die Steuerung seiner Industrieanlagen im Zusammenhang mit der Produktion, dem Transport und dem Verbrauch von Wärme erlaubt. IKT-Systeme werden von den Unternehmen auch zur Erledigung verschiedener organisatorischer Aufgaben im Tagesgeschäft bzw. in der Verwaltung genutzt. Dabei handelt es sich um Telekommunikationsinfrastrukturen, Kommunikationsdienste und integrierte Managementsysteme (ERP). Eine IKT-Störung an einem der in diesem Absatz beschriebenen Elemente kann das betreffende Unternehmen ganz oder teilweise lahmlegen und so die Wärmeversorgung des Landes und seiner Bevölkerung erschweren.

Basierend auf verschiedenen IKT-Verwundbarkeitsanalysen und anderen technischen Dokumenten[9] liefert der vorliegende Minimalstandard Empfehlungen zur Erhöhung des Sicherheitsniveaus der IKT bei allen Akteuren der Branche der thermischen Netze. So soll ein akzeptables Schutzniveau erreicht werden, damit die Unternehmen einem Ausfall ihrer IKT-Systeme nicht vollkommen hilflos ausgeliefert sind. Daher wird den Unternehmen nahegelegt, den IKT-Minimalstandard unter Berücksichtigung der in Kapitel 2 genannten kritischen Aktivitäten umzusetzen, das Maturitätsniveau ihrer IKT-Systeme anhand des Assessment Tools in Kapitel 5 zu bestimmen und die Sicherheit der im Rahmen der Beurteilung als ungenügend erachteten IKT-Systeme zu verbessern.

[7] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken. Informatiksteuerungsorgan des Bundes (ISB), Bern 2018.

[8] Insbesondere zu nennen sind in diesem Zusammenhang:

- *Leitfaden Fernwärme/Fernkälte. Verband Fernwärme Schweiz, Bern 2020.*
- *Faktenblatt Thermische Netze. EnergieSchweiz, Bundesamt für Energie BFE, Ittigen 2021.*

[9] Als Grundlage für den vorliegenden IKT-Minimalstandard wurden insbesondere die folgenden vier Dokumente verwendet:

- *IKT-Minimalstandard – Wirtschaftliche Landesversorgung. Bundesamt für wirtschaftliche Landesversorgung, Bern 2018.*
- *Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology (NIST), USA 2014.*
- *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Department of Homeland Security (DHS) und Industrial Control Systems Cyber Emergency Response Team (NCCIC), USA 2016.*
- *Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU). Information Security Society Switzerland (ISSS), Bern 2016.*

Das Bundesgesetz über die wirtschaftliche Landesversorgung (LVG; SR 531) überträgt dem Bundesrat die Kompetenz, vorsorgliche Massnahmen zur Förderung der Resilienz (Widerstandsfähigkeit) der für unser Land essenziellen Versorgungsprozesse umzusetzen. Dieser IKT-Minimalstandard ist eine solche Resilienzmassnahme, die jedoch von der Branche freiwillig übernommen werden kann. Thermische Netze Schweiz (TNS) – vormals Verband Fernwärme Schweiz (VFS) – und der Schweizerische Verein des Gas- und Wasserfaches (SVGW) empfehlen ihren Mitgliedern, den IKT-Minimalstandard für die Versorgung thermischer Netze in seiner Gesamtheit umzusetzen.

1.2 Ausgangslage und Zielsetzung

Die Branche der thermischen Netze ist wie die meisten anderen Industriebereiche erwiesenermassen von IKT-Systemen abhängig. Die fortschreitende Digitalisierung ermöglicht zwar Effizienzgewinne, erhöht aber auch die Komplexität des Versorgungsprozesses. Der Ausfall kritischer IKT-Systeme kann somit gravierende Folgen für den reibungslosen Betrieb der thermischen Netze in der Schweiz haben und folglich die Wärmeversorgung des Landes direkt beeinträchtigen.

Diese vom BWL, von TNS und vom SVGW erstellte Empfehlung setzt das Cyber-Sicherheitsprogramm NIST Framework Core um. Dieses stützt sich auf zwei kombinierte, auf dem Risikomanagement und der Defense-in-depth-Strategie beruhende Konzepte. Die Analyse eines akzeptablen Risikos ist für eine Organisation von entscheidender Bedeutung, da ihr dies ermöglicht, die Kernmassnahmen des NIST Framework Core an ihre eigenen Bedürfnisse anzupassen (je nach Branche, Grösse, Ressourcen und Bedrohungen). Bei der Defense-in-depth-Strategie wiederum handelt es sich um einen vom militärischen Prinzip abgeleiteten Ansatz, wonach ein komplexes vielschichtiges Verteidigungssystem schwieriger zu überwinden ist als eine einfache Barriere. Ziel dieser Strategie ist es daher, mehrere Sicherheitsmassnahmen auf unterschiedlichen Schutzniveaus anzuwenden (die z. B. vom Netzwerkschutz über den Schutz physischer Elemente bis hin zur Ausbildung des Personals reichen) und so potenzielle Angreiferinnen und Angreifer zur Überwindung einer Vielzahl komplexer Sicherheitshindernisse zu zwingen.

Mithilfe dieses Cyber-Sicherheitsprogramms soll die Resilienz der Organisationen in der Branche der thermischen Netze gegenüber IKT-Bedrohungen verbessert und letztlich die Sicherheit dieser Branche insgesamt erhöht werden, um einen funktionierenden Versorgungsprozess sicherzustellen. In diesem Zusammenhang werden IKT-Bedrohungen umfassend verstanden: von physischer Beschädigung über den Verlust oder die Manipulation von Daten bis hin zu Cyber-Angriffen in zerstörerischer Absicht. Dieser IKT-Minimalstandard umfasst neben technischen Massnahmen auch die Ausbildung und Schulung der Mitarbeitenden sowie die Governance, um die Resilienz von wichtigen IKT-Systemen zu verbessern. Dazu wird ein mehrschichtiger Ansatz empfohlen, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen:

- **Verfügbarkeit:** Gewährleisten, dass Informationen zum Zeitpunkt des Bedarfs verfügbar sind. Dies setzt voraus, dass die Systeme zur Verarbeitung und Übertragung einsatzfähig und verfügbar sind.
- **Integrität:** Gewährleisten, dass Informationen jederzeit vollständig und korrekt sind.
- **Vertraulichkeit:** Gewährleisten, dass Informationen ausschliesslich berechtigten Personen bzw. Systemen zugänglich sind.

1.3 Geltungsbereich und Abgrenzungen

Der vorliegende IKT-Minimalstandard konzentriert sich auf den Schutz der IKT-Systeme, die für den reibungslosen Betrieb der thermischen Netze in der Schweiz erforderlich sind. So soll sichergestellt werden, dass allfällige Störungen den Versorgungsprozess der thermischen Netze sowie die Wärmeversorgung der Schweiz nicht übermässig beeinträchtigen. Der Umfang dieses Minimalstandards ist wie folgt definiert:

Geltungsbereich

- Der IKT-Minimalstandard schliesst alle Informations- und Kommunikationstechnologien ein, die für den Betrieb der Systeme und der Infrastruktur der thermischen Netze (z. B. Energiezentralen, Fernleitungen, Unterstationen usw.) notwendig sind.
- Die Resilienz der Systeme soll branchenweit verbessert werden. Das angestrebte minimale Schutzniveau soll verhindern, dass der Versorgungsprozess der thermischen Netze sowie die Wärmeversorgung des Landes durch einen Cyber-Vorfall massgeblich gestört werden.

- Der vorliegende Standard konzentriert sich auf industrielle Kontrollsysteme (ICS), integrierte Managementsoftware (ERP)[10], Kommunikationsmittel und alle IKT-Systeme zur Steuerung der Anlagen. Hierunter fallen unter anderem Laptops und Desktop-Computer, Telefone, Instandhaltungssoftware, Schnittstellen zu SCADA-Systemen[11], Drucker, Smart Metering, angeschlossene Geräte (Internet of Things) sowie Netzwerke und Systeme in Unternehmen.
- Dieser Standard richtet sich an alle Schweizer Unternehmen, die in der Branche der thermischen Netze tätig sind. Die Umsetzung kann je nach den verfügbaren Ressourcen intern durch die eigenen Mitarbeitenden oder extern durch ein spezialisiertes Beratungsunternehmen erfolgen.

Abgrenzungen

- Nicht untersucht wurde die Fähigkeit der Unternehmen, die eigene Infrastruktur auch ohne IKT-Systeme im «manuellen Betrieb» aufrechtzuerhalten. Trotzdem wird an dieser Stelle empfohlen, diese Möglichkeit zu erhalten oder (erneut) zu schaffen, falls es die Umstände erlauben. Der manuelle Betrieb ist essenziell für kritische Infrastrukturen – zumindest das geordnete Abschalten der Infrastruktur sollte zu jeder Zeit noch möglich sein.
- Die Stromversorgung ist nicht Teil dieses IKT-Minimalstandards. Trotzdem wird ein Notkonzept zum Umgang mit Stromversorgungsengpässen oder einem allgemeinen Stromausfall (Blackout) für jede Infrastruktureinrichtung empfohlen. Es besteht eine grosse Abhängigkeit von der Stromversorgung. Ohne Strom könnten die IKT-Systeme und die von ihnen abhängigen Funktionen (z. B. Steuerung der Wärmeproduktionseinheiten, Kontrolle von Druck- oder Temperaturniveaus, Betrieb des Alarmsystems) nur manuell unter Einsatz umfangreicher personeller Ressourcen ausgeführt werden, sofern sich die betreffende Funktion ohne IKT-System überhaupt ausführen lässt.

[10] Enterprise-Resource-Planning-System (ERP-System): Dieses System ist eine komplexe Anwendung oder eine Vielzahl miteinander kommunizierender Anwendungssoftware- bzw. IT-Systeme, die zur Unterstützung der Ressourcenplanung des gesamten Unternehmens eingesetzt werden.

[11] SCADA: Supervisory Control and Data Acquisition (System zur Überwachung und Steuerung technischer Prozesse).

[12] Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in Abfallverwertungsanlagen. Verband der Betreiber Schweizerischer Abfallverwertungsanlagen (VBSA), Bundesamt für wirtschaftliche Landesversorgung (BWL), Schweiz 2022.

- Dieser Standard konzentriert sich ausschliesslich auf die Branche der thermischen Netze. Die Unternehmen dieser Branche, die vom industriellen Prozess der Abwärmenutzung Gebrauch machen, produzieren die Wärme jedoch nicht selbst. Daraus resultiert ein Abhängigkeitsverhältnis zwischen dem wärmeerzeugenden Betrieb und dem Unternehmen, das für die aufnehmenden thermischen Netze verantwortlich ist. Deswegen muss der gesamte Versorgungsprozess geschützt werden und nicht nur der Prozessbestandteil «thermische Netze». Für einen angemessenen Schutz des Gesamtprozesses wird empfohlen, die spezifischen Dokumente der verschiedenen Branchen heranzuziehen – wie zum Beispiel den IKT-Minimalstandard für die Abfallentsorgung[12], sollte die Abwärme durch eine Kehrichtverwertungsanlage (KVA) erzeugt werden. Weitere Informationen über die Abwärmenutzung sind in Kapitel 2.4.5.8. zu finden.
- Massnahmen zur Arbeitssicherheit sind nicht Bestandteil dieser Branchenempfehlung.

1.4 Notwendigkeit eines IKT-Minimalstandards

Dank der Entwicklungen im Bereich der digitalen Technologien lassen sich die IKT-Systeme zwar verbessern. Gleichzeitig entwickeln sich aber auch die Cyber-Bedrohungen weiter, was eine zunehmende Belastung für alle Unternehmen darstellt. Cyber-Angriffe hängen nicht von der Grösse oder Bedeutung eines Unternehmens ab; sie sind häufig sogar zufällig oder geschehen, weil sich günstige Gelegenheiten bieten. Aufgrund der fortschreitenden Digitalisierung werden solche Situationen immer häufiger auftreten.

Einige Unternehmen mit Verantwortung für thermische Netze schotten ihr industrielles Kontrollsystem (ICS) nicht richtig von der übrigen Geschäftstätigkeit ab. Dies kann zu neuen Verwundbarkeiten führen, die von Hackern ausgenutzt werden, um z. B. Daten zu stehlen, fremde IKT-Ressourcen zu nutzen oder die Kontrolle über industrielle Anlagen zu übernehmen. So kann es bei Angriffen mit Ransomware zur Verschlüsselung eines Teils oder aller IKT-Systeme eines Unternehmens kommen. Ein Zugriff auf die Daten ist dann erst wieder nach Zahlung des geforderten Lösegelds oder nach Wiederinbetriebnahme der Anlagen dank unversehrter Datensicherungen (Backups) möglich. Solche Angriffe können somit hohe finanzielle und auch industrielle Schäden verursachen, wodurch je nach Bedeutung des jeweiligen Unternehmens bzw. der betreffenden Branche die Landesversorgung beeinträchtigt werden kann. Deshalb muss ein Land seine «kritischen» Infrastrukturen unbedingt schützen.

Cyber-Angriffe können jede Branche und jedes Land treffen. In der Branche der thermischen Netze und im Energiesektor ganz allgemein haben bereits diverse Unternehmen mit Cyber-Bedrohungen zu kämpfen gehabt. So legte 2016 ein DDoS-Angriff (Distributed Denial of Service)[13] auf das finnische Hausverwaltungsunternehmen Valtia, das auch für thermische Netze verantwortlich ist, die IKT-Systeme für die Wärmeversorgung zweier Wohnblocks lahm. Deren Bewohnerinnen und Bewohner mussten daraufhin mehrere Tage ohne Heizung und Warmwasser auskommen. Zum Glück erfolgte der Angriff nicht während des rauen finnischen Winters, sodass für die betroffenen Menschen keine Lebensgefahr durch Unterkühlung bestand. Letztlich war es nur ein kleinerer Zwischenfall in zwei Gebäuden. Wenn von einem solchen Ausfall bei strenger Kälte aber ganze Quartiere oder Städte betroffen sind, wären die Folgen verheerend.[14]

Ein anderer, dieses Mal gross angelegter Cyber-Angriff traf im Mai 2021 die Colonial Pipeline. Das Unternehmen betreibt eine rund 8900 Kilometer lange Ölpipeline zwischen Houston und New York. Die IKT-Systeme der Firma wurden mit Ransomware infiziert, die dafür sorgte, dass der Betrieb augenblicklich eingestellt werden musste. Dem Vernehmen nach sollen die Verantwortlichen von Colonial Pipeline 5 Millionen US-Dollar Lösegeld gezahlt haben, um ihre Daten und die Steuerung für ihre Anlagen zurückzuerhalten. Neben der Lösegeldzahlung und dem Datendiebstahl kam es zu einem fünftägigen Ausfall der Ölpipeline, wodurch sich der finanzielle Verlust des Unternehmens weiter erhöhte. Der Angriff beeinträchtigte auch die Versorgung mehrerer Regionen in den USA und führte zu einem starken Preisanstieg und zur Verknappung von Öl und Benzin. US-Präsident Biden musste die Bürgerinnen und Bürger im Südosten der USA sogar beruhigen, da sich eine Krise abzuzeichnen drohte. Weil die meisten Tankstellen wegen Versorgungsengpässen geschlossen blieben, kam es nämlich vereinzelt zu Panik in der Bevölkerung. Das zeigt anschaulich, wie eine Störung der IKT-Systeme von kritischen Infrastrukturen die Versorgung eines Landes und seiner Bevölkerung so beeinträchtigen kann, dass es in besonders drastischen Fällen zu Panikreaktionen kommen kann.[15]

Cyber-Angriffe in Industriesektoren sind immer heikel, denn es muss verhindert werden, dass Hacker die Kontrolle der operativen Systeme übernehmen, die Unternehmen für ihre industriellen Prozesse benötigen. 2021 manipulierten Hacker das industrielle Kontrollsystem (ICS) eines Wasseraufbereitungsunternehmens in Florida. Sie konnten die Kontrolle über das System übernehmen und versuchten, den Gehalt an Natriumhydroxid im Wasser um das 100-fache zu erhöhen, wodurch dieses ungeniessbar und gesundheitsschädlich geworden wäre. Der Angriff wurde zufällig entdeckt. Ein Mitarbeiter bemerkte beim Überwachen der Monitore, wie sich der Cursor der Maus von alleine bewegte und verschiedene Parameter veränderte. So konnte er schnell reagieren, den böswilligen Angriff abwehren und eine Verunreinigung des Wassers im öffentlichen Versorgungsnetz sowie eine Vergiftung der Bevölkerung verhindern.[16]

Auch in der Schweiz waren schon mehrere Unternehmen mit Cyber-Angriffen konfrontiert. An dieser Stelle seien nur einige der bekanntesten Fälle erwähnt, wie etwa der DDoS-Angriff auf die Wasserversorgung der Gemeinde Ebikon. Die Attacke scheiterte dank des einige Monate zuvor erhöhten Cyber-Sicherheitsniveaus des Versorgers.[17] Durch einen weiteren Cyber-Angriff verlor das Unternehmen Meier Tobler den Zugriff auf seine für die Administration erforderlichen IKT-Systeme. Dadurch wurde der Geschäftsbetrieb mehrere Tage lang komplett lahmgelegt, was das Unternehmen mehrere Millionen Franken kostete.[18]

[13] Bei einem solchen Angriff werden die IKT-Systeme eines Unternehmens durch eine enorme Zahl von Anfragen überlastet, bis sie diese nicht mehr verarbeiten können, wodurch der Systemzugriff blockiert wird.

[14] Forbes. «Hackers Use DDoS Attack to Cut Heat to Apartments», 7. November 2016, https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/?sh=2c8083c41a09 (Stand: 13.12.2021).

[15] BBC. «US fuel pipeline ‹paid hackers $5m in ransom›», 14. Mai 2021, https://www.bbc.com/news/business-57112371 (Stand: 13.12.2021).

[16] Zerowaterloss. «D'autres attaques en Suisse – les producteurs d'eau potable investissent dans les systèmes de sécurité», 24. März 2021 (Stand: 4.1.2022).

[17] Blick. «Hacker-Attacke auf Wasserversorgung in Ebikon LU», Artikel in der Ausgabe vom 19. Dezember 2018 (Stand: 4.1.2022).

[18] ICTjournal. «La cyberattaque coûte des millions au suisse Meier Tobler», Artikel in der Ausgabe vom 21. März 2019 (Stand: 4.1.2022).

Der RUAG wurden bei einem mehrere Monate andauernden Cyber-Spionage-Angriff grosse Mengen an sensiblen Daten gestohlen.[19] Seit Beginn der Corona-Pandemie hat sich die Situation weltweit noch verschlechtert. In der Schweiz ist die Zahl der Cyber-Angriffe deutlich gestiegen. Dem Nationalen Zentrum für Cybersicherheit (NCSC) wurden im ersten Halbjahr 2021 doppelt so viele Cyber-Attacken gemeldet wie im gleichen Vorjahreszeitraum.[20] Dieser Trend ist bei allen Arten von Cyber-Angriffen zu beobachten. Laut den Zahlen des NCSC[21] gingen die grössten Bedrohungen 2021 aus von:

- Phishing: Die Opfer werden verleitet, ihre Passwörter und weitere persönliche Informationen anzugeben.
- Fake Sextortion: Erpresser drohen mit der Veröffentlichung kompromittierender Bilder oder Informationen.
- CEO-Betrug: Hacker senden eine angeblich dringende, jedoch gefälschte Zahlungsaufforderung im Namen eines Geschäftsleitungsmitglieds, für das sie sich ausgeben und das zu diesem Zeitpunkt oft nicht erreichbar ist.
- Ransomware: Daten auf einem Gerät werden verschlüsselt und sind für deren Eigentümerinnen bzw. Eigentümer nicht mehr zugänglich.

Diese Beispiele zeigen, dass derartige Bedrohungen sehr real sind. Um solche Risiken weitestmöglich zu beschränken, müssen die für die Steuerung der thermischen Netze benötigten IKT-Systeme hohen Sicherheitsanforderungen genügen. Mit einem einheitlichen standardisierten Vorgehen im Bereich Cyber-Sicherheit können die Unternehmen ihre IKT-Systeme möglichst adäquat schützen und diesen Schutz kontinuierlich verbessern. Der vorliegende IKT-Minimalstandard gibt praktische Handlungsanweisungen für die Umsetzung dieses Cyber-Sicherheitsprogramms. Die für die thermischen Netze verantwortlichen Unternehmen sind angehalten, ihre Risiken mittels des IKT-Minimalstandards selbst zu identifizieren und ihre Risikobereitschaft selbstständig zu definieren. Sie können diesen Standard entsprechend ihrer Grösse, ihren Ressourcen und den Bedrohungen, mit denen sie konfrontiert sind, anpassen. Der geschätzte finanzielle Aufwand für die Umsetzung dieses Cyber-Sicherheitsprogramms ergibt sich aus den entsprechenden Überlegungen. Letztlich sei darauf hingewiesen, dass es in der eigenen Verantwortung der Unternehmen der Branche der thermischen Netze liegt, für einen sicheren Betrieb ihrer Anlagen zu sorgen.

1.5 Umsetzung des IKT-Minimalstandards

Der vorliegende IKT-Minimalstandard kann von allen Unternehmen der Branche der thermischen Netze in der Schweiz umgesetzt werden. TNS und der SVGW empfehlen ihren Mitgliedern, diesen IKT-Minimalstandard in seiner Gesamtheit umzusetzen. Sie sind angehalten, ihr Maturitätsniveau mithilfe des Assessment Tools zu eruieren und kontinuierlich zu verbessern. Den für grosse thermische Netze verantwortlichen Unternehmen wird nahegelegt, ein über dem empfohlenen Minimalstandard liegendes Sicherheitsniveau anzustreben.

Dieses Dokument dient als Anleitung sowie Umsetzungshilfe. Der Minimalstandard gilt dann als erreicht, wenn das «Overall Cyber Security Maturity Rating» (siehe Assessment Tool in Kapitel 5) mindestens den vorgeschriebenen Minimalwerten (des eigenen risikobasierten Ansatzes) entspricht. Cyber-Sicherheit ist kein Zustand, sondern wird als dynamischer Prozess verstanden und gelebt. Sicherheit im Umgang mit IKT kann nie erreicht werden, sondern muss ständig angestrebt und regelmässig überprüft sowie verbessert werden. Die regelmässige Überprüfung und Verbesserung hat auf Grundlage des IKT-Minimalstandards zu erfolgen.

[19] Le Temps. «La cyberattaque de RUAG a réveillé la Suisse», Artikel in der Ausgabe vom 15. Januar 2017 (Stand: 4.1.2022).

[20] RTS. «Le nombre de cyberattaques a doublé au premier semestre en Suisse», Artikel publiziert auf der Website rts.ch am 2. November 2021 (Stand: 4.1.2022).

[21] Halbjahresbericht 2021/I (Januar–Juni). Nationales Zentrum für Cybersicherheit NCSC, Bern 2021.

Das Assessment Tool ist ein Hilfsmittel zur Selbsteinschätzung und übernimmt im Wesentlichen die Anforderungen des NIST Framework Core. Es umfasst fünf Funktionen (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen). Diese sind in 23 Kategorien aufgeteilt, die sich ihrerseits wiederum in 106 Aktivitäten gliedern (siehe Abbildung 1). Vor der Beurteilung mithilfe des Assessment Tools können die Funktionen und Kategorien des Rahmens für die Cyber-Sicherheit entsprechend der Risikobereitschaft der Organisation priorisiert werden. Dazu wird im Einklang mit dem risikobasierten Ansatz jede der 5 Funktionen und 23 Kategorien mit einer Note (zwischen 0 und 4)[22] bewertet. Die Unternehmen in der Branche der thermischen Netze entscheiden, welche Funktionen und Kategorien für die Organisation besonders wichtig sind (hohe Priorität) und welche als weniger relevant eingestuft werden. Dabei orientieren sie sich an den in Kapitel 2.4 definierten kritischen Aktivitäten.

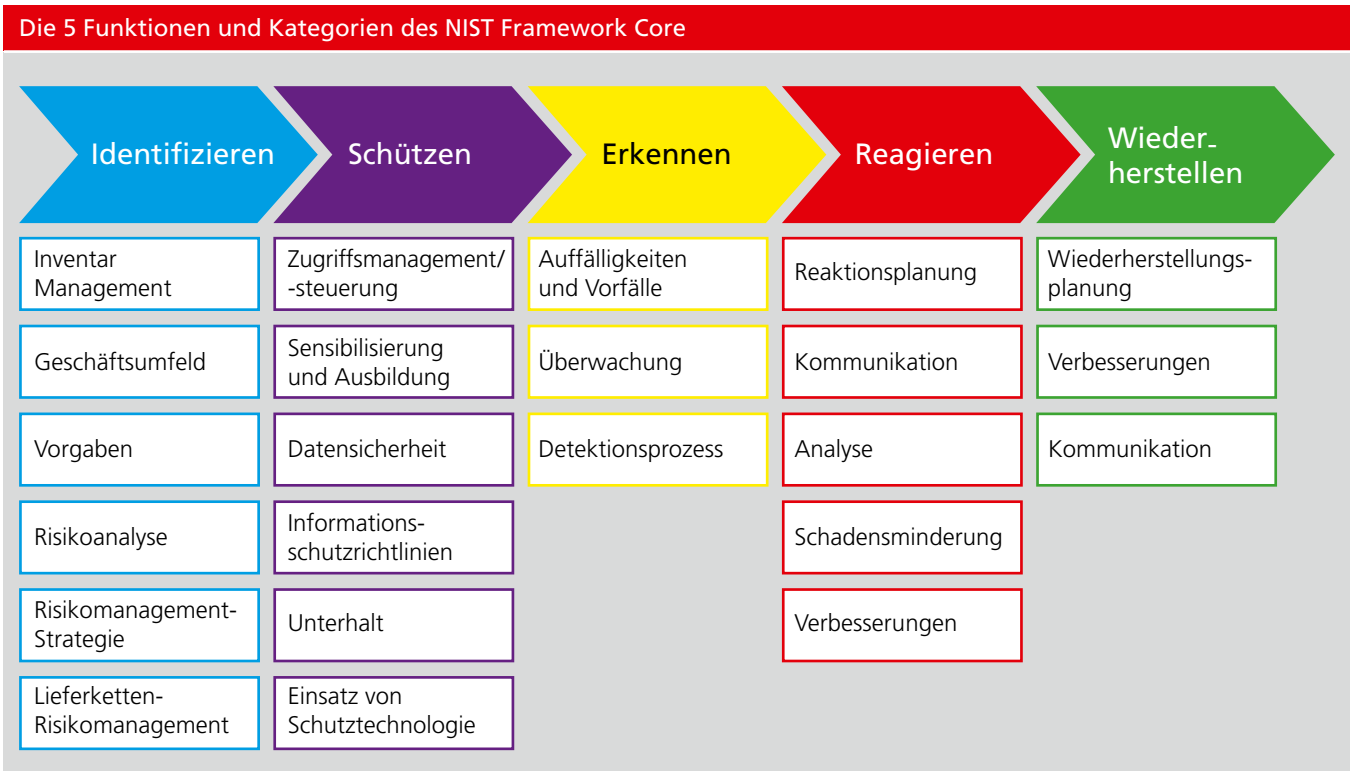

Abbildung 1: Funktionen und Kategorien des NIST Framework Core

[22] *Weitere Informationen hierzu in Kapitel 5 «Massnahmen des NIST Framework Core».*

2 Übersicht über die Branche der thermischen Netze

In diesem Kapitel werden die Marktstruktur, die Versorgungsprozesse und die kritischen Aktivitäten der Branche der thermischen Netze beschrieben. Ziel ist es, den IKT-Minimalstandard optimal auf diese Branche zuzuschneiden und die Unternehmen so in die Lage zu versetzen, bestimmte Massnahmen des Cyber-Sicherheitsprogramms je nach den verfügbaren Ressourcen, den identifizierten Bedürfnissen und den bestehenden Bedrohungen zu priorisieren.

2.1 Definition des Begriffs «thermisches Netz»

Als Einstieg in das Thema ist es wichtig, den Begriff «thermisches Netz» zu definieren. Dazu werden im Folgenden die Funktionsweise der thermischen Netze erklärt, Hintergrundinformationen geliefert, die mögliche Entwicklung dieser Netze angesichts des Wärmebedarfs in der Schweiz aufgezeigt sowie die verschiedenen Energiequellen und die industriellen Prozesse beschrieben, die in dieser Branche in diesem Zusammenhang zum Einsatz kommen.

2.1.1 Prinzip und Schweizer Kontext

Thermische Netze ermöglichen den Wärme- oder Kältetransport über grössere Entfernungen. Im Falle eines Fernwärmenetzes wird in einer oder mehreren Wärmezentralen dem Wärmeübertragungsmedium (meistens Wasser) Wärme zugeführt. Diese Wärme wird über das Netz bis zum Verbrauchsort transportiert, wo sie primär zur Gebäudebeheizung verwendet wird. Ein Fernkältenetz funktioniert nach dem gleichen Prinzip, nur dass der industrielle Prozess hier keine Wärme, sondern Kälte erzeugt. Die Netztemperatur in einem klassischen Fernwärmenetz bewegt sich zwischen 60 °C und 170 °C. Bei Temperaturen unter 60 °C spricht man von einem Niedertemperaturnetz. Ein solches wird zum Beispiel eingesetzt, um kleinere Bauten mit Temperaturen um die 30 °C zu beheizen. Liegt die vom Netz gelieferte Temperatur unter der Umgebungstemperatur, handelt es sich um ein Fernkältenetz.[23]

Vor allem im urbanen Umfeld existieren moderne thermische Netze schon seit mehreren Jahrzehnten. Praktisch alle grossen Städte in der Schweiz haben eines oder mehrere thermische Netze in Betrieb. Diese Netze wurden anfänglich mit Abwärme von Kehrichtverwertungsanlagen (KVA) versorgt. Später kamen Holzheizwerke und meist von Gewässern oder industrieller Abwärme versorgte Wärmepumpen als Wärmelieferanten dazu. Im ländlichen Raum waren thermische Netze ursprünglich auf die Versorgung mit Biomasse ausgelegt, die in diesen Regionen meist in Form von Holz und Biogas unter anderem aus Abwasserreinigungsanlagen (ARA) verfügbar ist. Die meisten thermischen Netze werden mit erneuerbaren Energien betrieben. Nicht selten sind die Anlagen aber zusätzlich mit Gas- bzw. Ölfeuerungen ausgestattet, die je nach Jahreszeit bis zu 20 Prozent der Wärme beisteuern. Diese fossilen Zusatzheizungen kommen vor allem für die Spitzenlastdeckung zum Einsatz. Sie können aber auch als redundante Systeme bei einer Störung der Hauptanlage verwendet werden. Aus Sicherheitsgründen stehen zur Versorgung thermischer Netze häufig mehrere unterschiedliche Systeme zur Wärmeerzeugung zur Verfügung.[23]

2.1.2 Einführung in den Branchenkontext: Energiequellen, industrielle Prozesse und erzeugte Temperaturen

Wie bereits erwähnt, können thermische Netze aus mehreren Energiequellen gespeist werden. Die Energieträger werden über verschiedene industrielle Prozesse in Wärme umgewandelt, die je nach erzeugter Temperatur für unterschiedliche Zwecke genutzt werden kann. Die Wärmeerzeugung stellt sich für die Branche der thermischen Netze somit sehr heterogen dar. Abbildung 2 veranschaulicht die verschiedenen Kombinationen von Energiequellen, die dabei zum Einsatz kommen können.

[23] *Faktenblatt Thermische Netze. EnergieSchweiz, Bundesamt für Energie BFE, Ittigen 2021.*

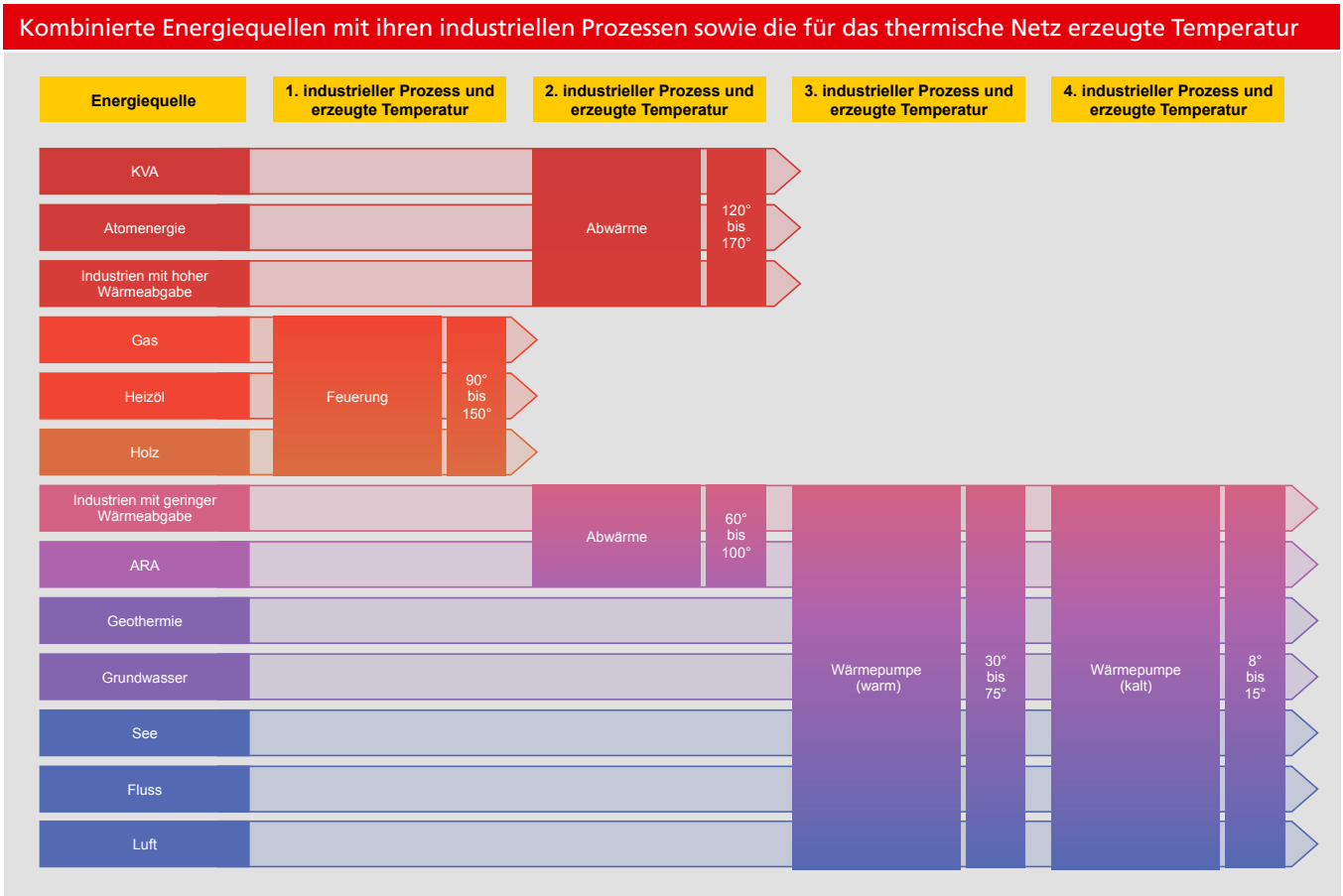

Abbildung 2: Energiequellen, industrielle Prozesse und erzeugte Temperaturen

Der erste industrielle Prozess wird über Feuerungen ausgeführt, die mit Holz, Heizöl oder Gas betrieben werden. Obwohl es zwischen diesen drei Energieträgern Temperaturunterschiede gibt, werden in diesem Prozess in jedem Fall hohe Temperaturen erzeugt. Beim zweiten industriellen Prozess entsteht Abwärme. Abhängig von der industriellen Aktivität, bei der die Anfangswärme produziert wird, werden unterschiedliche Temperaturniveaus erreicht. Hohe Temperaturen lassen sich durch industrielle Prozesse mit hoher Wärmeabgabe etwa in KVA oder Atomkraftwerken erzielen, während industrielle Aktivitäten mit niedrigerem Wärmepotenzial etwa in den ARA Abwärme mit niedrigeren Temperaturen erzeugen. Für den dritten industriellen Prozess, der Wärme mit begrenzter Temperatur (i.d.R. ≤75 °C) freisetzt, werden Wärmepumpen verwendet. Die Energiequellen zur Versorgung von Wärmepumpen finden sich im Boden (Geothermie und Grundwasser), im Wasser (See, Fluss, industrielle Aktivitäten mit geringer Wärmeabgabe) oder in der Luft. Der letzte industrielle Prozess dient der Erzeugung von Fernkälte mittels Wärmepumpen (kalt). Dabei kommen dieselben Verfahren zum Einsatz wie beim Betrieb von Wärmepumpen zur Wärmeerzeugung.

2.1.3 Entwicklungsperspektiven für die Branche der thermischen Netze

In den letzten Jahren ist die Schweiz verschiedene Umweltverpflichtungen eingegangen, die grosse Auswirkungen auf die Zukunft der thermischen Netze haben. Dabei handelt es sich um das Pariser Klimaabkommen von 2015, das festlegt, dass die CO_2-Emissionen bis 2030 im Vergleich zu 1990 um die Hälfte reduziert werden müssen, um den Bundesratsentscheid, wonach die Schweiz ab dem Jahr 2050 unter dem Strich kein Treibhausgas mehr ausstossen soll (Netto-Null-Emissionsziel), und insbesondere um die 2018 in Kraft getretene Energiestrategie 2050. Deren drei Hauptziele bestehen in der Senkung des Energieverbrauchs, der Steigerung der Energieeffizienz und der Förderung erneuerbarer Energien.[24]

Diese politischen Entscheide wirken sich auf die künftige Entwicklung der thermischen Netze aus und könnten zur Folge haben, dass diese Netze in der Schweiz eine wichtige Rolle bei der Energiewende spielen. Laut Expertenprognosen[25] ist mit einer deutlichen Erhöhung der Wärmeerzeugung durch diese Branche zu rechnen. Gemäss den Angaben im «Faktenblatt Thermische Netze» des BFE[26] hat die Schweiz 2020 rund 100 TWh Energie für ihren Wärmebedarf verbraucht. 60 % davon stammten noch aus fossilen Energieträgern. Der Anteil der Fernwärme (thermische Netze) belief sich auf ungefähr 9 %. Angesichts der oben erwähnten Verpflichtungen rechnet das BFE damit, dass der Energiebedarf der Schweiz für Wärme im Jahr 2050 rund 74 TWh pro Jahr betragen und der Anteil der Fernwärme ausgehend von den unterschiedlichen Entwicklungsannahmen zwischen 14 % und 24 % liegen wird. Die Branche muss nicht nur die Kapazitäten ausbauen, sondern auch den Anteil fossiler (Gas und Heizöl) und nicht erneuerbarer Energien (Atomkraft) ersetzen, die bei der Wärmeerzeugung derzeit noch oft zur Spitzenlastdeckung und als Sicherheitsreserve für einen allfälligen Ausfall der Hauptanlagen verwendet werden.

[24] Bundesamt für Energie. «Was ist die Energiestrategie 2050?», https://www.bfe.admin.ch/bfe/de/home/politik/energiestrategie-2050/was-ist-die-energiestrategie-2050.html (Stand: 10.1.2020).
[25] Leitfaden Fernwärme/Fernkälte. Verband Fernwärme Schweiz, Bern 2020.
[26] Faktenblatt Thermische Netze. EnergieSchweiz, Bundesamt für Energie BFE, Ittigen 2021.

Wärmebedarf der Schweiz und Anteil der thermischen Netze 2020 sowie Schätzung für 2050

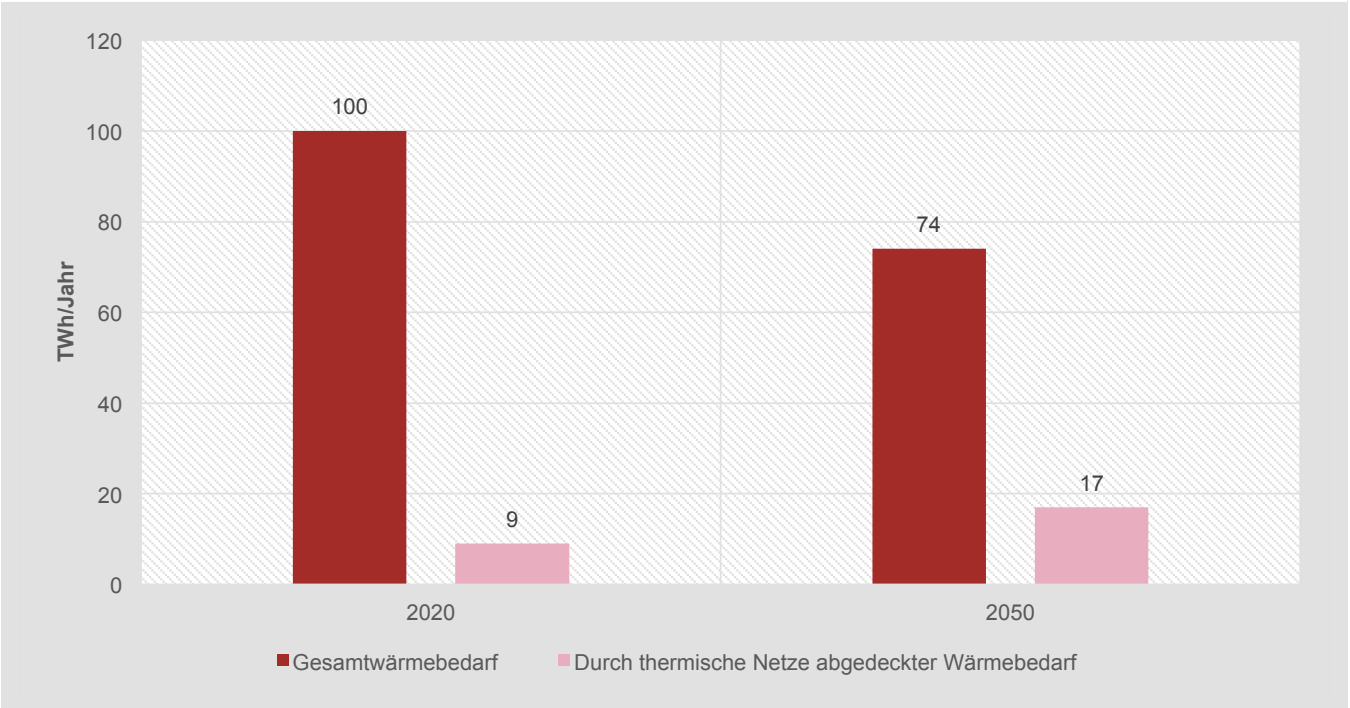

Abbildung 3: Wärmebedarf der Schweiz und Kapazität der thermischen Netze in den Jahren 2020 und 2050

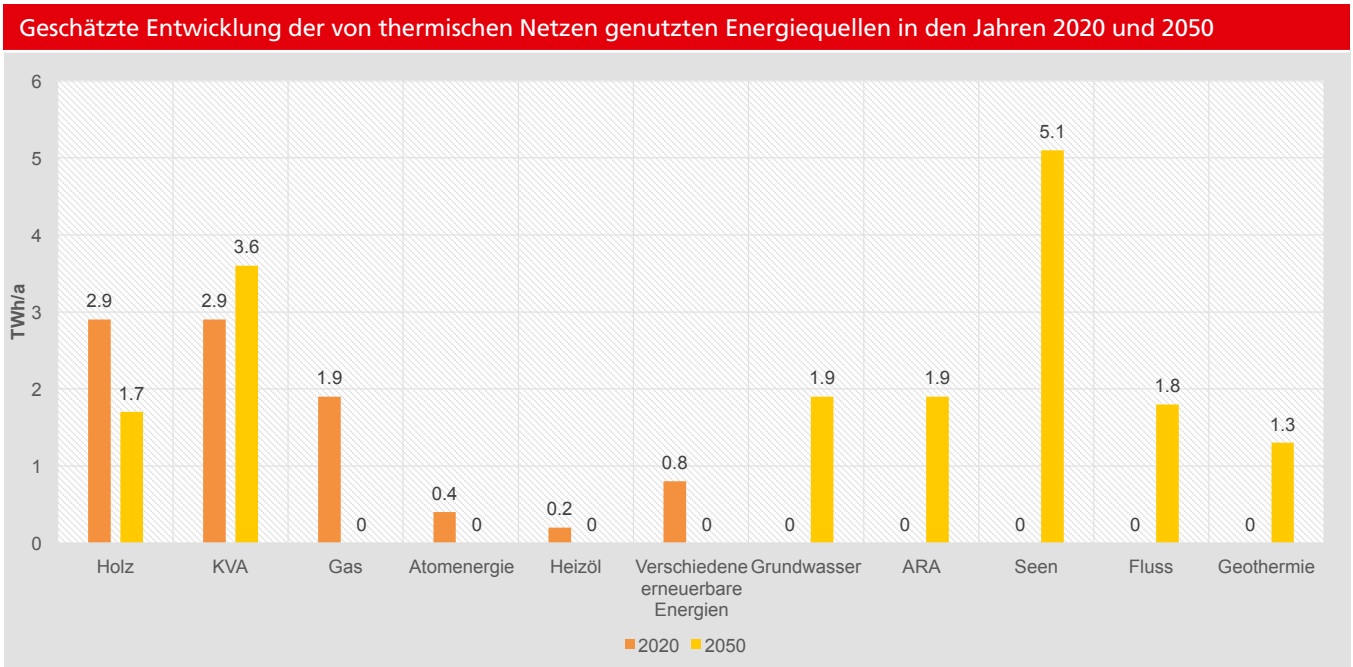

Abbildung 4: Entwicklung des Anteils der Energiequellen bis 2050

Für ein besseres Verständnis der künftigen Entwicklung im Bereich der thermischen Netze muss die mit den verschiedenen Energiequellen erzeugte Energie näher analysiert werden. Auf Grundlage der Zahlen im «Jahresbericht 2021»[27] TNS lässt sich die Verteilung auf die verschiedenen Energiequellen abschätzen. Rechnet man die Daten von Holzenergie Schweiz und TNS zusammen, haben die thermischen Netze 2020 rund 9 TWh an Wärme verkauft. 32,3 % davon stammten aus Holz, 31,8 % aus Kehrichtverwertungsanlagen (KVA), 20,7 % aus Erdgas, 8,5 % aus verschiedenen erneuerbaren Energien, 4,6 % aus Abwärme von Atomkraftwerken und 2,1 % aus Heizöl.

Was die Prognosen für 2050 anbelangt, die – wie in der Energiestrategie 2050 vorgesehen – ausschliesslich erneuerbare Energien berücksichtigen, rechnet TNS[28] mit einem Anstieg des Wärmeabsatzes der thermischen Netze auf 17,3 TWh (siehe Abbildung 3). 29 % der Wärme dürften dann aus Seen, 21 % von KVA, 11 % aus Grundwasser, 11 % aus ARA, 10 % aus Flüssen, 10 % aus Holz und 8 % aus Geothermie stammen. Abbildung 4 zeigt, wie viele TWh pro Jahr an Energie aus den verschiedenen Energiequellen gewonnen werden. Die Abbildung veranschaulicht auch das Ende der fossilen und den Ausbau der erneuerbaren Energien, insbesondere der See-Energie. Gemäss den Schätzungen von TNS verfügen die Seen über sehr grosses Entwicklungspotenzial. Demnach könnten sie sogar zur wichtigsten Energiequelle für die thermischen Netze avancieren und mehr Wärmeenergie beisteuern als die KVA, die ebenfalls deutlich zulegen und eine unverzichtbare Energiequelle bleiben werden.[29]

[27] *Jahresbericht 2021. Verband Fernwärme Schweiz, Bern 2022.*

[28] *Weissbuch: Fernwärme Schweiz – VFS Strategie. Verband Fernwärme Schweiz, Eicher+Pauli AG, Bern 2014.*

[29] *Leitfaden Fernwärme/Fernkälte. Verband Fernwärme Schweiz, Bern 2020.*

2.2 Akteure in der Branche der thermischen Netze

Die Branche umfasst mehrere hundert Akteure mit ganz unterschiedlichen Profilen. Wie bereits erläutert, unterscheiden sich die Energiequellen und die industriellen Prozesse erheblich von Anlage zu Anlage. Dasselbe gilt auch für die Länge der thermischen Leitungen sowie für die erzeugte Energiemenge. Ein Vergleich zwischen zwei höchst unterschiedlichen Akteuren soll diese Heterogenität verdeutlichen: Eines der grössten Unternehmen der Branche verfügt über ein Netz von mehr als 160 km und erzeugt rund 755 000 MWh pro Jahr, während eine kleine Lambda-Anlage mit einem Netz von 200 m Länge nur 600 MWh pro Jahr produziert.[30]

Trotz dieser Vielfalt ist die Marktzusammensetzung relativ einfach. Die meisten Akteure der Branche werden durch Thermische Netze Schweiz (TNS) und den Schweizerischen Verein des Gas- und Wasserfaches (SVGW) vertreten – den zwei in diesem Bereich aktiven Industrieverbänden. Die Regulierung und Aufsicht erfolgt wie in den meisten Energiesektoren durch das BFE. Um eine repräsentative Übersicht über die Branche zu erhalten, haben das BFE und TNS eine interaktive Karte mit fast allen thermischen Netzen des Landes erstellt. In Abbildung 5 ist jeder Akteur mit einem Punkt dargestellt, dessen Farbe über die verwendete Energiequelle Auskunft gibt. Die jeweils aktuelle Version dieser Karte und Detailinformationen über alle erfassten Akteure finden sich auf der Website TNS.[31]

Übersicht schweizerische Wärmeverbünde

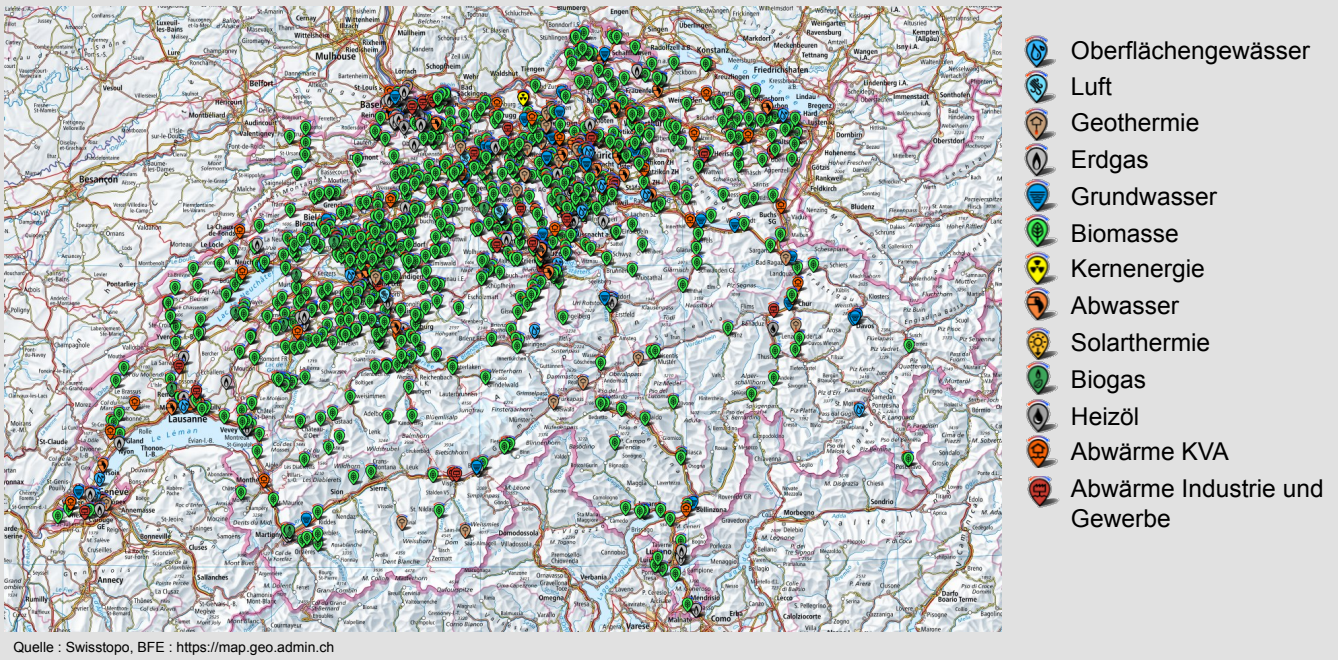

Abbildung 5: Übersicht schweizerische Wärmeverbünde

[30] *Thermische Netze Schweiz. «Karte Fernwärmenetze». Details: ERZ Entsorgung Recycling Zürich und CAD Bevaix. https://s.geo.admin.ch/925f2fecea (Stand: 10.1.2022).*

[31] *Link zur interaktiven Karte TNS: https://s.geo.admin.ch/925f2fecea*

2.3 Versorgungsprozess

Wie Abbildung 2 zeigt, gibt es nicht einen branchenweit einheitlichen Prozess zur Versorgung der thermischen Netze. Das liegt daran, dass sich die verwendeten Energiequellen und industriellen Prozesse zur Wärmeerzeugung von Infrastruktur zu Infrastruktur unterscheiden. Auf Grundlage der gesammelten Daten konnten drei zentrale Versorgungsprozesse identifiziert werden, die dieser Vielfalt Rechnung tragen. Jeder Prozess ist in vier Teilprozesse mit den jeweils wichtigsten Aktivitäten unterteilt.

2.3.1 Versorgungsprozess 1: Feuerung

Der erste Teilprozess «Rohstoffversorgung» umfasst gemäss Abbildung 6 die Aktivitäten im Zusammenhang mit der Produktion, dem Transport und der Beschaffung der Rohstoffe (Holz[32], Gas[33] bzw. Heizöl[34]), die für den Betrieb der Feuerung erforderlich sind. Die Unternehmen der Branche der thermischen Netze sind von den Rohstofflieferanten abhängig und haben praktisch keinen Einfluss auf diese Aktivitäten. Ihre Verantwortung beginnt, sobald sie Zugang zu den Brennstoffen erhalten. Der zweite Teilprozess betrifft die Wärmeerzeugung und umfasst unter anderem den Betrieb der Feuerung und aller IKT-Systeme zur Steuerung dieser Aufgaben. Durch die Verbrennung in der

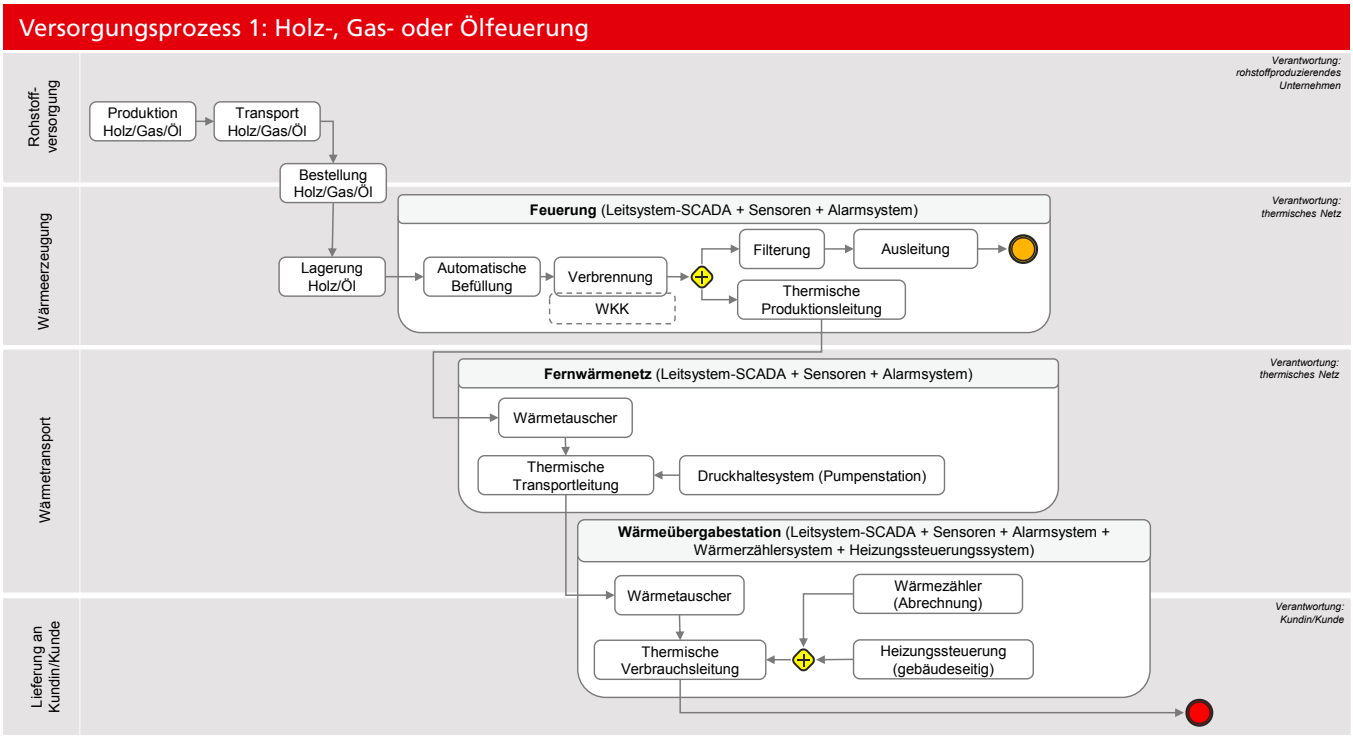

Abbildung 6: Versorgungsprozess mit Feuerungen

Feuerung werden hohe Temperaturen erzeugt, mit denen einerseits das Wärmeübertragungsmedium (hauptsächlich Wasser bzw. Dampf) in den thermischen Produktionsleitungen erhitzt und andererseits eine Wärme-Kraft-Kopplungsanlage betrieben wird, falls die Infrastruktur eine solche Komponente enthält (weitere Einzelheiten hierzu in Unterkapitel 2.3.4). Der dritte Teilprozess konzentriert sich auf den Wärmetransport. Durch den Wärmetauscher lässt sich die Wärme aus den thermischen Produktionsleitungen in die thermischen Transportleitungen übertragen, über die sie zu den Wärmetauschern der Kundinnen und Kunden gelangt. Mit den IKT-Systemen kann das gesamte

[32] *Energie-umwelt.ch. «Heizen mit Holz». https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/holz (Stand: 20.12.2021).*

[33] *Energie-umwelt.ch. «Heizen mit Erdgas (nicht erneuerbar) und Biogas (erneuerbar)». https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/erdgas-und-biogas (Stand: 20.12.2021).*

[34] *Energie-umwelt.ch. «Heizen mit Heizöl». https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/heizoel (Stand: 20.12.2021).*

Transportnetz einschliesslich der Unterstationen bei den Kundinnen und Kunden sowie der Druckniveaus aus der Ferne gesteuert und so ein optimaler Transport innerhalb der Leitungen sichergestellt werden. Der letzte Teilprozess umfasst die Lieferung der Wärme an die Kundinnen und Kunden und den Verbrauch der Wärme durch sie. Die Verantwortung der für das Fernwärmenetz zuständigen Organisation endet in der Regel an den Wärmeübergabestationen der Kundinnen und Kunden, es kann jedoch auch andere vertragliche Vereinbarungen zu den Prozessschnittstellen geben. Ab dann sind die Kundinnen und Kunden für das Heizsystem verantwortlich. IKT-Systeme kommen aber auch hier zum Einsatz, um die Daten über den Kundenverbrauch und für die Rechnungsstellung zu erheben. Ausserdem können die Kundinnen und Kunden die gewünschte Wärme über ihre Heizungssteuerung regulieren.

Der gesamte Versorgungsprozess wird über das Leitsystem (ICS) gesteuert, das eine zentrale Erfassung, Überwachung, Kontrolle und Verarbeitung der Daten aus den über die gesamte Infrastruktur verteilten Sensoren ermöglicht. Das ICS erlaubt die Fernsteuerung und Überwachung aller damit verbundener Aktivitäten. Erkennt das ICS, dass die kontrollierten Daten nicht der vordefinierten Sicherheitsrichtlinie entsprechen, löst es das Alarmsystem aus. Über dieses System wird den verantwortlichen Personen gemeldet, dass die Funktion beeinträchtigt sowie eine Korrektur und Reaktion notwendig ist.

Für eine bessere Lesbarkeit von Abbildung 6, Abbildung 7, Abbildung 8 und Abbildung 9 wurde das Verfahren des «Rücklaufs» nicht bildlich dargestellt. Alle thermischen Leitungen sind geschlossene Kreisläufe. Das Wärmeübertragungsmedium entweicht durch den Wärmeverbrauch nicht aus dem Netz, sondern nimmt den umgekehrten Weg zurück zur Heizzentrale, um dort erneut erhitzt zu werden.[35] Alle Abbildungen zu den Versorgungsprozessen sind im Anhang zusätzlich im Format A4 zu finden.

2.3.2 Versorgungsprozess 2: Abwärme

Bei der Abwärme produziert das für die thermischen Netze zuständige Unternehmen die Wärme nicht selbst. Vielmehr nutzt es die Wärme, die bei einer anderen vorgelagerten industriellen Aktivität entsteht, beispielsweise bei der Verbrennung von Abfällen in einer KVA[36] oder bei der Kernspaltung. Somit besteht ein Abhängigkeitsverhältnis zwischen dem Versorgungsprozess der thermischen Netze und der Aktivität, bei der die Wärme anfällt. Die Organisationsstruktur der beiden Aktivitäten ist nicht vordefiniert. Es existiert kein Standard in diesem Bereich. So kann ein einzelnes Unternehmen sowohl für die Hauptaktivität als auch für das thermische Netz verantwortlich sein. Möglich ist auch, dass sich zwei Firmen die Aufgaben untereinander aufteilen. Manchmal ist die Abgrenzung zwischen den beiden Unternehmen aber auch weniger eindeutig. Aufgrund der genannten Abhängigkeit muss das Unternehmen, das für die thermischen Netze zuständig ist, auch den erweiterten Versorgungsprozess berücksichtigen – einschliesslich der Aktivitäten, bei der die Wärme bzw. Abwärme erzeugt wird. Dasselbe gilt für den Schutz der IKT-Systeme: Diese können je nach Organisationsstruktur von mehreren Unternehmen gemeinsam genutzt werden oder komplett voneinander getrennt sein. In Unterkapitel 2.4.5.8 zu den kritischen Aktivitäten werden die Abhängigkeiten im Bereich der Abwärmeerzeugung näher behandelt, um die besonders beachtenswerten Punkte herauszustreichen.

[35] Energie-umwelt.ch. «Fernwärme (FW) und Fernwärmenetz». Fernwärme (FW) – energie-umwelt.ch (Stand: 20.12.2021).

[36] Energie-umwelt.ch. «Kehrichtverbrennungsanlage», https://www.energie-umwelt.ch/abfall-recycling/1446 (Stand: 20.12.2021).

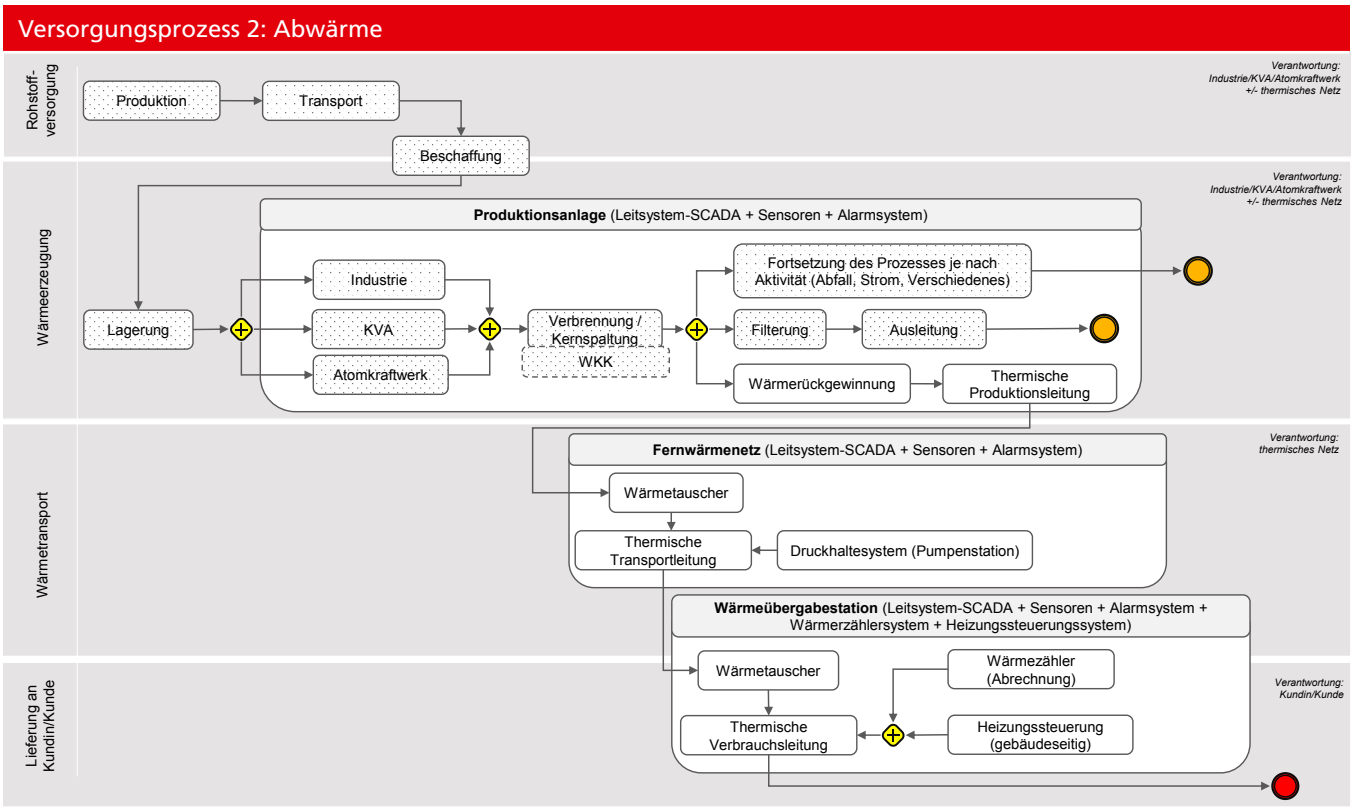

Abbildung 7: Versorgungsprozess mit Abwärme

Die Abhängigkeit von der Aktivität, bei der die Wärme erzeugt wird, wird in der Darstellung des Versorgungsprozesses der Abwärme (Abbildung 7) durch die gepunkteten Felder verdeutlicht. Die Aktivitäten in den gepunkteten Feldern sind für die Wärmeerzeugung erforderlich, dafür verantwortlich sind (je nach Organisationsstruktur) aber nicht unbedingt die für die thermischen Netze zuständigen Organisationen. Die Wärmeerzeugung erfolgt hier in verschiedenen Produktionsanlagen, primär in Kehrichtverwertungsanlagen (KVA), aber auch in Atomkraftwerken und anderen Industriebetrieben, die viel Abwärme produzieren. Die Fortsetzung des Versorgungsprozesses der Hauptaktivität ist in dieser Abbildung nicht im Detail dargestellt. Sie wird stattdessen unter dem Sammelbegriff «Fortsetzung des Prozesses je nach Aktivität» subsumiert und umfasst die Abfallbeseitigung, die Stromerzeugung und gegebenenfalls andere von der jeweiligen Branche abhängige Zwecke. Die Aktivität «Wärmerückgewinnung» besteht in der Rückgewinnung der Abwärme zur Erwärmung der thermischen Produktionsleitungen, über die dann die thermischen Netze versorgt werden. Die Fortsetzung des Versorgungsprozesses (Wärmetransport und Lieferung an die Kundinnen und Kunden) sowie die Nutzung der IKT-Systeme läuft genauso ab wie beim Versorgungsprozess der Feuerungen.[37]

[37] *Energie-umwelt.ch. «Fernwärme (FW) und Fernwärmenetz» Fernwärme (FW) – energie-umwelt.ch, (Stand: 20.12.2021).*

2.3.3 Versorgungsprozess 3: Wärmepumpe (WP)

Beim Versorgungsprozess mit Wärmepumpen übernimmt das für das thermische Netz zuständige Unternehmen ab dem ersten Teilprozess zur Rohstoffversorgung der Wärmepumpen die Verantwortung (Abbildung 8). Je nach Medium, aus dem die Wärme gewonnen wird, unterscheidet man drei Arten von Wärmepumpen: Die «Luft/Wasser»-Wärmepumpe[38], die die Umgebungsluft und die darin enthaltene Wärme mithilfe eines Kompressors ansaugt, die «Wasser/Wasser»-Wärmepumpe[39], die Wasser aus verschiedenen Umgebungen (Seen, Flüssen, Grundwasser und Abwasser verschiedener Anlagen wie etwa ARA) schöpft und daraus Wärme gewinnt, sowie die «Sole/Wasser»-Wärmepumpe[40], die dem Boden über Erdsonden Wärme entzieht, wobei die jeweilige Wärmemenge von der Bohrtiefe abhängt.

Die gewonnene Wärme lässt sich dann in der Wärmepumpe durch Kompression und Ausdehnung (Phasenwechsel) eines synthetischen Kältemittels vervielfachen. Konkret wird dabei die Wärmeenergie der primären Wärmequelle (Luft, Boden oder Wasser) auf das Kältemittel im Verdampfer übertragen. Das flüssige Kältemittel wechselt dadurch in den gasförmigen Zustand und dringt zum Kompressor vor, wo das Gas komprimiert wird. Durch Erhöhung des Drucks wird eine Reaktion ausgelöst, die die Temperatur des Gases deutlich erhöht. Das Gas strömt dann in den Verflüssiger (Kondensator), wo es seine Wärme auf die thermischen Produktionsleitungen überträgt. Dann wird das Gas zum Expansionsventil weitergeleitet, wo es durch Druckabbau verflüssigt wird. In diesem Aggregatszustand kann es im Verdampfer nun wieder Wärme aufnehmen und der Zyklus beginnt von Neuem. Die Aufgabe der ICS besteht dabei darin, die reibungslose Steuerung der Wärmepumpe zu gewährleisten. Das Leitsystem kontrolliert den Betrieb der Anlage, stellt einen optimalen Druck in den Leitungen sicher, sammelt und verarbeitet die Daten der Sensoren und löst im Falle von Unregelmässigkeiten das Alarmsystem aus.

Anders als bei den beiden anderen Versorgungsprozessen werden durch Wärmepumpen vergleichsweise niedrige Temperaturen (i.d.R. ≤75 °C) erzeugt. Wärmepumpen können aber auch Kälte produzieren. Das Prinzip ist dabei exakt dasselbe wie oben beschrieben, nur in umgekehrter Richtung: In diesem Fall wird Kälte in das thermische Netz eingeführt.[41] Der übrige Prozess läuft identisch ab wie bei den beiden anderen oben erläuterten Versorgungsprozessen.

[38] Energie-umwelt.ch. «‹Luft/Wasser›-Wärmepumpe (WP)», https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/luft-wasser-wp (Stand: 19.1.2022).
[39] Energie-umwelt.ch. «‹Wasser/Wasser›-Wärmepumpe (WP)», https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/wasser-wasser-wp (Stand: 19.1.2022).
[40] Energie-umwelt.ch. «Geothermie und ‹Sole/Wasser›-Wärmepumpe (WP)», https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/geothermie-und-sole-wasser-wp (Stand: 19.1.2022).
[41] Energie-umwelt.ch. «Allgemeines über die Wärmepumpen (WP)», https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/allgemeines-ueber-die-wp (Stand: 20.12.2021).

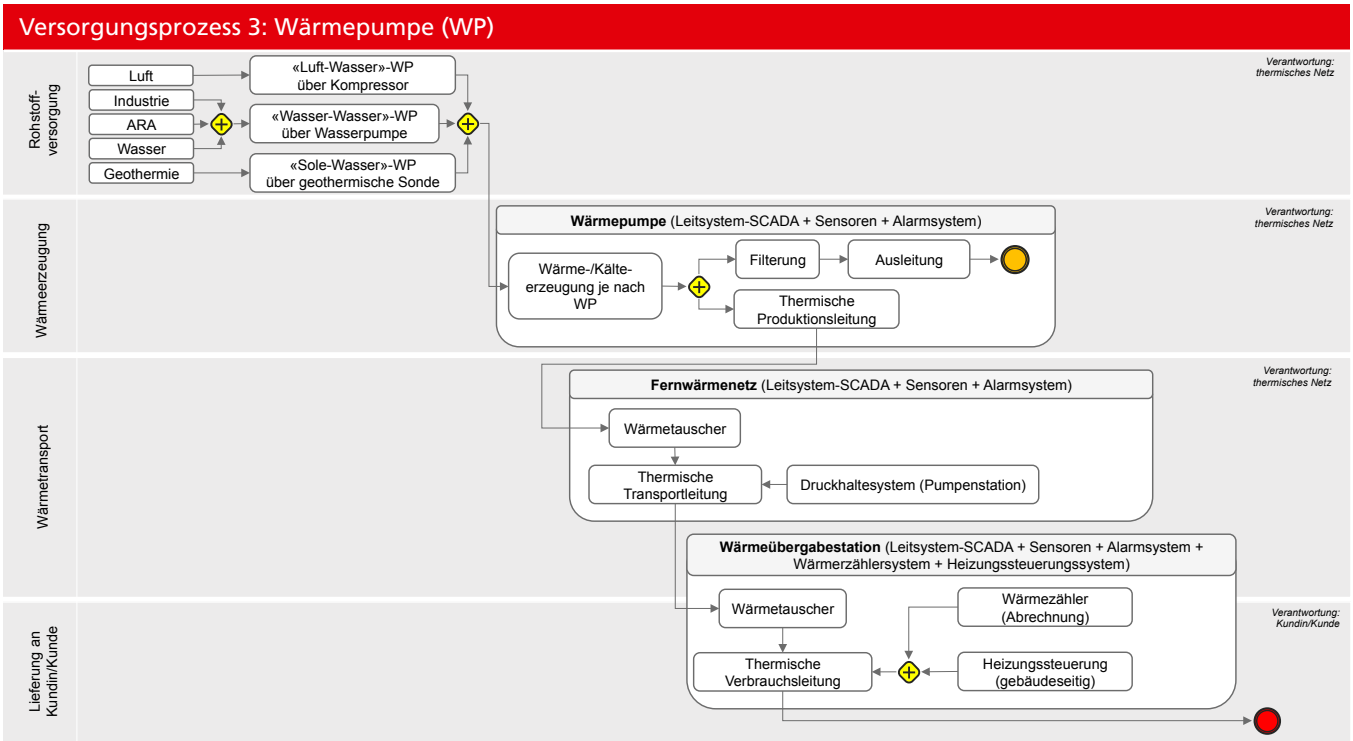

Abbildung 8: Versorgungsprozess mit Wärmepumpen

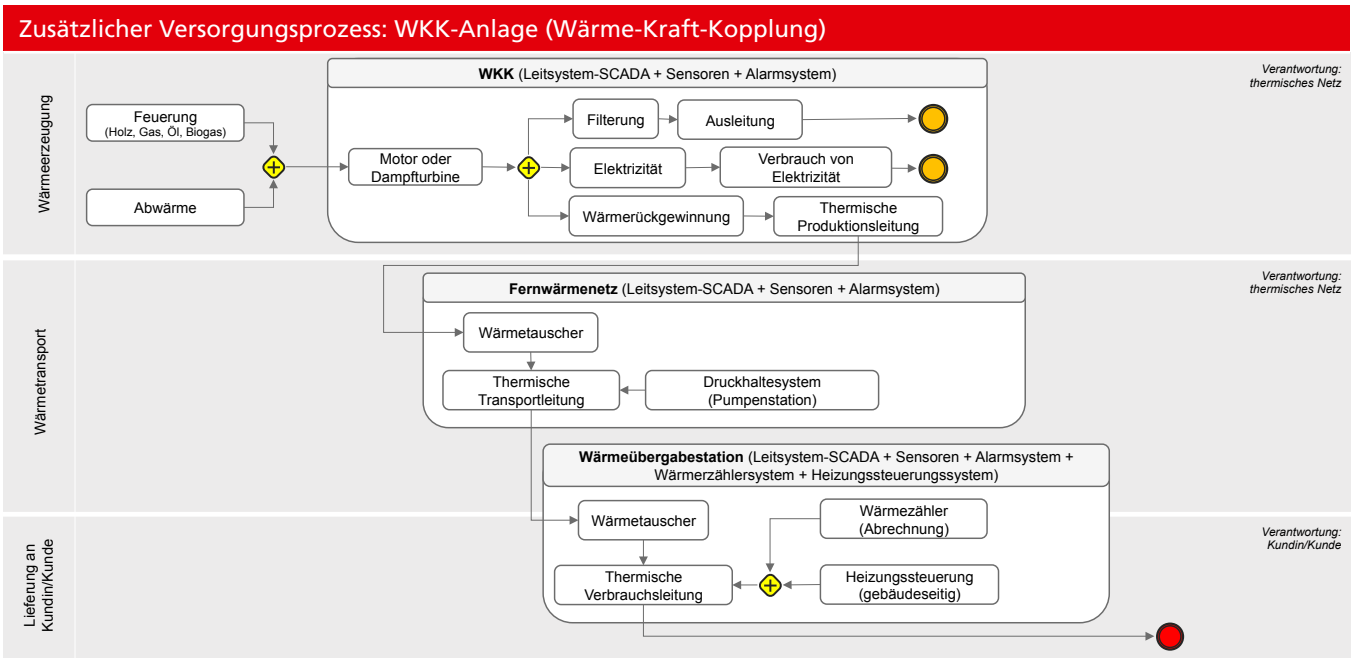

Abbildung 9: Zusätzlicher Versorgungsprozess – Wärme-Kraft-Kopplungsanlage

2.3.4 Zusätzlicher Versorgungsprozess: Wärme-Kraft-Kopplung (WKK)

Eine Wärme-Kraft-Kopplung stellt keinen eigenständigen industriellen Prozess dar, sondern wird mit einem anderen Produktionsprozess kombiniert. Da bei Wärmeerzeugungsanlagen recht häufig Wärme-Kraft-Kopplungsanlagen zu finden sind, ist es trotzdem sinnvoll, ihre Funktionsweise zu erläutern. Bei der Wärme-Kraft-Kopplung handelt es sich um ein Zusatzverfahren zur gleichzeitigen Erzeugung von Wärme und Strom, mit dem sich Heizungsanlagen effizienter nutzen lassen. Eine klassische Wärme-Kraft-Kopplungsanlage verwendet Gas, Heizöl, Holz oder Biogas, um einen Kolbenverbrennungsmotor oder eine Dampfturbine anzutreiben. Durch die Verbrennung entsteht Wärme, mit der sich ein Heizungskreislauf erhitzen lässt. Der Kolbenverbrennungsmotor bzw. die Dampfturbine ist an einen Generator angeschlossen, der Strom erzeugt.[42]

Bei den thermischen Netzen wird Wärme-Kraft-Kopplung in industriellen Feuerungs- und Abwärmeprozessen genutzt. Die hohen Temperaturen, die dabei erzeugt oder zurückgewonnen werden, lassen sich zur Dampfproduktion verwenden. Mit dem Dampf kann eine Turbine angetrieben werden, die an einen Generator gekoppelt ist. So ist es möglich, gleichzeitig Strom zu erzeugen und die thermischen Produktionsleitungen zu erhitzen. Ein Anschauungsbeispiel für den Einsatz der Wärme-Kraft-Kopplung findet sich in Unterkapitel 2.4.5.8. Dort werden in Abbildung 12 gleichzeitig auch die verschiedenen möglichen Anlagekombinationen aufgezeigt, mit denen sich die Effizienz von thermischen Infrastrukturen steigern lässt (KVA + WKK + ARA + thermische Netze).

Der zusätzliche Versorgungsprozess der Wärme-Kraft-Kopplung ist in Abbildung 9 dargestellt. Der Teilprozess «Rohstoffversorgung» wird hier nicht im Detail ausgeführt, weil er mit dem industriellen Prozess identisch ist, den die Wärme-Kraft-Kopplung ergänzt (Feuerung und Abwärme). Interessant ist, dass diese Anlagen für die Wärmeerzeugung häufig mit Biogas aus der Vergärung von Klärschlamm (ARA), organischen Abfällen oder Grünabfällen (Agrarbereich) betrieben werden.[43] Abgesehen von der Stromerzeugung, die ein charakteristisches Merkmal solcher Anlagen ist, entspricht das übrige Verfahren den zwei anderen Versorgungsprozessen, die die Wärme-Kraft-Kopplung ergänzen.

[42] Energie-umwelt.ch. «WKK – Wärme-Kraft-Kopplung», https://www.energie-umwelt.ch/haus/renovation-und-heizung/heizungssysteme/waerme-kraft-kopplung-wkk (Stand: 19.1.2022).
[43] Faktenblatt Thermische Netze. EnergieSchweiz, Bundesamt für Energie BFE, Ittigen 2021.

2.4 Kritische Aktivitäten

In Kapitel 2 werden die allgemeinen Anforderungen des IKT-Minimalstandards auf die branchenspezifischen Bedürfnisse angewendet. Hierzu werden verschiedene Themen behandelt und detailliert ausgeführt: vom aktuellen Kontext über die Versorgungsprozesse bis hin zu den Marktakteuren. Auf diese Weise sollen die «kritischen» Aktivitäten definiert werden, um die Organisationen dieser Branche für die wesentlichen Elemente zu sensibilisieren und ihnen zu ermöglichen, den IKT-Minimalstandard an ihre Bedürfnisse anzupassen. Dieser Ansatz erlaubt es somit, bestimmte Massnahmen des Cyber-Sicherheitsprogramms zu priorisieren und dabei die verfügbaren Ressourcen, das akzeptable Risiko sowie die Bedrohungen, denen die einzelnen Organisationen der Branche ausgesetzt sind, zu berücksichtigen.

2.4.1 Definition einer kritischen Aktivität

Eine Aktivität wird als kritisch eingestuft, wenn sie zwei Voraussetzungen erfüllt: Abhängigkeit von IKT-Systemen und Unverzichtbarkeit für den Versorgungsprozess. Zur Gewährleistung eines ausreichenden Sicherheitsniveaus musste indes noch ein dritter Begriff eingeführt werden. Denn es kann sein, dass eine IKT-Störung bei einer Aktivität den reibungslosen Ablauf des Versorgungsprozesses nicht beeinträchtigt, die Aktivität aber aus Gründen der Safety dennoch als kritisch eingestuft wird. Die Verwendung des englischen Begriffs erlaubt es, zwischen der Sicherheit der IKT-Systeme (Security) und dem Schutz von Menschenleben (Safety) zu unterscheiden. Zur Gewährleistung umfassender Sicherheit wurde entschieden, alle Aktivitäten, bei denen es infolge einer IKT-Panne zur Gefährdung von Menschenleben kommen kann, automatisch als kritisch einzustufen. Somit ist eine Aktivität dann kritisch, wenn sie 1. von den IKT-Systemen abhängt und 2. entweder den reibungslosen Ablauf des Versorgungsprozesses verhindert oder aber Menschenleben gefährdet.

2.4.2 Automatisierungspyramide

Zum besseren Verständnis wurden die identifizierten kritischen Aktivitäten den entsprechenden Ebenen der Automatisierungspyramide[44] zugeordnet. Mit dem Konzept der Automatisierungspyramide werden die verschiedenen IT-Ebenen (Anwendungen und Systeme) klassifiziert (siehe Abbildung 10). Ziel der Darstellung ist es, mit Blick auf die generischen Konzepte der Automatisierung besser sichtbar und verständlich zu machen, welche Technologien innerhalb eines Industriesektor verwendet werden. Die Pyramide ist in fünf Ebenen unterteilt, die jeweils eine bestimmte Art von Information oder System oder einen Zeitpunkt im Prozess darstellen.

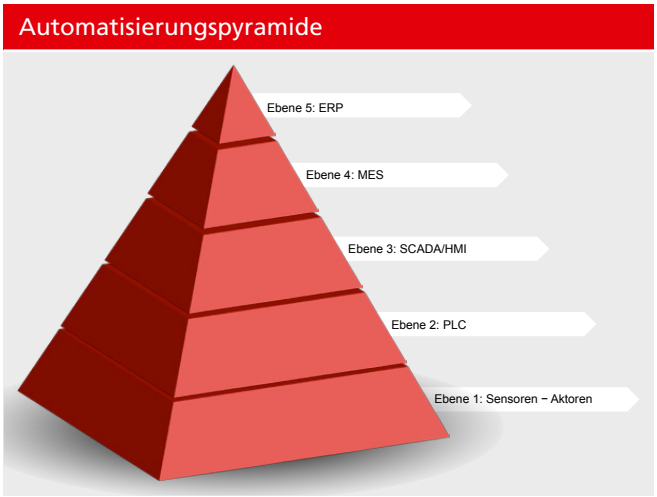

Abbildung 10: Automatisierungspyramide

- Ebene 1 umfasst alle physischen Elemente, die für den reibungslosen Ablauf der industriellen Tätigkeit erforderlich sind. Dazu gehören vor allem Sensoren und Aktoren (Zylinder, Motor, Pumpe, Ventil usw.), die einen direkten Einfluss auf die physische (materielle) Welt haben.

- Ebene 2 ist mit der Steuerung verbunden. Die speicherprogrammierbare Steuerung (PLC)[45] empfängt Signale von Sensoren und steuert die Aktoren, damit diese ihre Arbeit physisch ausführen.

- Ebene 3 dient der Steuerung und Überwachung mit einem SCADA-System. Ein SCADA-System ermöglicht also den Fernzugriff auf Daten und Leitsysteme und erlaubt konkret die Steuerung mehrerer PLC von einem Ort aus. Zudem sind SCADA-Systeme oft mit einer grafischen Benutzeroberfläche ausgestattet (HMI)[46], die die Überwachung und Steuerung aus der Ferne vereinfacht.

[44] Realpars. «What is the Automation Pyramid?», 11. Juni 2018. https://realpars.com/automation-pyramid/ (Stand: 7.7.2022).

[45] Programmable Logic Controller (PLC). Eine detaillierte Definition findet sich in Kapitel 3.1.

[46] Human Machine Interface (HMI)

- Auf Ebene 4 werden Verwaltungs- und Planungsaufgaben durchgeführt. Dazu kommen MES-Systeme[47] zum Einsatz, mit denen die gesamte Prozesskette von der Rohstoffbeschaffung bis zur Auslieferung des Endproduktes überwacht werden kann. Dank der MES-Systeme weiss die Geschäftsleitung jederzeit, was auf der Produktionsebene läuft, und kann auf Basis dieser Informationen strategische Entscheide für das gesamte Unternehmen treffen.

- Auf Ebene 5 sind die für das Management relevanten ERP-Systeme[48] angesiedelt, mit denen sich die operativen Informationen der unteren Ebenen mit den Verwaltungsdaten kombinieren lassen. Diese Integrationsstufe erlaubt der Geschäftsleitung die strategische Steuerung aller Unternehmensebenen vom Einkauf über die Produktion bis zum Verkauf, sowie Finanz- und Personalplanung usw.

[47] *Manufacturing Execution System (MES)*

[48] *Enterprise Resource Planning (ERP)*

2.4.3 Grafische Darstellung der kritischen Aktivitäten

Zum besseren Verständnis der verschiedenen kritischen Aktivitäten in der Branche der thermischen Netze (siehe Abbildung 11) wurden diese Aktivitäten in zwei Kategorien unterteilt. Die erste Gruppe umfasst alle kritischen Aktivitäten, die organisatorischer Natur sind, also Tätigkeiten, die sich auf den Verwaltungsbetrieb einer Organisation auswirken. Bei der zweiten Gruppe handelt es sich um kritische Aktivitäten operativer Natur, die spezifisch mit den industriellen Prozessen zusammenhängen. Diese Unterscheidung zwischen organisatorischen und operativen Aufgaben ist nicht unbedeutend, ist sie doch Teil einer umfassenderen Problematik infolge der Konvergenz zwischen Informationstechnologien (IT) und operativen Technologien (Operational Technology, OT). Diese Konvergenz ist die Ursache der Cyber-Sicherheitsprobleme von Industriebetrieben. Detaillierter behandelt wird dieses Thema in Kapitel 3.6. Jede kritische Aktivität ist in der Grafik kurz beschrieben, damit ihre Funktion auch ohne weitere Hilfsmittel verständlich ist, und die dafür jeweils notwendigen IKT-Systeme sind angegeben. Zudem zeigt die Grafik, ob eine Aktivität für die Safety relevant ist und auf welcher Ebene der Automatisierungspyramide sie angesiedelt ist. Zur besseren Lesbarkeit findet sich eine Version der Abbildung 11 im Format A4 in Anhang 7.3 dieses Dokumentes.

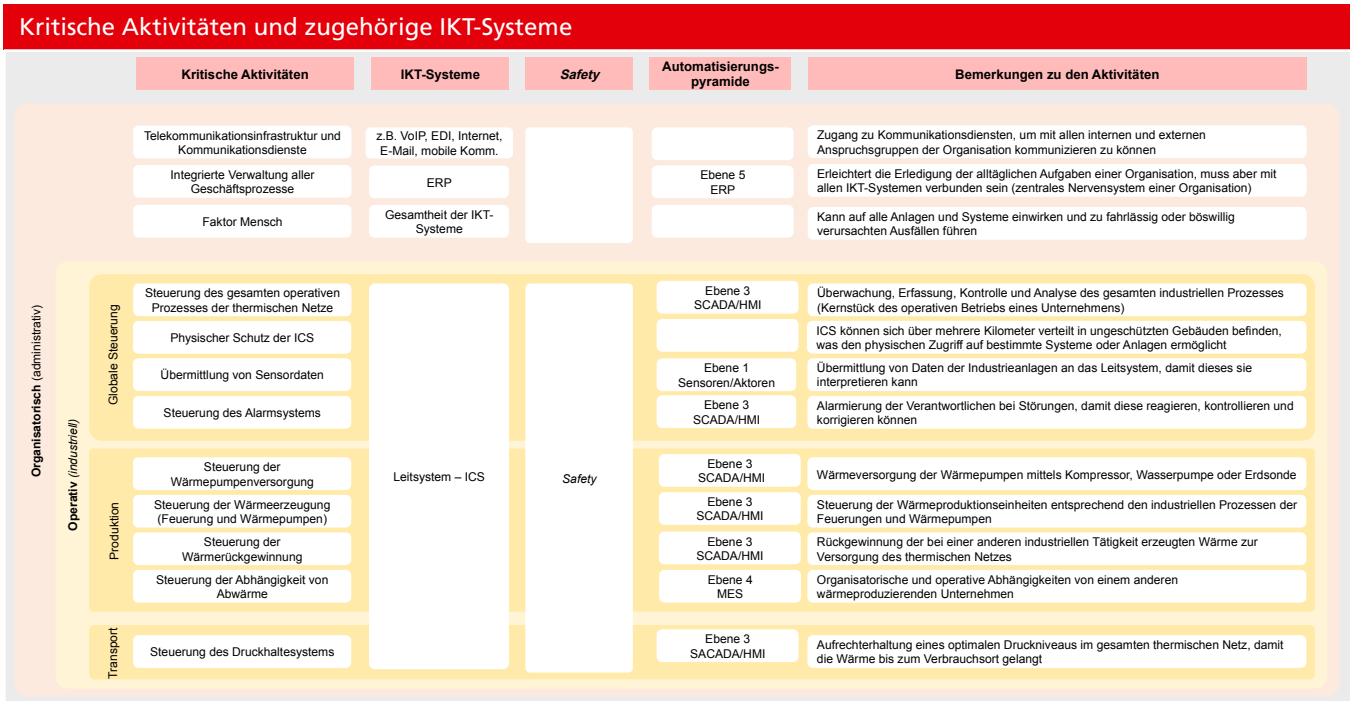

Abbildung 11: Kritische Aktivitäten und IKT-Systeme

2.4.4 Kritische Aktivitäten organisatorischer Natur

Wie oben erwähnt, handelt es sich dabei um die Aktivitäten, mit denen die Organisation einen Teil ihrer administrativen Aufgaben erledigt. Eine IKT-Störung bei einer dieser kritischen Aktivitäten kann zu einem Teil- oder Gesamtausfall der Infrastrukturen führen. Keine dieser Aktivitäten gilt allerdings aus Gründen der Safety als kritisch.

2.4.4.1 Telekommunikationsinfrastruktur und Kommunikationsdienste

Um ihre IKT-Systeme vollumfänglich nutzen zu können, müssen Organisationen Zugriff auf Telekommunikationsinfrastrukturen haben. Hierzu benötigen sie entsprechende Lieferanten (Provider), von denen sie somit abhängig sind. Deshalb sollte die Wahl auf einen Lieferanten fallen, der für seine Infrastrukturen ein hohes Schutzniveau bietet, auf die Bedürfnisse der Organisation zugeschnittene Dienstleistungen erbringt und bei einem Vorfall einen effizienten Support bietet. Um das Resilienzniveau einer Organisation zu erhöhen, ist es zudem empfehlenswert, Telekommunikationsinfrastruktur von mehreren Lieferanten zu beziehen. Dies verringert die Abhängigkeit von einzelnen Lieferanten und schafft Redundanzen, um Störungen der Infrastrukturen eines Dienstleisters abzufedern.

Telekommunikationsinfrastrukturen ermöglichen den Zugang zu einer Vielzahl von Kommunikationsdiensten, die für den reibungslosen Betrieb unverzichtbar sind. Dazu gehören zum Beispiel Sprachtelefonie (Voice-over-IP), elektronischer Datenaustausch (Electronic Data Interchange, EDI), Internetzugang, E-Mail, mobile Kommunikation und Zugang zur Cloud. Die Kommunikationsdienste spielen für die internen und externen Beziehungen der Unternehmen eine wesentliche Rolle. Beim Ausfall dieser Hilfsmittel ist der Informationsaustausch zwischen den verschiedenen Unternehmensteilen nicht mehr gewährleistet, wodurch der gesamte Betrieb lahmgelegt werden kann. Ohne Kommunikationsmittel lassen sich die organisatorischen und operativen Aktivitäten nur schwer zweckmässig durchführen, was die gesamte Organisation blockiert. Kann sie auf keine Telekommunikationsinfrastrukturen und Kommunikationsdienste mehr zugreifen, so kann sie auch ihre IKT-Systeme nicht mehr nutzen und ihrer Tätigkeit in diesem Fall nicht mehr nachgehen.

2.4.4.2 Integrierte Verwaltung aller Geschäftsprozesse

Dieses als Enterprise Resource Planning (ERP) bekannte IKT-System wird häufig als «zentrales Nervensystem eines Unternehmens» bezeichnet. Es erlaubt die Automatisierung, Integration und Bereitstellung der Informationen und Entscheidungsgrundlagen, die zur Erledigung aller alltäglichen administrativen Aufgaben erforderlich ist. Fast alle Daten der Organisation sind im ERP-System gespeichert, womit es ein exaktes, individuelles Bild der betrieblichen Realität eines Unternehmens liefert. Es übernimmt eine Reihe unterschiedlicher Aufgaben, beispielsweise im Zusammenhang mit der Rechnungsstellung, dem Personalwesen, der Produktion, der Lieferkette, dem Einkauf und der Lagerhaltung, um nur einige zu nennen. Um effizient funktionieren zu können, ist das ERP teilweise mit IKT-Systemen der Organisation verbunden, womit es einen neuralgischen Punkt der Infrastruktur darstellt. Ein Ausfall des ERP kann effektiv Störungen in verschiedenen Bereichen des Unternehmens, zur Folge haben. Daher gilt es, unbedingt zu vermeiden, dass das ERP als Angriffsvektor genutzt werden kann (indem es mit Air Gap, Demilitarized Zones (DMZ) usw. geschützt wird), um die kritischen IKT-Systeme einer Organisation wie etwa das Leitsystem (ICS) zu infizieren. Für den bestmöglichen Schutz des ERP sind regelmässige Datensicherungen (Backups) erforderlich, um das System auf einer soliden Grundlage neu starten zu können. Wichtig ist zudem der Aufbau einer segmentierten Netzwerkarchitektur (siehe Unterkapitel 4.2.4), um das industrielle Kontrollsystem angemessen vor einem Ausfall des ERP zu schützen. Bei der Wahl des Dienstleisters sollte zudem darauf geachtet werden, dass dieser einen effizienten Support und die ständige Weiterentwicklung der Software garantieren kann, damit diese möglichst resilient ist.

2.4.4.3 Faktor Mensch

Selbst die besten technischen Schutzmassnahmen können nicht garantieren, dass IKT-Systeme vor Fehlmanipulationen durch den Menschen gefeit sind. Solche Fehlmanipulation stellen die häufigste Gefahr dar und können weitreichende Systemausfälle verursachen. Die Organisation muss sich vor fahrlässig oder vorsätzlich begangenen Handlungen schützen. Zur Vermeidung fahrlässiger Fehlmanipulationen müssen die Mitarbeitenden vom Unternehmen hinsichtlich der Sicherheit der IKT-Systeme ausreichend geschult werden. Es wird den Unternehmen empfohlen, den Schulungsverlauf für alle Mitarbeitenden zu dokumentieren und die Schulungen regelmässig zu wiederholen. Dabei müssen sie für Best-Practices (Cyber-Hygiene) sensibilisiert, darin instruiert und auf ihre entsprechende Verantwortung hingewiesen werden, damit sie ihre Aufgaben während ihrer gesamten Beschäftigungszeit unter Einhaltung der Sicherheitsstandards erledigen können. Die Weisungen und Richtlinien zur IKT-Sicherheit müssen klar und umsetzbar sein, damit ein für die Mitarbeitenden zweckmässiger Rahmen und Modus Operandi entwickelt werden kann. Ausserdem müssen für den Fall einer IKT-Störung die Aufgaben und Rollen klar definiert und transparent zwischen den verschiedenen Mitarbeitenden aufgeteilt sein. Um die Risiken im Zusammenhang mit den Mitarbeitenden zu minimieren, kann das Unternehmen beispielsweise die Zugriffsrechte einschränken, indem es sie nur bestimmten verantwortlichen Personen gewährt. Es ist auch sinnvoll, verschiedene Arten von Profilen mit spezifischen und bedürfnisorientierten Rechten je nach IKT-System zu definieren (z. B. Administrator-, Modifikator-, Benutzerprofil). Um die Sicherheit bei bestimmten kritischen Aufgaben zu erhöhen, empfiehlt es sich zudem, eine doppelte Authentifizierung einzuführen. Vorsätzliche Fehlmanipulationen werden mehrheitlich von ehemaligen Beschäftigten begangen. Zur Abwehr von solchen Angriffen müssen die Organisationen ein strenges Verfahren befolgen, indem sie ehemaligen Mitarbeitenden den Zugang verunmöglichen und die Protokolle für den Zugriff auf die Infrastrukturen regelmässig ändern.

2.4.5 Kritische Aktivitäten operativer Natur

Während die organisatorischen Aktivitäten Auswirkungen auf das gesamte Unternehmen haben, betreffen die operativen Aktivitäten die industriellen Prozesse und sind somit spezifischer. In Kapitel 2.3 zu den Versorgungsprozessen sind hauptsächlich diese operativen Aktivitäten in verschiedenen Abbildungen dargestellt (Abbildung 6, Abbildung 7, Abbildung 8 und Abbildung 9). Die Störung einer dieser kritischen Aktivitäten beeinträchtigt die Produktion, den Transport oder die Lieferung von Wärme. In manchen Fällen kann ein Ausfall sogar den gesamten Versorgungsprozess thermischer Netze gefährden. Da es sich hier um industrielle Aktivitäten zur Steuerung verschiedener Hochtemperatur-Verbrennungssysteme und unter Druck stehender Leitungen handelt, werden die meisten von ihnen als kritisch eingestuft, zumal sie für den Versorgungsprozess benötigt werden und für die Safety relevant sind.

2.4.5.1 Steuerung des gesamten operativen Prozesses im Bereich der thermischen Netze

Die Steuerung der operativen Prozesse im Bereich der thermischen Netze erfolgt primär durch das ICS (Leitsystem, PLC, Direct Digital Control DDC usw.). Das Leitsystem ist für die zentrale Erfassung, Überwachung, Kontrolle und Verarbeitung von Daten aus Feldeinheiten zuständig, die geografisch über mehrere Kilometer verteilt sind. Damit lassen sich mehrere lokale Operationen fernsteuern, wie etwa das Einschalten, der Betrieb und das Ausschalten von Produktionsanlagen, die Erfassung von Daten verschiedener Sensoren, der Druck in den thermischen Leitungen sowie die Überwachung der gesamten Infrastruktur. Dieses System ist somit das zentrale Element zur Steuerung der operativen Prozesse. Bei einer Störung des Leitsystems ist die Organisation nicht mehr in der Lage, ihre Anlagen zu überwachen und zu steuern. Die Anlagen müssen jedoch auf Steuerungsebene auch bei einem Ausfall des Leitsystems autonom weiterlaufen. Weil das ICS auf fast alle industriellen Aktivitäten zugreifen kann, würde bei einer feindseligen Übernahme der Kontrolle durch Dritte über die betreffende Software beträchtlicher Schäden entstehen. In diesem Fall wäre auch die Sicherheit für Leib und Leben von Menschen möglicherweise bedroht (Safety), weshalb diese Aktivität als besonders kritisch einzustufen ist.

Hinzu kommt, dass diese spezifischen Systeme von spezialisierten Unternehmen entwickelt und verbessert werden. Dadurch entsteht ein weiteres Abhängigkeitsverhältnis gegenüber einem externen Dienstleister. Bei der Wahl des Anbieters sollte daher unbedingt darauf geachtet werden, dass dieser einen tadellosen Support und die ständige Weiterentwicklung des Systems garantieren kann, damit dieses möglichst sicher und resilient ist. Die Netzwerkarchitektur des Leitsystems ist ein weiteres wesentliches Element, das berücksichtigt werden muss. Um die Zugriffsmöglichkeiten auf das Leitsystem so weit wie möglich zu beschränken und so seine Resilienz zu erhöhen, ist es wichtig, das System von anderen abzuschotten. Dieser Punkt wird in Unterkapitel 4.2.4 noch detaillierter behandelt.

2.4.5.2 Physischer Schutz der ICS

Da ICS zur Steuerung von physischen Netzen eingesetzt werden, die über mehrere Kilometer verteilt sind, gilt es auch, eine grosse Zahl an Netzgeräten physisch zu schützen. Die wichtigsten physischen Zugangspunkte (PLC) befinden sich meist in Kellern (Heizungskeller) von Privatgebäuden. Da es sich hierbei oft um abgelegene und nicht unbedingt gut gesicherte Orte handelt, haben potenzielle Angreiferinnen und Angreifer viel Zeit, um einen solchen Angriff vorzubereiten und durchzuführen. Ausserdem ist es nicht möglich, all diese möglichen Zugangspunkte (mögliche Angriffsvektoren) physisch zu schützen. Je nach verwendeter Technologie kann ein möglicher Angriff über WLAN, Bluetooth oder Glasfaser erfolgen. Daher muss das Netz durch eine Defense-in-depth-Strategie umfassend geschützt werden (siehe Kapitel 4.2).

2.4.5.3 Übermittlung von Sensordaten

Im operativen Prozess der thermischen Netze kommen flächendeckend Sensoren zum Einsatz, die Daten zum Betrieb der verschiedenen Anlagen erfassen und an das Leitsystem (ICS) übermitteln. Diese physisch in sämtlichen Infrastrukturen des Versorgungsprozesses vorhandenen IKT-Elemente kommunizieren permanent mit dem Leitsystem. Sie liefern ihm sehr unterschiedliche Daten, die von der Temperatur der Wärmeproduktionsanlage über den Energieverbrauch der Kundinnen und Kunden bis zum Druckniveau in den thermischen Leitungen reichen. Bei einem grossflächigen Ausfall der Sensoren lässt sich die Anlage nicht mehr korrekt steuern, weil die PLC/DDC keine anlagenspezifischen Daten mehr erhalten. Die Organisation verliert dadurch den Gesamtüberblick und somit die Möglichkeit, die Infrastruktur fernzusteuern. Werden Sensoren manipuliert und übermitteln somit falsche Daten, wären die von der Organisation ergriffenen Massnahmen zudem nicht mehr auf die wirkliche Situation abgestimmt, wodurch sich diese durch das Eingreifen nicht verbessern, sondern weiter verschlechtern würde. Je nach Bedeutung der Infrastruktur, an die die Sensoren angeschlossen sind, könnte deren Ausfall oder die Übermittlung verfälschter Daten den Versorgungsprozess lahmlegen und/oder Menschenleben gefährden (Safety). Daher ist ein angemessener Schutz der Sensoren wichtig, um den gesamten Versorgungsprozess abzusichern.

2.4.5.4 Steuerung des Alarmsystems

Mit den von den Sensoren gesammelten und vom Leitsystem analysierten Daten lassen sich sämtliche Anlagen überwachen. Um ein ausreichendes Sicherheitsniveau zu gewährleisten, wird das Leitsystem mit einem Alarmsystem kombiniert. So können Auffälligkeiten in der gesamten Infrastruktur schnell erkannt werden. Bemerkt das industrielle Kontrollsystem, dass die kontrollierten Daten nicht dem vordefinierten Sicherheitsintervall entsprechen, löst es das Alarmsystem aus. Über dieses System wird den verantwortlichen Personen gemeldet, dass der Betrieb beeinträchtigt sowie eine Korrektur und Reaktion notwendig ist. Bei einer Störung des Alarmsystems ist die Organisation nicht mehr in der Lage, angemessen zu reagieren. Dadurch kann sich die Situation verschlimmern, was möglicherweise die Gefährdung von Menschenleben (Safety) oder die teilweise bzw. vollständige Blockierung der Anlagen zur Folge hat. Um dies zu verhindern, sind auf der Anlage weitere analoge und physische Sicherheitsvorkehrungen umzusetzen, wie etwa Überdruckventile, Pressostate (Druckschalter), Thermostate.

2.4.5.5 Steuerung der Wärmepumpenversorgung

Für die Versorgung der Wärmepumpen mit Wärme stehen drei Verfahren zur Verfügung: das Ansaugen von Umgebungsluft mithilfe eines Kompressors, die Entnahme von Wasser mit einer Wasserpumpe und der Entzug von Wärme aus dem Erdreich mittels einer Erdsonde. Bei einem Ausfall der IKT-Systeme (Sensoren, Leitsystem oder auch Alarmsystem) können die Wärmepumpen nicht mehr versorgt werden, womit dieser Versorgungsprozess komplett zum Erliegen kommt. Wenn kein redundantes Wärmeerzeugungssystem zur Erhitzung des thermischen Netzes zur Verfügung steht, wird das Netz nicht mehr mit Wärme versorgt.

2.4.5.6 Steuerung der Wärmeerzeugung (Feuerung und Wärmepumpe)

Wie zuvor erläutert, ist die Infrastruktur der thermischen Netze durchwegs mit Sensoren ausgestattet und mit dem Leitsystem (ICS) verbunden. Dies gilt auch für die Wärmeproduktionseinheiten, die vor Ort über die Maschinenschnittstelle (Programmable Logic Controller, PLC)[49] oder aus der Ferne mithilfe des ICS gesteuert werden können. Die IKT-Systeme kontrollieren somit verschiedene Aufgaben wie etwa das Ein- und Ausschalten der Anlage, die der Feuerung zugeführte Brennstoffmenge, die angestrebte Temperatur, den Druck in den Systemen sowie das Energieniveau, das produziert werden soll. Eine IKT-Störung an einer Feuerung oder Wärmepumpe führt unweigerlich zu einem Produktionsstopp, wodurch der Versorgungsprozess der thermischen Netze zum Stillstand kommt. Steht in diesem Fall kein redundantes Wärmeerzeugungssystem zur Verfügung, bleiben die Heizungen der Kundinnen und Kunden kalt. Je nach Netzgrösse und Jahreszeit kann dies eine Gefahr für sie darstellen (Safety). Werden IKT-Systeme vorsätzlich manipuliert, könnte die Wärmeproduktionseinheit absichtlich an ihre Kapazitätsgrenzen gebracht werden, was womöglich physische Schäden und eine Gefährdung von Menschenleben (Safety) zur Folge hat, sofern keine weiteren physischen Sicherheitsmassnahmen vorhanden sind (siehe oben).

2.4.5.7 Steuerung der Wärmerückgewinnung (Abwärme)

Anders als bei industriellen Prozessen, die mit Feuerungen oder Wärmepumpen funktionieren, wird bei der Abwärmenutzung Wärme nicht produziert, sondern zurückgewonnen. Die Verantwortung des für die thermischen Netze zuständigen Unternehmens beginnt hier mit der Wärmerückgewinnung. Seine Aufgabe besteht darin, die bei einer anderen industriellen Aktivität erzeugte Wärme zu gewinnen und auf die thermischen Leitungen zu übertragen. Mit den IKT-Systemen werden verschiedene Parameter (Menge, Temperatur, Druck usw.) kontrolliert, damit den thermischen Netzen die für ihren reibungslosen Betrieb erforderliche Wärme zur Verfügung steht. Bei einem Ausfall der IKT-Systeme wäre es nicht mehr möglich, die für die Erhitzung der Leitungen der thermischen Netze erforderliche Wärme zurückzugewinnen. Dies würde den Versorgungsprozess beeinträchtigen und somit womöglich zum Ausfall der Heizungen bei den Kundinnen und Kunden führen. Je nach Netzgrösse und Jahreszeit könnten die Folgen gravierend sein (Safety).

2.4.5.8 Steuerung der Abhängigkeit von Abwärme

Anders als bei Feuerungen und Wärmepumpen muss für die Abwärmenutzung ein weiterer Faktor berücksichtigt werden. Denn hier produziert das für die thermischen Netze zuständige Unternehmen die Wärmeenergie nicht selbst und ist somit vom Versorgungsprozess der Hauptaktivität, bei der die Wärme erzeugt wird, und vom dafür verantwortlichen Unternehmen abhängig. Diese Besonderheit verdeutlicht, wie wichtig es ist, dass bei der Umsetzung der Cyber-Sicherheitsstrategie drei Faktoren berücksichtigt werden:

Organisationsstruktur

Der erste Faktor ist organisatorischer Natur und betrifft die Aufteilung der Aufgaben und Verantwortungsbereiche zwischen den beiden Organisationen. Da es diesbezüglich keine vordefinierten Standards gibt, hängt die Auswahl der jeweiligen Struktur vom Kontext ab. So kann zum Beispiel ein einzelnes Unternehmen sowohl für die Hauptaktivität als auch für das thermische Netz verantwortlich sein. Möglich ist auch, dass sich zwei Organisationen die Aufgaben klar untereinander aufteilen und ihre Infrastrukturen sorgfältig voneinander trennen. Manchmal ist die Aufgabenabgrenzung zwischen den beiden Unternehmen aber auch weniger eindeutig und sie nutzen einen Teil der Anlagen bzw. Systeme gemeinsam. Diese organisatorische Unterscheidung wirkt sich sowohl auf den Betrieb als auch auf den Schutz dieser Organisationen aus: Je abhängiger die Unternehmen voneinander sind, desto besser müssen sie gemeinsam geschützt werden, damit eine IKT-Störung bei einem der beiden nicht den Ausfall des anderen nach sich zieht.

Netzwerkarchitektur

Beim zweiten Faktor geht es um die Netzwerkarchitektur, die von den Unternehmen zur Begrenzung ihrer gegenseitigen Abhängigkeit genutzt wird. Eine gute Netzwerkarchitektur ermöglicht die Segmentierung der verschiedenen IKT-Netze und die Isolierung der wichtigsten Netze, sodass es bei einem Angriff schwierig ist, sie zu erreichen. Das Hauptziel besteht generell in der Abschottung der IKT-Systeme des «operativen» Teils, um die

[49] *Siehe Erklärungen in Kapitel 3.1.*

der Produktion dienenden Infrastrukturen besser zu schützen und deren Manipulation zu verhindern. Sind zwei Unternehmen voneinander abhängig, ist eine wirksame Netzwerkarchitektur somit von zentraler Bedeutung. Eine ungeeignete Netzwerkarchitektur kann nämlich zu kaskadierenden Ausfällen führen, die möglicherweise eine physische Bedrohung für sämtliche Anlagen darstellen und Menschenleben gefährden (Safety). Weitere Informationen über die Netzwerkarchitektur finden sich in Kapitel 4.2.4.

Kritische Aktivitäten

Der dritte Faktor hängt mit der Steuerung der kritischen Aktivitäten zusammen. Ein Unternehmen, das für thermische Netze zuständig ist und Abwärme für deren Versorgung nutzt, kann sich durch eine korrekte Absicherung seiner kritischen Aktivitäten angemessen gegen Cyber-Risiken schützen. Das wird allerdings nicht ausreichen, denn für die Erhitzung der thermischen Leitungen nutzt das Unternehmen Wärme, die bei einer anderen Aktivität entsteht. Diese Aktivität wird aber unter Umständen von einem anderen Unternehmen mit kritischen Aktivitäten gesteuert, die von einem anderen Versorgungsprozess abhängen. Daher beschränken sich die kritischen Aktivitäten von Unternehmen, die Abwärme für ihre thermischen Netze nutzen, nicht auf die in diesem Minimalstandard genannten Tätigkeiten. Vielmehr zählen auch alle im Zusammenhang mit der Hauptaktivität stehenden kritischen Aktivitäten dazu. Daher ist es sehr wichtig, dass diese beiden Unternehmen gemeinsam auf die Erreichung eines ausreichenden Sicherheitsniveaus hinarbeiten. Das gilt auch für den Fall, dass ein einzelnes Unternehmen sowohl für die Hauptaktivität als auch für das thermische Netz verantwortlich ist. Auch dieses Unternehmen muss für einen wirksamen Schutz die kritischen Aktivitäten beider Sektoren berücksichtigen.

Übersicht über die Abhängigkeiten

In Abbildung 12 wird ein solches Abhängigkeitsverhältnis anhand einer Kehrichtverwertungsanlage (KVA) veranschaulicht, deren Wärme dazu genutzt wird, eine Wärme-Kraft-Kopplungsanlage zu betreiben, die Strom erzeugt und ein thermisches Netz versorgt. Diese Abbildung zeigt in vereinfachter Weise die verschiedenen Aktivitäten beim Betrieb einer solchen Anlage. In diesem Beispiel wird der gesamte industrielle Prozess in vier Teile gegliedert, die unterschiedliche Industriezweige mit jeweils einem eigenen branchenspezifischen IKT-Minimalstandard abdecken. Das erste Rechteck bezieht sich auf die thermischen Netze, das zweite auf die Stromversorgung[50], das dritte auf die Abfallentsorgung[51] und das vierte auf Abwasser[52]. Die Darstellung verdeutlicht die Folgen der Abhängigkeit zwischen der Hauptaktivität (Abfallentsorgung) und der Wärmerückgewinnung für das thermische Netz. Die Abbildung zeigt ebenfalls, dass hinsichtlich der Abwärme die Branche der thermischen Netze nicht isoliert, sondern als Teil eines aus mehreren Branchen bestehenden Ganzen betrachtet werden sollte. Bei der Umsetzung eines Cyber-Sicherheitsprogramms ist es daher notwendig, sämtliche Infrastrukturen zu schützen, um Kaskadenrisiken zu minimieren. Den Unternehmen wird entsprechend empfohlen, einen ganzheitlichen Überblick über all ihre Abhängigkeiten sicherzustellen und alle Abhängigkeiten ihres Versorgungsprozesses zu identifizieren. Sie sollten die eigenen Verantwortlichkeiten und jene der Organisationen, von denen sie abhängig sind, festlegen, eine geeignete Netzwerkarchitektur entwerfen und die verschiedenen branchenspezifischen IKT-Minimalstandards sinnvoll nutzen, um alle IKT-Systeme, auf die sie angewiesen sind, angemessen zu schützen.

[50] Handbuch Grundschutz für «Operational Technology» in der Stromversorgung. Verband Schweizerischer Elektrizitätsunternehmen (VSE), Bundesamt für wirtschaftliche Landesversorgung (BWL), Schweiz 2018.
[51] Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Abfallentsorgung. Verband der Betreiber Schweizerischer Abfallverwertungsanlagen (VBSA), Bundesamt für wirtschaftliche Landesversorgung (BWL), Schweiz 2022.
[52] Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in Abwasserbetrieben. Verband Schweizer Abwasser- und Gewässerschutzfachleute (VSA), Bundesamt für wirtschaftliche Landesversorgung (BWL), step by STEP, Schweiz 2021.

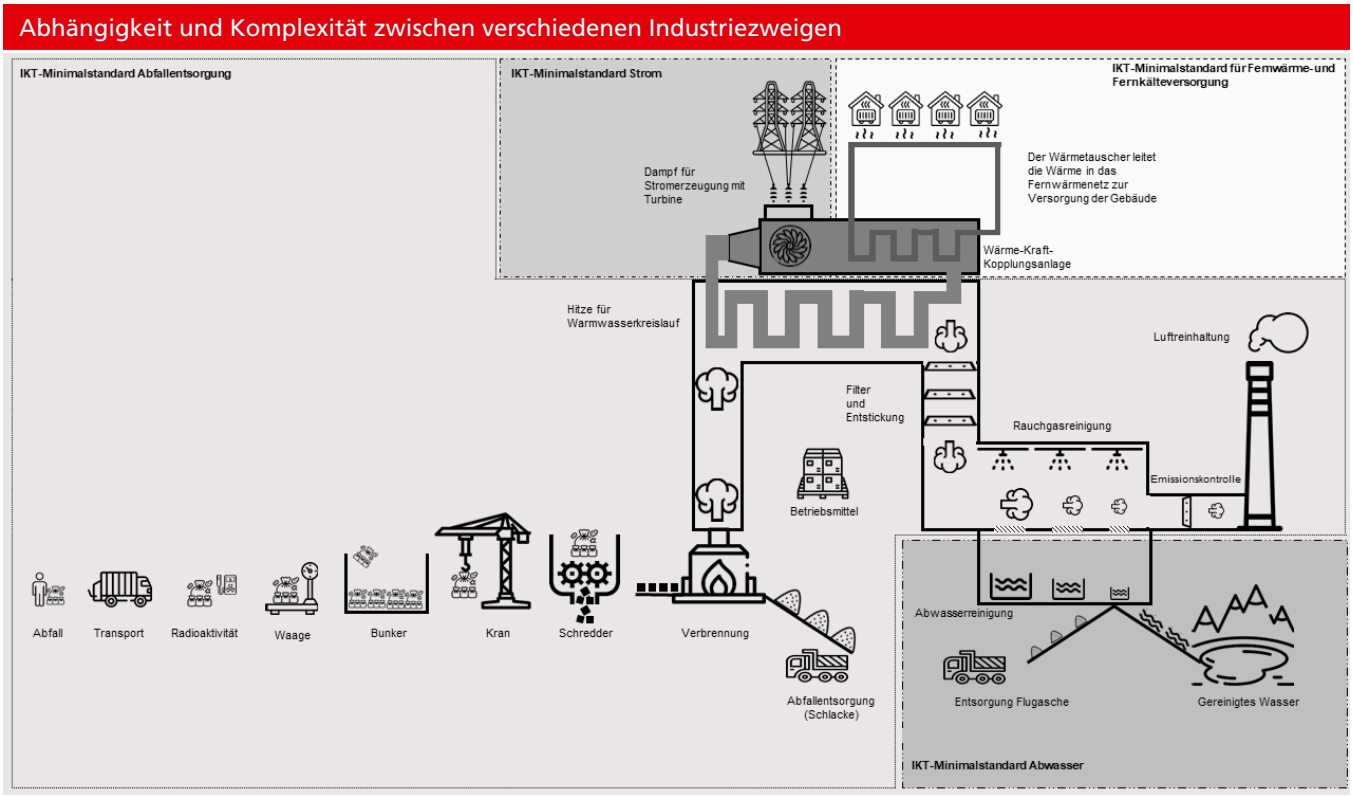

Abbildung 12: Abhängigkeiten zwischen KVA, thermischem Netz, Strom und Abwasser

2.4.5.9 Steuerung des Druckhaltesystems

Zur Lieferung der Wärme an die Kundinnen und Kunden werden die thermischen Leitungen unter Druck gesetzt, damit das Wärmeübertragungsmedium (hauptsächlich Wasser oder Dampf) die Wärme sodann zu den Wärmeübergabestationen am jeweiligen Verbrauchsort transportieren kann. Um ein optimales Druckniveau aufrechtzuerhalten, übernehmen mit den Leitsystemen verbundene Pumpenstationen diese Aufgabe. Eine IKT-Störung bei dieser Aktivität würde zu einem Ausfall des Drucksystems führen. Bei Unterdruck könnte das Medium somit nicht mehr korrekt in allen Leitungen zirkulieren. In der Folge würden nicht mehr alle Kundinnen und Kunden versorgt. Bei Überdruck wiederum könnten die thermischen Leitungen versagen, was zu einem physischen Ausfall führen und die Versorgung ebenfalls blockieren würde. In beiden Fällen fällt bei einem Problem mit dem Leitungsdruck der Versorgungsprozess vollständig oder teilweise aus. Wenn ausserdem ein thermisches Netz sehr weitläufig ist (d. h. viele Kundinnen und Kunden werden versorgt) und grosse Kälte herrscht (Winter), kann ein Heizungsausfall Menschenleben gefährden, weshalb diese Aktivität aus Gründen der Safety ebenfalls als kritisch einzustufen ist.

3 ICS-Bedürfnisse und Einschränkungen

In den vorangegangenen Kapiteln wurde der Begriff ICS (industrielles Kontrollsystem) kurz eingeführt und erläutert, dass er sich auf Geräte zur Steuerung industrieller Systeme bezieht. Um diese Systeme wirksam zu schützen, ist es wichtig, ihre Zusammensetzung, Funktionsweise, Entwicklung und Besonderheiten genauer zu kennen.

3.1 Verschiedene Arten von ICS

Ein ICS besteht aus mehreren Steuerkomponenten, die elektrisch, mechanisch, hydraulisch oder pneumatisch sein können und die zusammenwirken, um ein gemeinsames Ziel zu erreichen, wie z. B. die Steuerung der Wärmeproduktion einer Holzfeuerungsanlage. Die Aufgabe dieses Systems ist es, Daten von variablen Prozessen oder den Zustand von Industriemaschinen zu erfassen, aber auch diese Maschinen vor Ort oder aus der Ferne zu steuern.[53] Der Oberbegriff ICS umfasst mehrere Arten von Steuerungssystemen. Zu den hier relevantesten zählen unter anderem Systeme wie SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control System) und PLC (Programmable Logic Controller).[54]

Die Besonderheit eines Kontroll- und Datenerfassungssystems (SCADA) besteht darin, Betriebskontrollen über grosse Entfernungen mithilfe von Funkwellen, Satellitenübertragung, Telefonnetz oder WAN[55] durchzuführen. Diese Art von ICS wird daher hauptsächlich im industriellen Vertrieb eingesetzt. Es ermöglicht die Zentralisierung der Erfassung, Überwachung, Steuerung und Verarbeitung von Daten aus Feldeinheiten, die geografisch über Hunderte oder Tausende von Kilometern verteilt sind. Ein SCADA-System bietet auch die Möglichkeit, mehrere lokale Operationen fernzusteuern, wie das Öffnen und Schliessen von Ventilen oder Leistungsschaltern, die Erfassung von Daten von verschiedenen Sensoren sowie die Überwachung von Feldeinheiten und die Möglichkeit, bei Bedarf zu reagieren.[56]

Im Gegensatz zu einem SCADA-System kommunizieren DCS und PLC hauptsächlich über ein lokales Netzwerk (LAN)[57] und werden zur Steuerung von Produktionssystemen am gleichen geografischen Standort eingesetzt. Mit DCS ist es möglich, einen Prozess in mehrere separate Aufgaben (Produktionsmodule) zu zerlegen und jede Aufgabe einzeln zu steuern. Diese Aufteilung erlaubt, die Auswirkungen eines Fehlers im gesamten Produktionssystem zu begrenzen. DCS sind mit Sensoren und Aktoren verbunden und verwenden eine Sollwertsteuerung, um den Materialfluss durch die Anlage zu steuern. Damit kann die Anlage in Echtzeit überwacht und gesteuert werden.[58]

Die speicherprogrammierbare Steuerung (PLC) war ursprünglich ein kleiner Industriecomputer, der grundlegende logische Funktionen wie Relais, Schalter oder Zeitgeber ausführen sollte. Heute haben sich PLC so entwickelt, dass sie in der Lage sind, komplexe Prozesse zu steuern. Sie werden häufig als Steuerungskomponente in SCADA- und DCS-Systemen eingesetzt, aber auch als Hauptsteuerung in kleinen Steuerungssystemen (wie z. B. in Automobil-Montagelinien oder Russbläsersteuerungen in Kraftwerken.[59]

[53] National Institute of Standards and Technology. «Glossary: industrial control system ICS». https://csrc.nist.gov/glossary/term/industrial_control_system (Stand 17. April 2020).

[54] Falco, J., Scarfone, k. & Stouffer, K. (2013). NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology.

[55] Beim WAN (Wide Area Network) handelt es sich um ein Weitverkehrsnetzwerk, das die Datenübertragung an eine grosse Anzahl von Benutzerinnen bzw. Benutzern über ein viel grösseres geografisches Gebiet als das LAN ermöglicht.

[56] National Institute of Standards and Technology. «Glossary: Supervisory Control and Data Acquisition SCADA». https://csrc.nist.gov/glossary/term/Supervisory_Control_and_Data_Acquisition (Strand 17. April 2020).

[57] Local Area Network: lokales Netzwerk, das Geräte am gleichen geografischen Standort verbindet. National Institute of Standards and Technology. «Glossary: Local Area Network LAN». https://csrc.nist.gov/glossary/term/Local_Area_Network (Stand 17. April 2020).

[58] National Institute of Standards and Technology. «Glossary: Distributed Control System DCS». https://csrc.nist.gov/glossary/term/Distributed_Control_System (Stand 17. April 2020).

[59] National Institute of Standards and Technology. «Glossary: Programmable Logic Controller PLC». https://csrc.nist.gov/glossary/term/Programmable_Logic_Controller (Stand 17. April 2020).

3.2 Entwicklung von ICS

ICS werden heute in vielen Industriezweigen eingesetzt, insbesondere in der Produktion und im Vertrieb. Bei Produktionsunternehmen sind ICS in der Regel an einem Standort zentralisiert (DCS und PLC), während sie bei Verteilungsunternehmen (z. B. Gas, Wasser oder Elektrizität) geografisch auf mehrere Standorte verteilt sind (SCADA).

Historisch gesehen wurden ICS auf operativer Technologie (Operational Technology, OT) implementiert. Ursprünglich war diese Betriebstechnik in erster Linie mechanisch und hing von Bedienungspersonal ab, dessen Aufgabe es war, Wähler, Hebel und andere mechanische Elemente zu bedienen, um den ordnungsgemässen Betrieb der Anlage zu ermöglichen. Steigende Nachfrage und die Notwendigkeit, die operativen Fähigkeiten zu erhöhen, beschleunigten die Automatisierung von Industrieprozessen. Bereits 1950 wurden industrielle Verfahren eingesetzt, bei denen computergesteuerte Prozessoren zur Steuerung von Aktivitäten eingesetzt wurden, insbesondere im Produktions- und Versorgungssektor.

Der Begriff «Supervisory Control and Data Acquisition System» (SCADA) wurde erstmals in den 1970er- Jahren als Bezeichnung für eine Kombination von Hardware und Software zur (automatisierten) Überwachung eines industriellen Prozesses verwendet. In ihren frühen Tagen waren SCADA-Systeme gross und vollständig proprietär. Sie verfügten nur über wenige oder gar keine Kommunikationsmittel, die nicht in den Zuständigkeitsbereich des jeweiligen Anbieters fielen. In den 1990er- und 2000er-Jahren begannen SCADA-Anbieter, offene Architekturen für ihre Produkte einzuführen, die eine Vernetzung der Systeme ermöglichen.[60]

3.3 Konvergenz zwischen IT und OT innerhalb eines ICS

Um die Kosten zu senken und das Funktionieren der Systeme zu verbessern, unter anderem durch bessere Konnektivität, Überwachung und Analyse, begann die OT mit der IT zu verschmelzen. Diese Konvergenz zwischen OT und IT hat industrielle Systeme «intelligent», d. h. verbunden und automatisiert, gemacht. Das Aufkommen der «intelligenten Industrie» wird allgemein als «Industrie 4.0» bezeichnet.[61] Infolgedessen ermöglichen die aktuellen Geräte, auf denen die OT basiert, und die darin implementierten SCADA-Systeme eine digitale Steuerung dieser Werkzeuge aus der Ferne unter Verwendung von Standard-IT-Kommunikationsprotokollen. Diese OT-IT-Konvergenz weist darauf hin, dass IT-Systeme in allen Sektoren zunehmend OT-Systemdaten nutzen und damit den allgemeinen Trend zur Automatisierung unterstützen, der für die vierte industrielle Revolution charakteristisch ist.[62]

Obwohl es eine Konvergenz zwischen IT und OT gibt, sind die beiden Technologien immer noch für unterschiedliche Aufgaben konzipiert. IT umfasst alle Computersysteme, die die tägliche Arbeit eines Unternehmens unterstützen. Dabei handelt es sich um Computer, Hilfsgeräte, Software, Firmware oder Dienste, die für die automatisierte Erfassung, Speicherung, Änderung, Steuerung, Übertragung und den Empfang von Daten oder Informationen verwendet werden.[63] OT hingegen wird für die operative, prozessbezogene Arbeit einer Organisation eingesetzt. Sie umfasst alle Geräte, die mit der physischen Umgebung interagieren und die es ermöglichen, durch die Überwachung und Steuerung bestimmter Geräte eine Veränderung zu erkennen oder zu bewirken, die sich direkt auf einen industriellen Prozess auswirkt.[64]

[60] Balmelli, Laurent. «Build a Cyber Security Program for Industrial Control Systems». Medium, 14. Februar 2020. https://medium.com/@laurentbalmelli/build-a-cyber-security-program-for-industrial-control-systems-5026064aa633 (Stand: 20.2.2020).

[61] Marr, Bernard. «What is Industry 4.0? Here's a super easy explanation for anyone». Forbes, 2. September 2018. https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#3c395f7e9788 (Stand: 2.3.2020).

[62] World Economic Forum. «What is the fourth industrial revolution?». https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/ (Stand: 2.3.2020).

[63] National Institute of Standards and Technology. «Glossary: information technology IT». https://csrc.nist.gov/glossary/term/information_technology (Stand: 17.4.2020)

[64] National Institute of Standards and Technology. «Glossary: Operational Technology OT». https://csrc.nist.gov/glossary/term/operational_technology (Stand: 17.4.2020).

3.4 Neue Anforderungen an die ICS-Sicherheit

Wie oben erläutert, hat die Konvergenz von OT und IT die Produktivität von Industrieprozessen verbessert, aber auch Nachteile mit sich gebracht. Die neue Interdependenz hat die Betriebstechnik anfälliger für Störungen von aussen gemacht und damit die Zuverlässigkeit und Sicherheit industrieller Systeme verringert. Doch diese neue Schwachstelle wurde schnell erkannt und ist seit den 2000er-Jahren Forschenden und Fachleuten im Bereich Cyber-Sicherheit ein Anliegen.

Der vom Idaho National Laboratory durchgeführte «Aurora-Generator-Test»[65] zeigte 2007 auf, wie ein Cyber-Angriff Komponenten eines Stromnetzes physisch zerstören kann. Dazu brauchte es lediglich ein paar Zeilen Code, um den Generator «selbstzerstörerisch» zu machen. Die Sicherheit der OT ist auch heute noch eine reale und sich stets verändernde Anforderung und Herausforderung, sodass sich einige der grossen Namen der IT-Branche (z. B. Microsoft, ABB, BlackBerry, Cylance, Fortinet)[66] zusammengeschlossen haben, um diese zu meistern.

Einer der Vorteile dieser Verbindung zwischen OT und IT ist die Verbesserung und Standardisierung der TCP/IP-Konnektivität. Obwohl ICS dadurch auch Angriffen auf der Basis von IP-Adressen ausgesetzt sind. Es ist daher wichtig, die verschiedenen Zugangspunkte zu sichern (Endpoint Security), d. h. sicherzustellen, dass alle Elemente, die an ein eingeschränktes Netz angeschlossen sind, sicher und konform sind. Wie bei einem IKT-Netzwerk müssen auch im Falle eines ICS Brancheninformationen wie Betriebs- und Finanzdaten gesichert werden. Der Zugang zu diesen Informationen ist für Angreiferinnen und Angreifer von grossem Interesse, da sie diese leicht z. B. durch Ransomware zu Geld machen oder sogar anhand von raffinierteren Cyber-Angriffen eine physische Zerstörung der industriellen Infrastruktur herbeiführen können.

Zusätzlich zu diesen wenigen Beispielen hat die Sicherheit eines ICS auch eine physische Dimension. Die Zuverlässigkeit und Sicherheit des Prozesses muss gewährleistet sein, da – wie der oben erwähnte Fall des Aurora-Generators zeigt – eine digitale Sicherheitsverletzung zur Zerstörung physischer Elemente führen kann, was direkte Auswirkungen auf das menschliche Leben, die Produktion oder den Vertrieb haben kann.[67]

Die Interkonnektivität und Interdependenz der ICS für den Vertrieb, die Teil der kritischen Infrastruktur der Schweiz sind, ist gross. Infolgedessen kann der Ausfall eines wichtigen Elements zu kaskadierenden Ausfällen und damit zu immer schwereren Störungen führen. Es ist daher von grösster Wichtigkeit, diese zu schützen.

3.5 Sicherheitseinschränkungen für ICS

Ein ICS arbeitet basierend auf den spezifischen Bedürfnissen, die mit der Art der physikalischen Prozesse der verschiedenen in den Feldeinheiten vorhandenen Controller (z. B. PLC) zusammenhängen. Es ist daher wichtig, diese Einschränkungen bei der Entwicklung eines Sicherheitsprogramms zu berücksichtigen, um geeignete Sicherheitsmassnahmen anwenden zu können.

Ein ICS stützt sich auf operative Systeme, die in Echtzeit arbeiten, was bei der Anwendung aktiver Sicherheitsmassnahmen zu einer problematischen Zeit- und Leistungseinschränkung führen kann. Tatsächlich können solche aktiven Massnahmen die Ausführung des Systems in Abhängigkeit von sicherheitsrelevanten Ereignissen beeinflussen. Um dieses Problem zu vermeiden, werden bei den aktuellen ICS-Überwachungslösungen passive Massnahmen bevorzugt.

[65] CNN. Staged cyber attack reveals vulnerability in power grid. https://edition.cnn.com/2007/US/09/26/power.at.risk// (Stand: 2.3.2020).
[66] Businesswire. New Operational Technology Cyber Security Alliance Launches to Deliver Comprehensive Cyber Security Guidelines for Operational Technology. https://www.businesswire.com/news/home/20191021005857/en/New-Operational-Technology-Cyber-Security-Alliance-Launches (Stand: 2.3.2020).
[67] Balmelli, Laurent. «Build a Cyber Security Program for Industrial Control Systems». Medium, 14. Februar 2020. https://medium.com/@laurentbalmelli/build-a-cyber-security-program-for-industrial-control-systems-5026064aa633 (Stand: 20.2.2020).

Eine weitere Anforderung an ein ICS ist die Notwendigkeit eines kontinuierlichen Betriebs. Aus diesem Grund werden Unterbrechungen oft Tage oder Wochen im Voraus geplant. Gängige IT-Praktiken, wie z. B. das Neustarten einer Komponente, sind nicht möglich und würden sich negativ auf die Zuverlässigkeit des Systems und seine Verfügbarkeit und Wartbarkeit auswirken. Dieser kontinuierliche Betrieb hat einen direkten Einfluss auf den gesamten Change-Management-Prozess und macht das Patch- und Schwachstellen-Management in ICS generell zu einer schwierigen Aufgabe. Die typische Lebensdauer der Komponenten, die in der Grössenordnung von 10 bis 15 Jahren liegt, erschwert diese Aufgabe zusätzlich. Eine derart lange Lebensdauer steht im Allgemeinen im Widerspruch zum rasanten Tempo des technologischen Wandels.

Ein ICS hat auch Ressourcenbeschränkungen, insbesondere wegen der Forderung nach Echtzeitausführung. Die Komponenten eines ICS verfügen daher nicht über alle typischen IT-Funktionalitäten wie Verschlüsselung, Fehlerprotokollierung oder Passwortschutz, was ICS verwundbarer machen. Das Bewusstsein für das Sicherheitsbedürfnis ist jedoch seit der Entdeckung bestimmter Malware (wie Stuxnet)[68] gestiegen und hat zu einem Umdenken sowohl auf Kunden- als auch auf Anbieterseite geführt.[69]

[68] Diese Malware wurde 2010 entdeckt. Es war die erste Cyberwaffe, die ein industrielles Ziel angreifen sollte. Sie war in der Lage, ein ICS auszuspionieren und PLC umzuprogrammieren, wobei die vorgenommenen Änderungen verborgen blieben.

[69] Balmelli, Laurent. «Build a Cyber Security Program for Industrial Control Systems». Medium, 14. Februar 2020. https://medium.com/@laurentbalmelli/build-a-cyber-security-program-for-industrial-control-systems-5026064aa633 (Stand: 20.2.2020).

3.6 Sicherheitsunterschiede zwischen den IT- und OT-Komponenten eines ICS

Zuvor wurde erklärt, dass es seit einigen Jahren eine Konvergenz zwischen Computer- und Betriebstechnologien gibt (IT und OT). Diese Konvergenz vollzieht sich im OT-Teil des ICS-Netzwerks in Form von Industriegeräten, die IT-Standards unterstützen, und durch die zunehmende Präsenz von Universalrechnern, die unter einem standardisierten Betriebssystem laufen.

Trotz dieser Konvergenz können die beiden Technologien allerdings nicht auf die gleiche Weise geschützt werden. Es ist notwendig, die zum Schutz von OT und IT eingesetzten Sicherheitsmittel anzupassen. Die Komponenten des IT-Teils eines Netzwerks, die sich auf die organisatorischen Aufgaben einer Organisation beziehen, funktionieren wie die meisten gängigen IT-Geräte mit einer klassischen Antivirenlösung, regelmässigen Updates und einem eher kurzen Lebenszyklus von zwei bis drei Jahren. Die Komponenten des OT-Teils eines Netzwerks, die mit der operativen bzw. industriellen Arbeit verbunden sind, erfordern hingegen besondere Sicherheitsmassnahmen (siehe Kapitel 3.5). Um geeignete Sicherheitsmassnahmen anwenden zu können, beschreibt Tabelle 1 die wichtigsten Sicherheitsunterschiede zwischen dem OT- und dem IT-Teil eines ICS.

Sicherheitsthema	IT (z. B. Verwaltung von E-Mails, Druckern, Telefonen usw.)	OT (z. B. SCADA, DCS, PLC)
Antivirus	Weit verbreitet. Einfach zu installieren und zu aktualisieren. Möglichkeit zur Personalisierung. Antivirenschutz lässt sich auf Geräte- oder Unternehmensebene konfigurieren.	Der Speicherbedarf und die Verzögerung des Datenaustauschs durch den Scanvorgang der Antiviren-Software können sich negativ auf ein ICS aus-wirken. Ältere ICS-Komponenten lassen sich meist nur mit Produkten aus dem Sekundärmarkt schützen. Antivirenlösungen verlangen zudem im ICS-Umfeld oft nach «Ausnahme»-Ordnern, um zu verhindern, dass geschäftskritische Dateien unter Quarantäne gestellt werden.

Tabelle 1: Sicherheitsunterschiede zwischen IT und OT

Sicherheitsthema	IT (z. B. Verwaltung von E-Mails, Druckern, Telefonen usw.)	OT (z. B. SCADA, DCS, PLC)
Sicherheitsupdate (Update Management)	Klar definiert, unternehmensweit ausgeführt, automatisiert über Fernzugriff.	Lange Vorlauf- und Planungszeit bis zur erfolgreichen Patch-Installation; immer herstellerspezifisch; kann das ICS (temporär) zum Erliegen bringen. Festlegen des diesbezüglich akzeptablen Risikos notwendig.
Technologie-lebenszyklus (Technology Support Lifecycle)	2–3 Jahre, mehrere Anbieter, laufende Weiterentwicklung und Upgrades.	10–20 Jahre, i.d.R. derselbe Anbieter bzw. Dienstleister über den gesamten Lebenszyklus; Ende des Lebenszyklus verursacht neue Sicherheitsgefährdungen.
Methoden für Tests und Audits (Testing and Audit Methods)	Einsatz von modernen (möglichst automatisierten) Methoden. Die Systeme sind i.d.R. resilient und zuverlässig genug, um Assessments im laufenden Betrieb zu ermöglichen.	Automatisierte Assessmentmethoden u. a. aufgrund des hohen Individualisierungsgrads häufig nicht geeignet. Hohe Fehleranfälligkeit während Assessments, weshalb diese im laufenden Betrieb tendenziell schwierig durchzuführen sind.
Change Management	Regulär und in regelmässigem Rhythmus geplant. Abgestimmt auf die Unternehmensvorgaben zur minimalen/maximalen Einsatzdauer.	Komplexer Prozess mit potenziellen Auswirkungen auf die Geschäftstätigkeit. Strategische, individuelle Planung notwendig.
Asset-Klassifikation (Asset Classification)	Relativ üblich, wird jährlich ausgeführt. Ausgaben/Investitionen werden gemäss den Ergebnissen geplant.	Wird nur durchgeführt, wenn dies notwendig und vorgeschrieben ist. Ohne Inventar sind Gegenmassnahmen oftmals nicht auf die Bedeutung des Systemelements zugeschnitten.
Vorfallreaktion/ -analyse (Incident Response and Forensics)	Einfach zu entwickeln und umzusetzen. Unter Umständen sind regulatorische Vorschriften (Datenschutz) zu beachten.	Fokussiert primär auf den Neustart des Systems. Forensikprozesse wenig entwickelt.
Physische Sicherheit (Physical Security)	Variiert zwischen gering (Büroinformatik) bis hoch (gesicherte Rechenzentren).	Variiert zwischen gering (Einfamilienhaus) bis hoch (gesicherte Rechenzentren).
Sichere System-entwicklung (Secure Software Development)	Integraler Teil des Entwicklungsprozesses.	ICS werden historisch bedingt meist als physisch isolierte Systeme konzipiert. Sicherheit als integraler Teil der Systementwicklung ist entsprechend wenig verbreitet. Anbieter von ICS haben diesbezüglich Fortschritte gemacht, jedoch weniger grosse als im IT-Bereich. Kernelemente von ICS lassen oft keine nachträglichen Sicherheitslösungen zu.
Sicherheitsvorgaben (Safety Rules)	Allgemeine regulatorische Vorgaben, branchenabhängig (nicht alle Branchen).	Branchenspezifische regulatorische Richtlinien (nicht alle Branchen).

Tabelle 1: Sicherheitsunterschiede zwischen IT und OT

3.7 Wiederkehrende Angriffe auf ICS

In Kapitel 3 wurden bisher die Definition, der Betrieb, die Entwicklung sowie sicherheitsspezifische Aspekte von ICS erörtert. Als letztes Element gilt es Angriffe gegen ICS zu berücksichtigen. Aufgrund ihrer komplexen Architektur weisen ICS bestimmte Schwachstellen auf, die in den schwerwiegendsten Fällen sehr lange Zeit unerkannt bleiben können. Wenn diese Schwachstellen ausgenutzt werden, können sie zu einer fortgeschrittenen anhaltenden Bedrohung (Advanced Persistent Threat)[70] werden. Um dies zu veranschaulichen, werden hier einige typische Angriffsmethoden für ICS aufgeführt, gegen die das Sicherheitsprogramm des Minimalstandards einen angemessenen Schutz bietet:

- Angriffe aus dem Internet auf ein online zugängliches ICS mit dem Ziel, einen dauerhaften Fernzugriff zu etablieren.
- Fernzugriffe auf das ICS unter Ausnutzung gestohlener Zugangsdaten.
- Angriffe auf das ICS durch Ausnutzen von Schwachstellen der Webschnittstelle.
- Einschleusen von Malware in das ICS über kompromittierte Datenträger (z. B. USB-Sticks, Smartphones).
- Angriffe über IT-Systeme (z. B. mittels Phishing-Mails, Drive-by-Infektionen) mit dem Ziel, über allfällige Schnittstellen in das ICS einzudringen.

[70] Es handelt sich um einen diskreten und gezielten Cyber-Angriff, der über einen langen Zeitraum wirksam ist. Im Allgemeinen besteht das Ziel eines Advanced Persistent Threat darin, die Netzwerkaktivität zu überwachen und/oder Daten zu stehlen, ohne das Netzwerk zu beeinträchtigen.

4 Cyber-Sicherheitsprogramm

Als Grundlage für das Cyber-Sicherheitsprogramm des IKT-Minimalstandards wurde das NIST Framework Core gewählt. Diese amerikanische Methodik[71], die vom National Institute of Standards and Technology (NIST) entwickelt wurde, bietet einen umfassenden und vor allem kontinuierlichen Schutz für IKT-Geräte. Ziel des NIST Framework Core und seiner Empfehlungen ist es, den Betreiberinnen und Betreibern von kritischen Infrastrukturen und weiteren von IKT abhängigen Organisationen ein Instrument zur Verfügung zu stellen, mit dem diese selbstständig und eigenverantwortlich ihre Resilienz gegenüber IKT-Sicherheitsrisiken erhöhen können. Zusätzlich bietet es eine ausgewogene Kombination an Sicherheitsmassnahmen zwischen gemeinsamer IT und spezifischen OT-Komponenten. Das NIST Framework Core basiert auf einer Auswahl an bestehenden Standards, Richtlinien und Best-Practice-Vorgaben und ist technologieneutral. Zusätzlich ist es kompatibel zu den Standards ISO 2700x.

In seinem Sicherheitsprogramm kombiniert das NIST Framework Core einen risikobasierten Ansatz mit einer umfassenden Defense-in-depth-Strategie. Die Analyse eines akzeptablen Risikos ist für eine Organisation von entscheidender Bedeutung, da ihr dies ermöglicht, die Kernmassnahmen des NIST-Rahmens auf ihre eigenen Bedürfnisse anzupassen (je nach Branche, Grösse, Ressourcen und Bedrohungen). Nach dieser Analyse ist jede Organisation in der Lage, auf der Grundlage ihrer Ressourcen das optimale Schutzniveau zu bestimmen, das erreicht werden soll. Die Defense-in-depth-Strategie ihrerseits ist ein vom militärischen Prinzip abgeleiteter Ansatz, wonach ein komplexes vielschichtiges Verteidigungssystem schwieriger zu überwinden ist als eine einfache Barriere. Ziel dieser Strategie ist es daher, mehrere Sicherheitsmassnahmen auf unterschiedlichen Schutzniveaus anzuwenden (die z. B. vom Netzwerkschutz über den Schutz physischer Elemente bis hin zur Ausbildung des Personals reichen) und so potenzielle Angreiferinnen und Angreifer zur Überwindung einer Vielzahl komplexer Sicherheitshindernisse zu zwingen.

Das letzte Element dieses Sicherheitsprogramms betrifft die Massnahmen des NIST Framework Core. Es handelt sich um etwa 100 Massnahmen, die in fünf Funktionen unterteilt sind: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Jede Organisation muss alle diese Massnahmen bewerten (zwischen 0 und 4), damit sie ihre Schwächen erkennen und entsprechende Sicherheitslösungen anwenden kann. Die Beurteilung dieser Massnahmen bietet einen umfassenden Sicherheitsrahmen, mit dem Organisationen ihr Sicherheitsprogramm kontinuierlich an ihre Bedürfnisse anpassen können. Weitere Informationen und Einzelheiten zu allen Sicherheitsmassnahmen des NIST Frame-work Core werden in Kapitel 5 ausführlich erörtert.

4.1 Risikomanagement

Das Risikomanagement ist ein erster Schritt der Defense-in-depth-Strategie, der Unternehmen hilft, ihre Risiken und ihre Risikoneigung (akzeptables Risiko) zu identifizieren. Ziel ist es, korrekt zu definieren, welche Ressourcen eingesetzt werden sollen, welches Schutzniveau erreicht werden soll und vor welchen Risiken man sich schützen möchte.

4.1.1 Risikomanagementprogramm

Voraussetzung zur Implementierung einer Defense-in-depth-Strategie ist das Verständnis der Geschäftsrisiken einer Organisation aufgrund von IKT-Bedrohungen. Diese Risiken müssen entsprechend der Risikoneigung des Unternehmens bewirtschaftet werden. Die Verantwortlichen für Betrieb und Unterhalt der IKT-Systeme müssen Cyber-Risiken erkennen, bewerten und adressieren können. Dafür braucht es ein klares Verständnis der Bedrohungsszenarien, der operativen und technischen Prozesse sowie der eingesetzten Technologien. Erst dann kann eine Defense-in-depth-Strategie in das normale Tagesgeschäft integriert werden. Es ist Aufgabe des Managements, «Sicherheit» als Voraussetzung aller IKT-gesteuerten Aktivitäten in der Organisation zu etablieren.

[71] *National Institute of Standards and Technology. An Introduction to the Components of the Framework. https://www.nist.gov/cyberframework/online-learning/components-framework (Stand: 9.1.2020).*

Die oben stehenden Grundsätze im Umgang mit Risiken gelten generell. Gewisse IKT-Anwendungen sind aufgrund ihrer Kritikalität aber von spezieller Bedeutung. Dazu gehören insbesondere industrielle Kontrollsysteme (ICS). Das Design einer wirkungsvollen ICS-Sicherheitsarchitektur setzt voraus, dass die Unternehmensrisiken in Relation zu den funktionalen (operativen) Anforderungen an das ICS gestellt werden. Das kann auch die physische Welt betreffen (z. B. Perimeterschutz um Rechenzentren). Entscheidungsträgerinnen und -träger auf allen Ebenen der Organisation müssen die Bedeutung von Cyber-Risiken kennen und sich aktiv in den Risikomanagementprozess einbringen. Regelmässige Risikoanalysen für kritische Systeme, Applikationen und Prozesse, inklusive der zugehörigen Netzwerke, sind unabdingbar. Diese Analysen sollten nach strengen Vorgaben durchgeführt und dabei ein strukturierter, systematischer Ansatz verwendet werden.

4.1.2 Risikomanagementframework

IKT-Risikoanalysen sollen in ein Risikomanagementframework eingebettet sein und regelmässig für klar definierte Untersuchungsobjekte durchgeführt werden. Dies gilt beispielsweise für geschäftskritische Anlagen, Prozesse und Applikationen (auch in der Entwicklungsphase) sowie für deren Abhängigkeiten von weiteren Systemen, Netzen und Diensten. Das Ziel des Risikomanagementframeworks ist, den identifizierten Risiken verantwortliche Personen/Rollen zuzuweisen, die die Risiken überwachen (Monitoring), beurteilen und adäquate Massnahmen umsetzen, um die Risiken innerhalb der vorgängig definierten akzeptablen Grenzen zu halten (= Risikoneigung).

4.1.3 Risikoanalyse

Der Umfang der IKT-Risikoanalyse soll klar abgesteckt sein. Die betroffenen Geschäftsprozesse und die betreffenden technischen Elemente sowie mögliche externe Faktoren müssen beschrieben werden und ihre Gewichtung in der Analyse festgelegt sein. Damit werden auch die Inhalte und Grenzen der Analyse definiert.

4.1.4 Business-Impact-Analyse

Im Rahmen einer Business-Impact-Analyse sollen die potenziell realistischste und die potenziell schlimmste Auswirkung (auf die Geschäftstätigkeit) aufgrund der Störung einer IKT-Komponente (inkl. Personen, Daten, Prozesse, Dienste, Netze) für unterschiedliche Kategorien erhoben werden (z. B. Reputations-, finanzielles, operatives, rechtliches, gesundheitliches Risiko). Schlussendlich muss festgelegt werden, welche Auswirkungen auf die Geschäftstätigkeit das Unternehmen zu tragen bereit ist, falls die dafür notwendigen IKT-Ressourcen nicht wie vorgesehen verfügbar sind. Entsprechend sind die Anforderungen und Schutzniveaus zu definieren, die notwendig sind, um die Verfügbarkeit, Integrität und Vertraulichkeit der entsprechend dem akzeptablen Risiko identifizierten IKT-Ressourcen zu gewährleisten.

4.1.5 Risikomassnahmen

Zu den in der Business-Impact-Analyse beschriebenen Risiken sollen Massnahmen identifiziert, überprüft und validiert werden. Diese Massnahmen sind anschliessend zusammen mit den Plänen zum exakten Vorgehen durch die Geschäftsleitung freizugeben. Dabei muss das Restrisiko für alle Betriebsmittel im entsprechenden Umfeld ermittelt und in geeigneter Weise (z. B. gemildert, vermieden, übertragen oder akzeptiert) und gemäss der Risikoneigung des Unternehmens gesteuert werden. Für jedes einzelne Betriebsmittel (engl. «asset») soll so das maximal akzeptable Risiko bestimmt werden, um die (kumulierten) IKT-Risiken bewerten zu können.

4.2 Defense-in-depth-Strategie

4.2.1 Umsetzung der Defense-in-depth-Strategie

Die IT-Sicherheitsstrategie eines Unternehmens ist auf den Schutz der für die Geschäftsprozesse notwendigen kritischen IKT-Ausrüstung auszurichten. Dies erfordert einen mehrschichtigen Ansatz. Im Bereich Cyber-Sicherheit zielt die Defense-in-depth-Strategie darauf ab, Verletzungen der IKT-Sicherheit zu erkennen, darauf zu reagieren und die Folgen der Sicherheitsverletzung zu reduzieren. Defense-in-depth verfolgt einen ganzheitlichen Ansatz, der die gesamte (IKT-)Ausrüstung gegen beliebige Risiken zu schützen versucht. Die Ressourcen des Unternehmens sollen so eingesetzt werden, dass der Schutz vor bekannten Risiken sowie die Überwachung potenzieller zukünftiger Risiken gewährleistet ist. Die entsprechenden Massnahmen müssen die Gesamtheit der IKT-Systeme schützen. Dazu gehören Personen, Prozesse, Gebäude, Daten und Geräte. Angreiferinnen und Angreifer stellen erst dann eine Bedrohung für ein IKT-System dar, wenn es ihnen gelingt, eine existierende Schwachstelle bei einem dieser Elemente zu finden und auszunutzen. Die Unternehmen sind gehalten, die Wirksamkeit der Schutzmassnahmen regelmässig zu überprüfen und gegebenenfalls an neue Bedrohungen anzupassen.

Folgende Faktoren sind bei der Anwendung eines Defense-in-depth-Konzeptes zur Verringerung von Bedrohungen für ICS/SCADA zu berücksichtigen:

- Die Kosten, um alte Systeme nach zeitgemässen Bedürfnissen abzusichern.
- Der wachsende Trend, ICS mit Geschäftsnetzwerken zu verbinden.
- Die Möglichkeit, Fernzugriffe für die Anwenderinnen und Anwender sowie die Lieferanten (Dienstleistungsanbieter) zu ermöglichen, und zwar sowohl im IT- als auch im OT-Umfeld.
- Vertrauen in die eigene Zulieferkette (Supply Chain).
- Zeitgemässe Möglichkeiten, ICS-spezifische Protokolle zu überwachen und zu schützen.
- Die Möglichkeit, das Fachwissen über sich neu entwickelnde Bedrohungen für ICS stets aktuell zu halten.

Der Defense-in-depth-Ansatz erschwert direkte Angriffe auf IKT-Systeme und erhöht die Wahrscheinlichkeit, auffälliges oder unübliches Verhalten innerhalb des Systems frühzeitig zu entdecken. Dieser Ansatz ermöglicht auch die Schaffung von gesonderten Zonen u. a. für die Implementierung von Technologien, die ein Eindringen ins System erkennen können (Intrusion Detection Technology).

Für einen umfassenderen Überblick über dieses Konzept wird in Tabelle 2 eine Auswahl verschiedener Schutzebenen der Defense-in-depth-Strategie des NIST Framework Core dargestellt und in den folgenden Unterkapiteln näher erläutert.

Repräsentative Elemente der Defense-in-depth-Strategie	
Schutz der Applikationen (Monitoring)	• Intrusion Detection Systems IDS (Eindringungserkennungssysteme) • Sicherheits-Audit-Logging • Sicherheitsvorfall und Event-Überwachung
Schutz des Hosts	• Patch- & Schwachstellen-Management • Endgeräte • Virtuelle Geräte
Schutz des Netzes	• Standards/Empfehlungen • Richtlinien und Vorgehensweisen • Standardisierte Sicherheitszonen • Virtual LAN
Schutz des Netzwerk-Perimeters	• Demilitarized Zones (DMZ) und Firewall • Fernzugriff & Authentifizierung • Jump Server/Hosts
Schutz der physischen Elemente	• Schutz von Endgeräten • Zugangskontrollen zum Kontrollzentrum • Videoüberwachung, Zugangskontrollen & Barrieren
Lieferantenmanagement	• Lieferketten-Überwachung & -Management • Managed Services & Outsourcing • Nutzung von Cloud-Diensten • Management des Fernzugriffs
Mitarbeitermanagement	• Richtlinien • Vorgehensweisen • Schulung und Bewusstmachung
Informationssicherheitsstrategie	• Klare Richtlinien • Anwendung der Informationssicherheitsstrategie • Kontrolle der Informationssicherheitsstrategie

Tabelle 2: Repräsentative Elemente der Defense-in-depth-Strategie

4.2.2 Schutz der Applikationen (Monitoring)

Der Einsatz von Monitoring-Systemen und Netzwerk-Komponenten, die abnormale Verhaltensweisen[72] und Angriffssignaturen[73] erkennen, bringen zusätzliche Komplexität in eine IT-Umgebung oder ein ICS. Allerdings sind die Überwachungs- und Erkennungsfunktionen für das Defense-in-depth-Konzept zum Schutz kritischer Betriebsmittel unerlässlich. Um kritische Assets vor unbefugtem Zugriff zu schützen, reicht eine elektronische Barriere um das ICS-Netzwerk nicht aus. Nach dem Defense-in-depth-Konzept soll ein Monitoring-System eine Organisation bei einem Sicherheitsvorfall frühzeitig alarmieren. Die meisten Organisationen verfügen über ein gewisses Standard-Monitoring in der IT-Umgebung, das sie aber mehrheitlich nicht in den ICS-Netzwerken einsetzen.

Deshalb ist es unerlässlich, umfassende, unabhängige und regelmässige Sicherheits-Audits (kritische Bereiche im Unternehmen, Prozesse, Anwendungen und unterstützte Systeme/Netzwerke) durchzuführen, die Datenflüsse in IKS-Systemen zu überwachen, um unangemessenes Verhalten aufzudecken, IT-Risiken zu überwachen, sicherheitsrelevante gesetzliche, regulatorische und vertragliche Anforderungen zu erfüllen und die Geschäftsleitung regelmässig über die IT-Sicherheit zu informieren.

4.2.3 Schutz des Hosts

Auf Host- resp. Workstation-Ebene muss eine weitere Sicherheitsschicht implementiert werden. Firewalls schützen die meisten Geräte gegen das Eindringen von aussen. Allerdings erfordert ein gutes Sicherheitsmodell mehrstufige Verteidigungsschichten. Zur vollständigen Sicherung des Netzwerks gehört auch die Sicherung aller Hosts (Server, Verbindungen, Endgeräte). Eine solche Schicht für die Host-Sicherheit soll Betreiberinnen und Betreibern ermöglichen, verschiedene Betriebssysteme und Anwendungen zu nutzen, während ein adäquater Schutz der Geräte sichergestellt ist.

Es muss ein Konzept zu Passwortrichtlinien für alle Anwenderinnen und Anwender auf einem System erstellt werden und die bekannten Accounts (wie z. B. «Administrator») müssen umbenannt und mit einem neuen Passwort versehen werden. Zu restriktive Passwortrichtlinien werden von den Anwenderinnen und Anwendern möglicherweise unterlaufen, indem die Passwörter unsicher aufbewahrt (z. B. Notizzettel) oder immer wieder ähnliche Passwörter verwendet werden. Die Komplexität der Passwortbestimmungen soll der Berechtigungsstufe der Anwenderinnen und Anwender angemessen sein. Optional können Zyklen zum Wechsel der Passwörter definiert werden.

Die folgenden allgemeinen Empfehlungen sollen durch die Organisationen für jeden ICS-Host und jedes Gerät, das Zugriff auf das Unternehmensnetzwerk hat, umgesetzt werden (unabhängig vom Betriebssystem):

- Installation und Konfiguration einer host-basierten Firewall.
- Deaktiviertes Autologin.
- Bildschirmschoner mit kurzen Intervallen und Aufforderung zur Passworteingabe wo möglich (Autologout aktiviert).
- Regelmässige Patches für Betriebssysteme und Aktualisierung Firmware.
- Konfiguration von Logs auf allen Geräten aktiviert.
- Nicht benutzte Services und Accounts deaktivieren, auch solche, die gar nicht mehr benutzt werden.
- Nicht sichere Services, wie Telnet, Remote Shell oder FTP, durch sichere Alternativen wie sTelnet, SSH, sFTP usw. ersetzen.
- Anwenderinnen und Anwender können Services nicht deaktivieren.
- Backups von Systemen durchführen und prüfen, besonders, wenn diese nicht zentral gesteuert werden.
- Vom Betriebssystem bereitgestellte Sicherheitsmodule wie Sicherheitsscanner aktivieren oder durch eine adäquate Software ersetzen.
- Für Laptops und andere mobile Geräte, die nicht durchgehend mit dem Firmennetz verbunden sind, gelten die gleichen Richtlinien. Bei mobilen Geräten Harddisk zusätzlich verschlüsseln.

[72] Intrusion Detection Systems zur Anomalieerkennung analysieren den Netzwerkfluss und reagieren, wenn sie abnormales Verhalten entdecken.

[73] Signaturbasierte Intrusion Detection Systems speichern Bibliotheken mit Angriffsbeschreibungen und reagieren, wenn sie einen dieser Angriffe im Netzwerk erkennen.

4.2.4 Schutz des Netzes

Die Cybersicherheits-Architektur umfasst die spezifischen Massnahmen und ihre strategische Platzierung innerhalb des Netzwerks zur Etablierung einer Sicherheitsschicht im Sinne der Defense-in-depth-Strategie. Sie soll zudem die Erfassung von Informationen zum Datenfluss zwischen allen Systemen und deren Verbindungen ermöglichen. Ebenso soll die Cybersicherheits-Architektur auf das physische Inventar der Anlagen und die IKT-Betriebsmittel abgestimmt sein, um ein ganzheitliches Verständnis der Informationsflüsse innerhalb der Organisation sicherzustellen.

Die Cybersicherheits-Architektur soll im Einklang mit dem NIST Framework Core stehen. Sie berücksichtigt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten, Diensten und Systemen. Zur Umsetzung soll ein Implementierungsplan erstellt werden, der sich an der Unternehmenskultur und den strategischen Zielen orientiert, gleichzeitig aber dem Sicherheitsbedürfnis angemessen Rechnung trägt und den diesbezüglichen Ressourcenbedarf ausweist. In der Regel wird die Cybersicherheits-Architektur durch einen integrierten Aufgabenplan ergänzt, der erwartete Ergebnisse (Indikationen und Auslöser für die weitere Überprüfung und Ausrichtung) identifiziert, Projektzeitpläne festlegt, Ressourcenbedarfsabschätzungen liefert und wesentliche Projektabhängigkeiten identifiziert.

4.2.4.1 Hauptkomponenten einer Netzwerkarchitektur

In diesem Unterkapitel werden verschiedene Konzeptmodelle auf der Grundlage von Verteilungs-ICS (hauptsächlich SCADA) diskutiert. Allerdings sind nicht alle diese Elemente ausschliesslich SCADA-Systemen vorbehalten und können daher auch auf andere Arten von ICS übertragen werden.

Wie bereits erläutert, besteht eine der Besonderheiten eines SCADA-Systems in seiner Fähigkeit, über grosse Entfernungen mittels WAN, Funkwellen oder Telefonnetz zu kommunizieren, sodass es mit all seinen über mehrere Standorte verteilten Feldeinheiten verbunden bleiben kann. Ein SCADA-System ermöglicht es daher, die Überwachung und Verwaltung von Daten, die von den Feldstandorten (Field Sites) kommen, in einem Kontrollzentrum zu zentralisieren. Das Kontrollzentrum beherbergt in der Regel einen SCADA-Server[74], Engineering Workstations (EWS, Engineering-Arbeitsstationen), Human Machine Interfaces (HMI, Mensch-Maschine-Schnittstellen) und einen Data Historian[75], bei dem es sich um eine zentralisierte Datenbank handelt, die eine Datenanalyse unter Verwendung statistischer Prozesssteuerungstechniken ermöglicht. Die Rolle des SCADA-Servers ist wichtig, da er die Verbindung zwischen dem Kontrollzentrum und den Feldstandorten über PLC oder Remote Terminal Unit (RTU, Fernbedienungsterminal) herstellt. Diese ermöglichen es den Betreiberinnen und Betreibern, vom Kontrollzentrum aus Ferndiagnosen und reparaturen an den Feldstandorten durchzuführen und auch physikalische Prozesse über die Aktoren und Sensoren, an die sie angeschlossen sind, zu steuern.

Alle Elemente, die zu den Kontrollzentren und Feldstandorten gehören, werden im Allgemeinen unter dem Namen Kontrollnetzwerk (Control Network) zusammengefasst und stellen den OT-Teil des Netzwerks dar, da sie direkt mit der operativen Arbeit verbunden sind. Im Gegensatz dazu gibt es den IT-Teil des Netzwerks, der auch als Unternehmensnetzwerk (Corporate Network) bezeichnet wird und die Backoffice-Funktionen beherbergt, die zur Verwaltung der organisatorischen und finanziellen Aspekte des Unternehmens erforderlich sind.[76] Im Allgemeinen hat das Unternehmensnetzwerk Zugang zu allen Kontrollzentren und Aussendienststandorten, z. B. für die Fehlerbehebung und Wartung. Aus Sicherheitsgründen ist das Kontroll-Netzwerk in der Regel durch Firewall-Technologie und/oder eine Demilitarized Zone (DMZ) vom Unternehmensnetzwerk getrennt, um den Zugriff auf alle operativen Systeme zu vermeiden. Weitere Informationen über den Umfang der Netzwerksicherheit finden sich in Unterkapitel 4.2.5.

Es gibt mehrere Möglichkeiten, ICS zu implementieren. Die verwendete Architektur hängt hauptsächlich von der Branche und dem Umfang des Betriebs ab. Abbildung 13 veranschaulicht die allgemeine Funktionsweise sowie die verschiedenen Komponenten eines ICS-Systems, die in diesem Kapitel dargelegt wurden. Es handelt sich eher um ein Erklärungsmodell als um ein reales Modell und orientiert sich an einem ICS im Vertrieb.[77]

[74] Auch bekannt als: Control Server, Master Terminal Unit (MTU) oder Supervisory Controller.

[75] National Institute of Standards and Technology. «Glossary: data historian». https://csrc.nist.gov/glossary/term/Data_Historian (Stand: 29.4.2020).

[76] Es gilt zu beachten, dass ein Data Historian auch im Unternehmensnetzwerk vorhanden sein kann.

[77] Falco, J., Scarfone, k. & Stouffer, K. (2013). NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology.

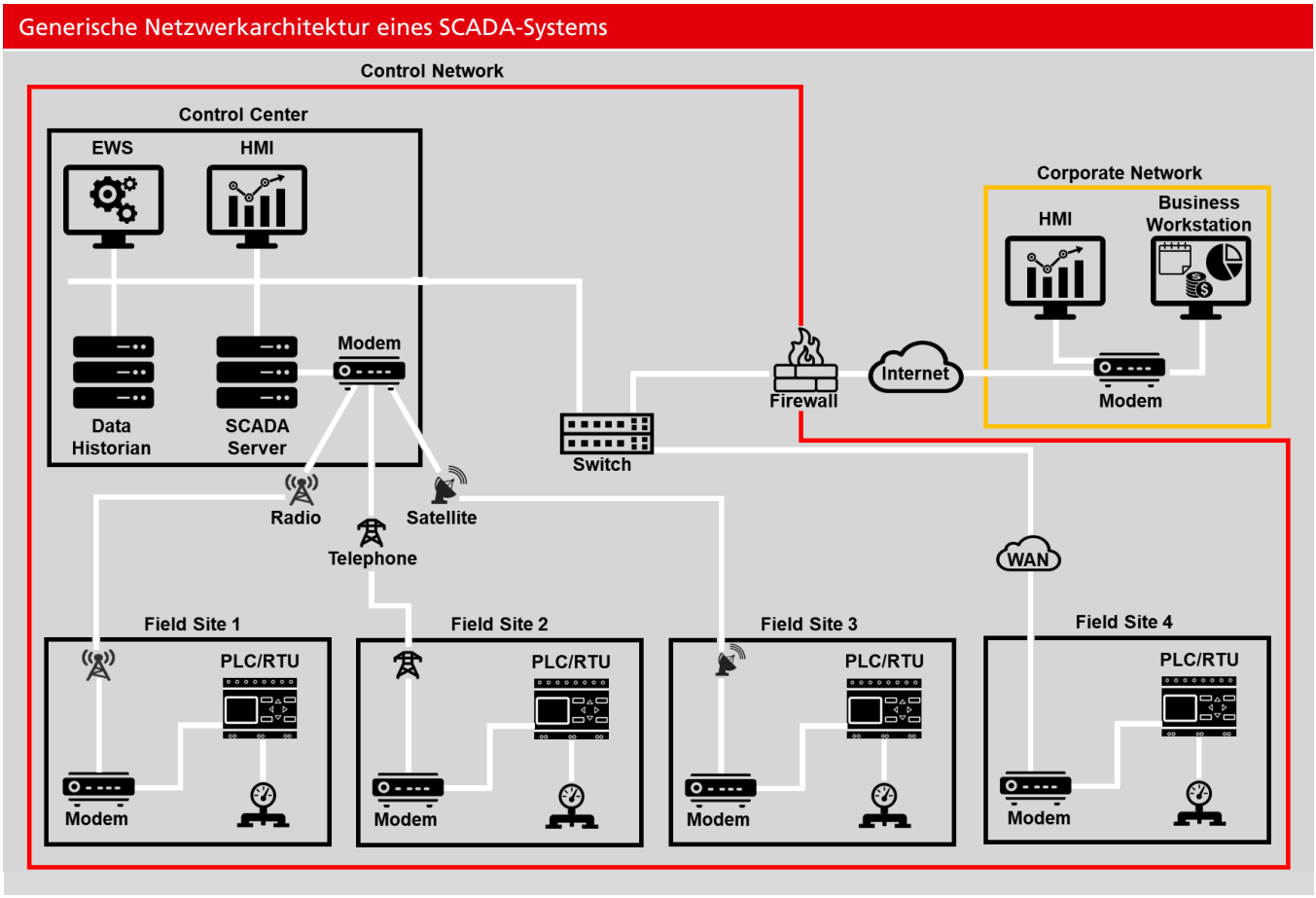

Abbildung 13: Generische Netzwerkarchitektur eines SCADA-Systems

4.2.4.2 Segmentierung der Netzwerkarchitektur

Eine sichere und robuste Netzwerkarchitektur bildet eine der wichtigsten Voraussetzungen für einen erfolgreichen Schutz gegen Angriffe. Jede Schnittstelle, jeder Übergang und jede Verbindung stellt eine potenzielle Gefahr dar. Daher ist es zwingend erforderlich, dass sämtliche Prozesse in den verschiedenen Netzen sowie Geräten und Anlagen bekannt sind und entsprechend gesteuert werden. Dabei bilden die richtige Gruppierung und Segmentierung der Netzwerkarchitektur die Basis. Wichtig ist, dass das Netzwerk in mindestens zwei Sicherheitszonen unterteilt wird. Die erste Sicherheitszone (Sicherheitszone des Unternehmens) beinhaltet die IT-Systeme für die Planung und die Ressourceneinteilung (z. B. ERP, Warenwirtschaftssystem). Die zweite Sicherheitszone, die den operativen Systemen gewidmet ist, umfasst die ICS, die zur Steuerung des Versorgungsprozesses der thermischen Netze dienen. Im Gegensatz zur Abbildung oben, die die verschiedenen Komponenten einer Netzwerkarchitektur im Detail darstellt, zeigt Abbildung 14 sehr schematisch die Netzwerkarchitektur der Branche der thermischen Netze mit ihren kritischen Aktivitäten im Bereich der IT und OT sowie den Sicherheitszonen. Auch hier ist eine klare und sichere Trennung zwischen dem Unternehmens- und dem Kontrollnetzwerk zu erkennen, dargestellt durch die Zonen «Organisation» bzw. «Produktion».

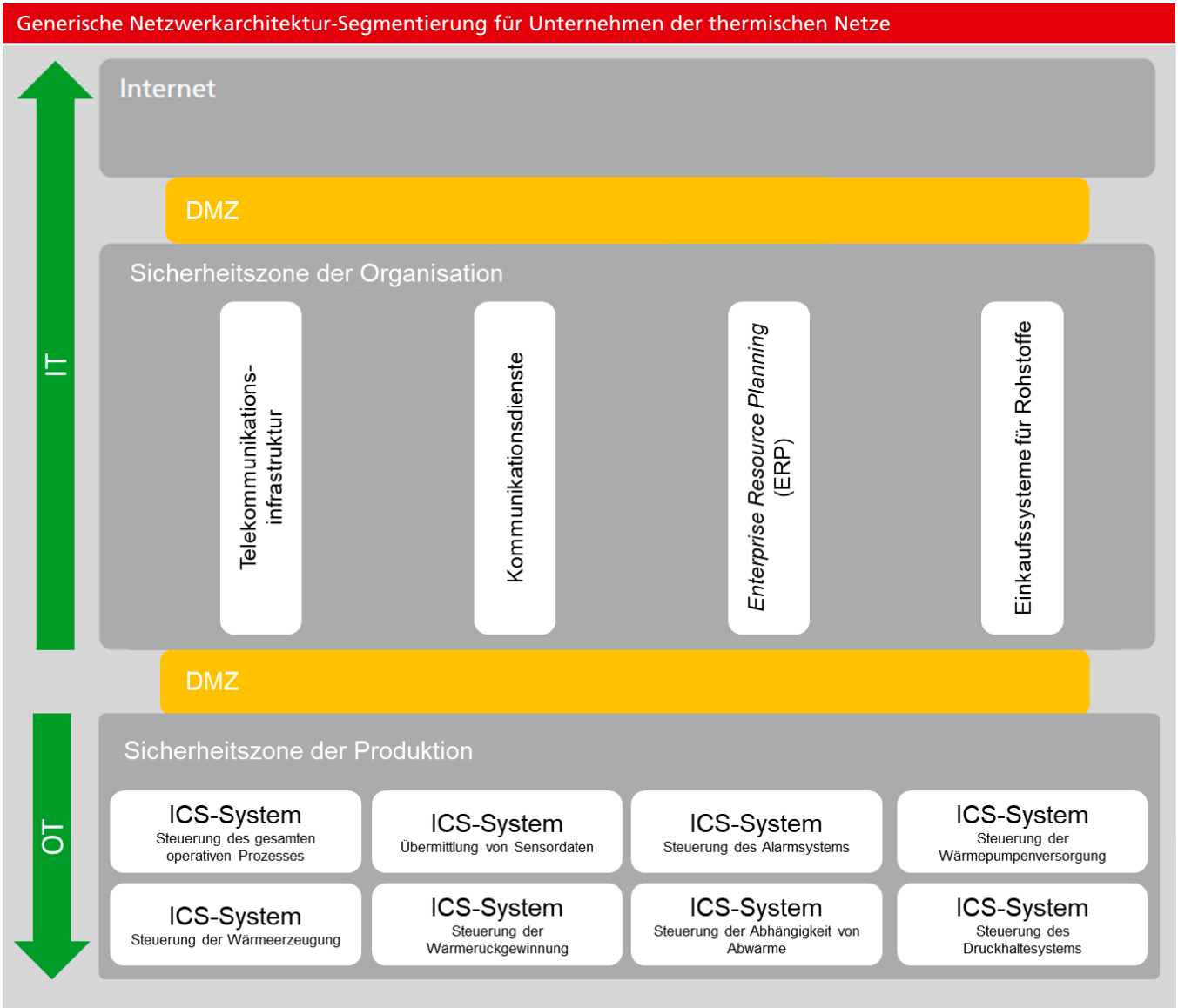

Abbildung 14: Generische Netzwerkarchitektur-Segmentierung für Unternehmen der thermischen Netze

4.2.5 Schutz des Netzwerk-Perimeters

Die Kosten eines ICS-Systems und die Aufrechterhaltung einer homogenen Netzwerkinfrastruktur machen eine Verbindung zwischen dem Kontroll- und dem Unternehmensnetzwerk oft unabdingbar. Diese (aus Abbildung 13 und Abbildung 14 ersichtliche) Verbindung stellt ein erhebliches Sicherheitsrisiko dar und sollte technisch geschützt werden. Müssen die Netzwerke zwingend verbunden werden, wird dringend empfohlen, dass nur minimale (wenn möglich einzelne) Verbindungen erlaubt werden und dass die Verbindung über eine Firewall und eine DMZ (separates Netzwerksegment) erfolgt. ICS-Server, die Daten aus dem Unternehmensnetzwerk enthalten, müssen in eine dieser DMZ gestellt werden. Externe Verbindungen müssen bekannt sein und auf einen minimalen Zugriff über die Firewall beschränkt werden. Der Datenaustausch kann zusätzlich durch Systeme zur Anomalieerkennung überwacht und plausibilisiert werden.

4.2.6 Schutz der physischen Elemente

Nachdem die «technischen» Elemente, die mit den verschiedenen von der Organisation verwendeten Netzwerken zusammenhängen, gesichert sind, muss auch der Zugang zur physischen Ausrüstung sowie zur Arbeitsumgebung geschützt werden. Neben der physischen Sicherung bestimmter Komponenten ist es wichtig, den Lebenszyklus der physischen Komponenten zu berücksichtigen. Einige Komponenten, insbesondere OT, können einen besonders langen Lebenszyklus haben (zwischen 10 und 20 Jahre) und ihre Sicherheit muss während ihrer gesamten Nutzungsdauer gewährleistet sein. Bei mobilen Geräten, die häufig verloren oder vergessen gehen oder die gestohlen werden können, muss eine Standardkonfiguration gewählt werden, die mögliche Schäden so weit wie möglich begrenzt.

4.2.6.1 Physischer Schutz von Geräten und Anlagen

Physische Sicherheitsmassnahmen reduzieren das Risiko von versehentlichen oder vorsätzlichen Verlusten oder Schäden an IKT-Betriebsmitteln der Organisation oder deren Umfeld. Zu den zu schützenden Betriebsmitteln gehören unter anderem physische Vermögenswerte wie Hilfsmittel und Anlagen, die Umwelt (im ökologischen Sinn), das erweiterte Umfeld sowie das geistige Eigentum, einschliesslich proprietärer Daten wie Prozesseinstellungen und Kundeninformationen. Physische Sicherheitskontrollen müssen häufig spezifische Umwelt-, Sicherheits-, Regulierungs- und sonstige Anforderungen erfüllen. Organisationen sollen physische Sicherheitskontrollen wie technische Kontrollen dem Schutzbedarf anpassen. Um einen umfassenden Schutz zu gewährleisten, umfasst der physische Schutz auch den Schutz von IKT-Komponenten (=Security) und Daten aus dem mit der IKT verbundenen Umfeld. Die physische Sicherheit der IKT-Infrastruktur ist eng mit der Anlagensicherheit (=Safety) verbunden. Es gilt, das Personal vor Gefahren zu schützen, ohne sie bei ihrer Arbeit zu behindern. Physische Sicherheitskontrollen sind aktive oder passive Massnahmen, die den physischen Zugriff auf alle Bestandteile der IKT-Infrastruktur begrenzen. Diese Schutzmassnahmen sollen u. a. folgende Fälle verhindern:

- Unbefugter physischer Zutritt zu sensiblen Orten.
- Physische Veränderung, Manipulation, Diebstahl oder sonstige Entfernung oder Zerstörung bestehender Systeme, Infrastruktur, Kommunikationsschnittstellen oder physischer Standorte.
- Unbefugte Beobachtung von sensiblen Anlagen durch visuelle Betrachtung, Fotografien oder jede andere Art von Aufzeichnungen.
- Unerlaubte Einführung/Installation von neuen Systemen, Infrastrukturen, Kommunikationsschnittstellen oder anderer Hardware.
- Unerlaubte Einführung von Geräten (USB-Stick, Wireless Access Point, Bluetooth- oder Mobilgeräte), die dazu dienen, Manipulationen an Hardware vorzunehmen oder die Kommunikation abzuhören, oder die andere schädlichen Auswirkungen haben.

4.2.6.2 Hardware Life Cycle Management

Um den Anforderungen an die Informationssicherheit zu genügen, sind physische Betriebsmittel, einschliesslich Systeme und Netzwerkausrüstung, Bürogeräte (z. B. Netzwerkdrucker und Multifunktionsgeräte) und Spezialausrüstung (z. B. ICS) über ihren gesamten Lebenszyklus vom Erwerb (z. B. Kauf oder Leasing) über die Wartung bis zur Entsorgung zu schützen. Die Beschaffung (Kauf oder Leasing) von widerstandsfähiger, zuverlässiger Hardware soll immer den Sicherheitsanforderungen entsprechen. Mögliche Schwachstellen an der Hardware sollen immer identifiziert werden. So soll sichergestellt werden, dass die Hardware die erforderliche Funktionalität bietet und die Sicherheit kritischer oder sensibler Informationen und Systeme über den gesamten Lebenszyklus hinweg nicht beeinträchtigt.

4.2.6.3 Konfiguration von mobilen Geräten gegen Diebstahl oder Verlust

Um Daten vor unbefugtem Zugriff, Verlust und Diebstahl zu schützen, sollen mobile Geräte (einschliesslich Laptops, Tablets und Smartphones) immer über eine Standardkonfiguration verfügen, die den Sicherheitsanforderungen entspricht (beschränkter Zugriff, Installation von Sicherheitssoftware und zentrale Steuerung der Geräte). Ziel der Standardkonfiguration ist es, auch bei Verlust oder Diebstahl die Informationssicherheit von gespeicherten oder übermittelten Daten auf den mobilen Geräten zu gewährleisten.

4.2.7 Lieferantenmanagement

Das Lieferantenmanagement befasst sich mit der Identifizierung und der Verwaltung von IT-Risiken im Zusammenhang mit externen Anbietern (d. h. Lieferanten von Hard- und Software, Outsourcing-Anbieter, Cloud-Service-Anbieter usw.). Durch die Definition und die Regelung der Einhaltung von Anforderungen an die Informationssicherheit in formalen Verträgen sollen die Risiken minimiert werden.

4.2.8 Mitarbeitermanagement

Die von Menschen verursachten Fehlmanipulationen stellen Organisationen vor zahlreiche Herausforderungen. Technische Massnahmen können böswillige oder unabsichtliche Fehlmanipulationen nie vollständig ausschliessen. Unternehmen sind umso fehleranfälliger, je grösser ihr Anteil an unerfahrenen oder unqualifizierten Mitarbeitenden ist. Die Bekämpfung von Aktivitäten mit bösartigen Absichten von Insidern stellt eine weitere Herausforderung dar. Im Umgang mit diesen Herausforderungen sind Unternehmen gehalten, sich mit den nachfolgenden Themen zu befassen.

4.2.8.1 Beschäftigungszyklus von Mitarbeitenden

Informationssicherheit muss für das Unternehmen ein ständiges Anliegen sein. Die Sensibilisierung, Schulung und Weiterbildung sowie die Befähigung der Mitarbeitenden müssen auf permanenter Basis erfolgen, und zwar von der Anstellung bis zum Ende des Arbeitsverhältnisses und darüber hinaus. Die Mitarbeitenden müssen die notwendigen Fähigkeiten erwerben, um ihre Aufgaben in einer Weise erfüllen zu können, die die Sicherheit und die Unternehmenswerte wahrt. Die verschiedenen Zugänge, sowohl physisch als auch digital, wie z. B. der Zugang zu Räumlichkeiten, Gebäuden, Servern und Software, die den Mitarbeitenden zur Verfügung stehen, müssen regelmässig überprüft und im Falle eines Tätigkeitswechsels oder einer Versetzung innerhalb des Unternehmens geändert werden. Ein HR-Prozess muss sicherstellen, dass die verschiedenen Zugänge bzw. Zugriffe am Ende des Arbeitsverhältnisses aufgehoben werden.

4.2.8.2 Weisungen und Richtlinien

Klare, umsetzbare Weisungen und Richtlinien für Mitarbeitende regeln ihr Verhalten im Umgang mit sicherheitsrelevanten Themen. Sie setzen einen Rahmen und ermöglichen Kontrollen mit dem Ziel, Systeme zu schützen und die Richtlinien durchzusetzen. Sie legen zudem Verfahren fest und definieren die Erwartungen der Organisation an ihre Mitarbeitenden. Richtlinien und Weisungen definieren, was eingehalten werden muss und wie Verletzungen sanktioniert werden.

4.2.8.3 Sicherheitsprozesse

Das Sicherheitsmanagement liegt in der Verantwortung der mit der IT-Sicherheit betrauten Unternehmenseinheit, die auch die entsprechenden Prozesse festlegt. Ihre Hauptfunktion ist der Schutz von Unternehmensinformationen und -daten. Organisationen sind gehalten, Sicherheitsmanagementprozesse auch auf industrielle Kontrollsysteme (ICS) anzuwenden. Dazu gehört die Definition von Prozessen, wie Verfahren durchgeführt oder bestimmte Systeme konfiguriert werden sollen. Diese Prozesse sollten stets standardisiert und reproduzierbar sein. So werden neue Mitarbeitende stets auf einem gleichbleibenden Sicherheitsniveau geschult und es kann sichergestellt werden, dass alle erforderlichen Vorschriften und Standards bekannt sind. Der Prozess zur Erkennung eines Cyber-Vorfalles und die Reaktion darauf (Intrusion Detection and Response) ist von besonderer Bedeutung. Im Umgang mit herstellerspezifischen Protokollen und Legacy-Systemen sind netzwerkbasierte Sicherheitsverfahren besonders wichtig.

4.2.8.4 Aufgaben und Verantwortlichkeiten in kritischen Geschäftsumgebungen

Aufgaben und Verantwortlichkeiten in kritischen Geschäftsumgebungen, vom Prozessmanagement bis zur Nutzung spezifischer Anwendungen (einschliesslich unterstützte Systeme/Netzwerke), sowie der Zugang zu Informationen sollten klar kommuniziert und kompetenten Personen zugewiesen werden. Ziel ist es, bei den Mitarbeitenden ein individuelles Verantwortungsbewusstsein zu schaffen. Die so etablierte Unternehmenskultur trägt dazu bei, dass Mitarbeitende ihre Aufgaben unter Berücksichtigung der Vorgaben für die Informationssicherheit wahrnehmen.

4.2.8.5 Kommunikation/Security-Awareness-Programm

Ein Security-Awareness-Programm und eine offene Kommunikation fördern das Bewusstsein und das gewünschte Verhalten aller Mitarbeitenden über sämtliche Hierarchiestufen des Unternehmens. Ziel ist eine Unternehmenskultur, die das individuell gewünschte Sicherheitsverhalten fördert. Jede und jeder Einzelne soll in ihrem bzw. seinem persönlichen Zuständigkeitsbereich befähigt sein, risikobasierte Entscheidungen zu treffen.

4.2.9 Informationssicherheitsstrategie

Die Definition, Aufrechterhaltung und Überwachung einer umfassenden Informationssicherheitsstrategie ermöglicht es der Geschäftsleitung, klare Richtlinien zu setzen, und unterstützt sie sowohl bei der Durchsetzung von Vorgaben als auch im Risikomanagement.

5 Massnahmen des NIST Framework Core

5.1 Einführung in das NIST Framework Core

Ziel des Cyber-Sicherheitsrahmens (NIST Framework Core) des Minimalstandards und seiner Empfehlungen ist es, für die Unternehmen der Branche der thermischen Netze ein Instrument bereitzustellen, mit dem diese selbstständig und eigenverantwortlich ihre IKT-Resilienz erhöhen können. Dabei werden auch das Streben nach Effizienz, die Vertraulichkeit und der Schutz der Privatsphäre zur Erlangung wirtschaftlichen Wohlstandes berücksichtigt. Um Weiterentwicklung und technische Innovation zu ermöglichen, ist der Cyber-Sicherheitsrahmen (NIST Framework Core) technologieneutral. Das NIST Framework Core basiert auf einer Auswahl an existierenden Standards, Richtlinien und Best-Practice-Vorgaben.

Der Cyber-Sicherheitsrahmen entspricht im Wesentlichen dem NIST Framework Core und berücksichtigt einen risikobasierten Ansatz, um Cyber-Sicherheitsrisiken zu adressieren und zu managen. Er besteht aus fünf Funktionen:

1. *Identifizieren (Identify)*
2. *Schützen (Protect)*
3. *Erkennen (Detect)*
4. *Reagieren (Respond)*
5. *Wiederherstellen (Recover)*

Diese fünf Funktionen bilden gemeinsam eine strategische Sicht auf die Steuerung von IKT-Risiken einer Organisation.

5.2 Implementierung «Tiers»

Das NIST Framework Core umfasst vier Stufen, die sogenannten Implementation Tiers. Diese beschreiben die Ausbaustufe (Schutzniveau), die ein Unternehmen umgesetzt hat. Sie reichen von teilweise (Tier 1) bis dynamisch (Tier 4). Zur Festlegung des eigenen Schutzniveaus (Tier-Level) muss eine Organisation ihre Risikomanagementpraktiken, Infrastruktur, IT/OT-Architektur, die Art der möglichen Bedrohungen sowie rechtliche und regulatorische Anforderungen, ihre Geschäftsziele und organisatorischen Vorgaben genau kennen.

Tier 0: nicht umgesetzt

Obschon sich die Organisation bewusst ist, dass die betroffene Massnahme eigentlich seit Langem umgesetzt sein sollte, wurde noch nichts unternommen.

Tier 1: partiell

Das Tier-Level 1 bedeutet, dass Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit nicht formalisiert sind (keine festen Regeln) und dass IKT-Risiken üblicherweise nur ad hoc oder reaktiv verwaltet werden. Ein integriertes Risikomanagementprogramm auf organisatorischer Ebene besteht, aber ein Bewusstsein für IKT-Risiken und ein organisationsweiter Ansatz zur Bewältigung dieser Risiken sind nicht etabliert. Die Organisation verfügt in der Regel nicht über Prozesse, um Informationen zur Cyber-Sicherheit innerhalb der Organisation gemeinsam zu nutzen. Ebenso verfügt die Organisation für den Fall eingetretener IKT-Risiken oft nicht über standardisierte Prozesse zum Informationsaustausch oder zur koordinierten Zusammenarbeit mit externen Partnern.

Tier 2: Risiko erkannt

Organisationen, die sich selber auf dem Tier-Level 2 einordnen, verfügen gewöhnlich über Risikomanagementprozesse für den IKT-Bereich. Diese sind jedoch nicht als konkrete Handlungsanweisungen implementiert. Auf der organisatorischen Ebene sind IKT-Risiken ins unternehmensweite Risikomanagement integriert und das Bewusstsein für IKT-Risiken ist auf allen Unternehmensstufen vorhanden. Hingegen fehlen in der Regel unternehmensweite Ansätze zur Steuerung und Verbesserung des Bewusstseins (Awareness) für aktuelle und zukünftige IKT-Risiken. Genehmigte Prozesse und Verfahren sind definiert und umgesetzt. Das Personal verfügt über ausreichende Ressourcen, um seine Aufgaben im Bereich der Cyber-Sicherheit wahrzunehmen. Informationen bezüglich der Cyber-Sicherheit werden innerhalb der Organisation auf informeller Basis geteilt. Die Organisation ist sich ihrer Rolle bewusst und kommuniziert mit externen Partnern zum Thema Cyber-Sicherheit (Kundschaft, Lieferanten, Dienstleistungsanbieter usw.). Es bestehen jedoch keine standardisierten Prozesse zur Kooperation oder zum Informationsaustausch mit diesen Partnern.

Tier 3: reproduzierbar

Organisationen auf Tier-Level 3 verfügen über formell genehmigte Risikomanagementpläne und Vorgaben zu deren unternehmensweiten Anwendung. Der Umgang mit IKT-Risiken ist in unternehmensweit gültigen Richtlinien definiert. Die standardisiert erfassten IKT-Risiken sowie die Vorgaben zum Umgang mit denselben werden regelmässig aktualisiert. Dabei werden sowohl Veränderungen der Geschäftsanforderungen berücksichtigt als auch technische Weiterentwicklungen und eine sich verändernde Bedrohungslandschaft, etwa durch neue Akteure oder ein sich wandelndes politisches Umfeld.

Prozesse und Verfahren zum Umgang mit veränderten Risiken sind schriftlich definiert. Es werden standardisierte Methoden eingesetzt, um auf Veränderungen der Risiken zu reagieren. Das Personal verfügt über die notwendigen Kenntnisse und Fähigkeiten, um seine Aufgaben zu erfüllen.

Die Organisation kennt ihre Abhängigkeiten von externen Partnern und tauscht mit diesen Informationen aus, die Managemententscheidungen innerhalb der Organisation als Reaktion auf Vorfälle ermöglichen.

Tier 4: dynamisch

Das Tier-Level 4 bedeutet, dass eine Organisation alle Anforderungen aus den Tier-Leveln 1–3 vollständig erfüllt und zusätzlich die eigenen Prozesse, Methoden und Fähigkeiten ständig überprüft und bei Bedarf verbessert. Grundlage für die kontinuierliche Verbesserung ist eine lückenlose Dokumentation sämtlicher Cyber-Sicherheitsvorfälle. Die Organisation zieht die notwendigen Lehren aus der Analyse vergangener Vorfälle und passt die eigenen Prozesse und eingesetzten Sicherheitstechnologien dynamisch dem neusten Stand der Technik oder sich wandelnden Bedrohungslagen an. IKT-Risikomanagement ist fester Bestandteil der Unternehmenskultur. Erkenntnisse aus vergangenen Vorfällen, Informationen von externen Quellen und aus der permanenten Überwachung der eigenen Systeme und Netzwerke werden fortwährend in den Risikomanagementprozess integriert. Die Organisation teilt laufend Informationen mit Partnern und verfügt dazu über standardisierte Prozesse.

n/a: nicht zutreffend

Diese Massnahme wird von der Organisation entsprechend der eigenen Risikobewertung bewusst nicht umgesetzt.

5.3 Profile

Ein Profil kann als eine Angleichung von Standards, Richtlinien und Praktiken aus dem Cyber-Sicherheitsrahmen mit einem individuellen Implementierungsszenario charakterisiert werden. Profile können verwendet werden, um Optionen zur Verbesserung der Cyber-Sicherheit zu identifizieren, indem sie ein Ist-Profil mit einem Soll-Profil verknüpfen (siehe Abbildung 15). Um ein solches Profil zu entwickeln, kann das mit diesem IKT-Minimalstandard mitgelieferte Assessment Tool verwendet werden. Die Resultate aus der Beantwortung der 106 Aufgaben werden entsprechend den fünf Funktionen des Cyber-Sicherheitsrahmens dargestellt (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen). Das erforderliche Minimalniveau gilt dann als erreicht, wenn im «Overall Cyber Security Maturity Rating» der Ist-Zustand mindestens den entsprechenden Minimalwerten (Soll-Zustand) entspricht. Eine Anleitung zum Umgang mit dem Assessment Tool befindet sich im Tool selbst.

Beispiel: Cyber Security Maturity Rating

Overall Cyber Security Maturity Rating	Ist	Soll
Identifizieren (Identify)	2.8	2.6
Schützen (Protect)	2.7	2.6
Erkennen (Detect)	2.9	2.6
Reagieren (Respond)	2.0	2.6
Wiederherstellen (Recover)	1.4	2.6

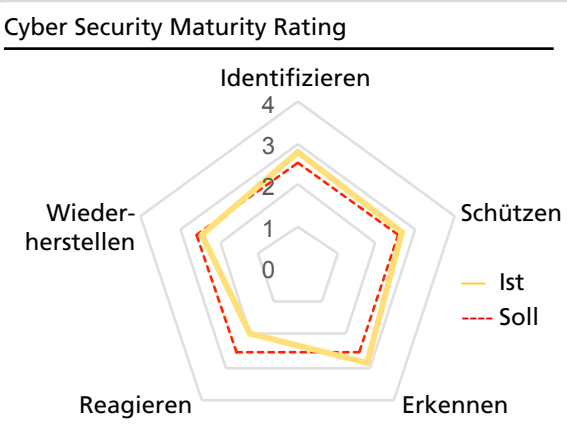

Abbildung 15: Beispiel «Overall Cyber Security Maturity Rating»

5.4 Identifizieren – Identify

5.4.1 Inventarmanagement – Asset Management

Die Daten, Personen, Geräte, Systeme und Anlagen einer Organisation sind identifiziert, katalogisiert und bewertet. Die Bewertung soll ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse sowie der Risikostrategie der Organisation entsprechen.

Bezeichnung	Aufgabe
ID.AM-1	Erarbeiten Sie einen Inventarisierungsprozess, welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar Ihrer IKT-Betriebsmittel (Assets) vorhanden ist.
ID.AM-2	Inventarisieren Sie all Ihre Softwareplattformen, -lizenzen und -applikationen innerhalb Ihrer Organisation.
ID.AM-3	Katalogisieren Sie all Ihre internen Kommunikations- und Datenflüsse.
ID.AM-4	Katalogisieren Sie alle externen IKT-Systeme, die für Ihre Organisation relevant sind.
ID.AM-5	Priorisieren Sie die inventarisierten Ressourcen (Geräte, Anwendungen, Daten) hinsichtlich ihrer Kritikalität.
ID.AM-6	Definieren Sie klare Rollen und Verantwortlichkeiten im Bereich der Cyber-Sicherheit.

Tabelle 3: Aufgaben ID.AM

Standard	Referenz
CCS CSC 1	1, 2, 13, 14, 17, 19
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO10.04, DSS01.02, APO03.03, APO03.04, APO12.01, BAI04.02, APO01.02, APO07.06, APO13.01, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6, A.12.5.1, A.13.2.1, A.13.2.2
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, PM-5, AC-20, SA-9, CP-2, RA-2, SA-14, SC-6, PS-7, PM-11

Tabelle 4: Referenzen ID.AM

5.4.2 Geschäftsumfeld – Business Environment

Die Ziele, Aufgaben und Aktivitäten des Unternehmens sind priorisiert und bewertet.
Diese Informationen dienen als Grundlage für die Zuweisung der Verantwortlichkeiten.

Bezeichnung	Aufgabe
ID.BE-1	Definieren, dokumentieren und kommunizieren Sie die exakte Rolle Ihres Unternehmens innerhalb der (kritischen) Versorgungskette.
ID.BE-2	Identifizieren und kommunizieren Sie die Bedeutung Ihrer Organisation als kritische Infrastruktur und ihre Position innerhalb des kritischen Sektors.
ID.BE-3	Bewerten und priorisieren Sie die Ziele, Aufgaben und Aktivitäten innerhalb der Organisation.
ID.BE-4	Katalogisieren Sie alle externen IKT-Systeme, die für Ihre Organisation relevant sind.
ID.BE-5	Priorisieren Sie die inventarisierten Ressourcen (Geräte, Anwendungen, Daten) hinsichtlich ihrer Kritikalität.

Tabelle 5: Aufgaben ID.BE

Standard	Referenz
CCS CSC 1	1, 2
COBIT 5	APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, APO02.06, APO03.01, APO02.01, APO10.01, BAI04.02, BAI03.02, DSS04.02, BAI09.02
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	SA-12, SA-14, CP-2, PM-11, PM-8, CP-8, PE-9, PE-11, CP-11, SA-13

Tabelle 6: Referenzen ID.BE

5.4.3 Vorgaben – Governance

Die Governance regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische, rechtliche und operationelle Anforderungen aus dem Geschäftsumfeld eingehalten werden.

Bezeichnung	Aufgabe
ID.GV-1	Erlassen Sie Vorgaben zur Informationssicherheit in Ihrem Unternehmen.
ID.GV-2	Koordinieren Sie die Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit mit den intern verantwortlichen Personen (z. B. aus dem Riskmanagement) sowie externen Partnern.
ID.GV-3	Stellen Sie sicher, dass Ihr Unternehmen alle gesetzlichen und regulatorischen Vorgaben im Bereich der Cyber-Sicherheit erfüllt, inkl. Vorgaben zum Datenschutz.
ID.GV-4	Stellen Sie sicher, dass Cyber-Risiken Teil des unternehmensweiten Risikomanagements sind.

Tabelle 7: Aufgaben ID.GV

Standard	Referenz
COBIT 5	APO13.01, APO01.02, APO10.03, DSS05.04, APO13.02, MEA03.01, MEA03.04, DSS04.02, BAI02.01, EDM03.02, APO12.02, APO12.05
ISA 62443-3:2013	
ISO 27001:2013	A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5, Clause 6
NIST-SP-800-53 Rev. 4	PM-1, PM-2, PS-7, PM-9, PM-10, PM-11, Rev.4-1 controls from all security control families, SA-2, PM-3, PM-7

Tabelle 8: Referenzen ID.GV

5.4.4 Risikoanalyse – Risk Assessment

Die Organisation kennt die Auswirkungen von Cyber-Risiken auf die Geschäftstätigkeit, auf Betriebsmittel und Individuen, inklusive Reputationsrisiken.

Bezeichnung	Aufgabe
ID.RA-1	Identifizieren Sie die (technischen) Verwundbarkeiten Ihrer Betriebsmittel und dokumentieren Sie diese.
ID.RA-2	Tauschen Sie sich regelmässig in Foren und Fachgremien aus, um aktuelle Informationen über Cyber-Bedrohungen zu erhalten.
ID.RA-3	Identifizieren und dokumentieren Sie interne und externe Cyber-Bedrohungen.
ID.RA-4	Identifizieren Sie mögliche Auswirkungen auf die Geschäftstätigkeit und bewerten Sie ihre Eintretenswahrscheinlichkeit.
ID.RA-5	Bewerten Sie die Risiken für Ihre Organisation, basierend auf den Bedrohungen, Verwundbarkeiten, Auswirkungen (auf die Geschäftstätigkeit) und Eintretenswahrscheinlichkeiten.
ID.RA-6	Definieren Sie mögliche Sofortmassnahmen bei Eintritt eines Risikos und priorisieren Sie diese.

Tabelle 9: Aufgaben ID.RA

Standard	Referenz
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02, BAI08.01, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2013	A.12.6.1, A.18.2.3, A.6.1.4, Clause 6.1.2, A.16.1.6, Clause 6.1.3
NIST-SP-800-53 Rev. 4	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, RA-3, SI-5, PM-12, RA-2, PM-9, PM-11, SA-14, PM-4

Tabelle 10: Referenzen ID.RA

5.4.5 Risikomanagementstrategie – Risk Management Strategy

Legen Sie die Prioritäten, Einschränkungen und die maximal akzeptablen Risiken Ihrer Organisation fest. Beurteilen Sie Ihre operativen Risiken auf dieser Grundlage.

Bezeichnung	Aufgabe
ID.RM-1	Etablieren Sie Risikomanagementprozesse, managen Sie diese aktiv und lassen Sie sich diese von den beteiligten Personen/Anspruchsgruppen bestätigen.
ID.RM-2	Definieren und kommunizieren Sie die maximal akzeptablen Risiken Ihrer Organisation.
ID.RM-3	Stellen Sie sicher, dass die Definition der maximal akzeptablen Risiken unter Berücksichtigung der Bedeutung Ihrer Organisation als kritische Infrastruktur und unter Einbezug von sektorspezifischen Risikoanalysen erstellt wurde.

Tabelle 11: Aufgaben ID.RM

Standard	Referenz
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06, APO12.02
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2013	Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 4	PM-8, PM-9, PM-11, SA-14

Tabelle 12: Referenzen ID.RM

5.4.6 Lieferketten-Risikomanagement – Supply Chain Risk Management

Legen Sie die Prioritäten, Einschränkungen und maximalen Risiken fest, die Ihre Organisation in Zusammenhang mit Lieferantenrisiken zu tragen gewillt ist.

Bezeichnung	Aufgabe
ID.SC-1	Etablieren Sie klare Prozesse für das Risikomanagement im Zusammenhang mit Lieferkettenstörungen. Lassen Sie diese Prozesse durch alle beteiligten Anspruchsgruppen überprüfen und holen Sie ihre Zustimmung ein.
ID.SC-2	Identifizieren und priorisieren Sie die Lieferanten und Dienstleistungsanbieter Ihrer kritischen Systeme, Komponenten und Dienste unter Anwendung der definierten Prozesse aus ID.SC-1.
ID.SC-3	Verpflichten Sie Ihre Lieferanten und Dienstleistungsanbieter vertraglich dazu, angemessene Massnahmen zu entwickeln und zu implementieren, um die Ziele und Vorgaben aus dem Supply-Chain-Risikomanagementprozess zu erfüllen.
ID.SC-4	Etablieren Sie ein Monitoring, um sicherzustellen, dass all Ihre Lieferanten und Dienstleistungsanbieter ihre Verpflichtungen gemäss den Vorgaben erfüllen. Lassen Sie sich dies regelmässig durch Audit-Berichte oder technische Prüfergebnisse bestätigen.
ID.SC-5	Definieren Sie mit Ihren Lieferanten und Dienstleistungsanbietern Reaktions- und Wiederherstellungsprozesse nach Cyber-Sicherheitsvorfällen. Testen Sie diese Prozesse in Übungen.

Tabelle 13: Aufgaben ID.SC

Standard	Referenz
COBIT 5	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI01.03, BAI02.03, BAI04.02, APO10.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05, DSS04.04
ISA 62443-3:2013	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.2.6., 4.3.2.5.7, 4.3.4.5.11
ISO 27001:2013	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.3
NIST-SP-800-53 Rev. 4	SA-9, SA-12, PM-9, RA-2, RA-3, SA-14, SA-15, SA-11, AU-2, AU-6, AU-12, AU-16, PS-7, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Tabelle 14: Referenzen ID.SC

5.5 Schützen – Protect

5.5.1 Zugriffsmanagement und -steuerung – Access Control

Stellen Sie sicher, dass der physische und logische Zugriff auf IKT-Betriebsmittel und -Anlagen nur für autorisierte Personen, Prozesse und Geräte und auch nur für zulässige Aktivitäten möglich ist.

Bezeichnung	Aktivität
PR.AC-1	Etablieren Sie einen klar definierten Prozess zur Erteilung und Verwaltung von Berechtigungen und Zugangsdaten für Benutzer/innen, Geräte und Prozesse.
PR.AC-2	Stellen Sie sicher, dass nur autorisierte Personen physischen Zugriff auf die IKT-Betriebsmittel haben. Sorgen Sie mit (baulichen) Massnahmen dafür, dass die IKT-Betriebsmittel vor unautorisiertem physischem Zugriff geschützt sind.
PR.AC-3	Etablieren Sie Prozesse zur Verwaltung der Fernzugriffe.
PR.AC-4	Definieren Sie Ihre Berechtigungsstufen nach dem Prinzip der kleinstmöglichen Berechtigung sowie der Trennung von Funktionen.
PR.AC-5	Stellen Sie sicher, dass die Integrität Ihres Netzwerks geschützt ist. Segregieren Sie Ihr Netzwerk logisch und physisch, wo notwendig und sinnvoll.
PR.AC-6	Stellen Sie sicher, dass digitale Identitäten überprüft und bestätigt sind und nur bestätigten Berechtigungsstufen und Zugangsdaten zugeordnet sind.

Tabelle 15: Aufgaben PR.AC

Standard	Referenz
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS01.05, DSS05.02, DSS05.07, DSS05.10, DSS06.10
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3, SR 1.10
ISO 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.6.2.1, A.6.2.2, A13.1.1, A.13.2.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.6.1.2, A.7.1.1, A.9.2.5, A.9.2.6, A.13.1.3, A.14.1.2, A.14.1.3, A.18.1.4
NIST-SP-800-53 Rev. 4	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, AC-17, AC-19, AC-20, SC-15, AC-3, AC-5, AC-6,AC-14, AC-16, AC-24, AC-4, AC-10, SC-7, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14

Tabelle 16: Referenzen PR.AC

5.5.2 Sensibilisierung und Ausbildung – Awareness and Training

Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Cyber-Sicherheit angemessen geschult und informiert sind. Sorgen Sie dafür, dass sie ihre sicherheitsrelevanten Aufgaben gemäss den definierten Vorgaben und Prozessen ausführen.

Bezeichnung	Aufgabe
PR.AT-1	Stellen Sie sicher, dass alle Mitarbeitenden bezüglich Cyber-Sicherheit informiert und geschult sind.
PR.AT-2	Stellen Sie sicher, dass Anwender/innen mit höheren Berechtigungsstufen sich ihrer Rolle und Verantwortung besonders bewusst sind.
PR.AT-3	Stellen Sie sicher, dass sich alle beteiligten Akteure ausserhalb Ihres Unternehmens (Lieferanten, Kunden, Partner) ihrer Rolle und Verantwortung bewusst sind.
PR.AT-4	Stellen Sie sicher, dass sich alle Führungskräfte ihrer besonderen Rolle und Verantwortung bewusst sind.
PR.AT-5	Stellen Sie sicher, dass die Zuständigen für physische Sicherheit und Informationssicherheit sich ihrer besonderen Rolle und Verantwortung bewusst sind.

Tabelle 17: Aufgaben PR.AT

Standard	Referenz
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS05.04, DSS06.03, APO07.06, APO10.04, APO10.05, EDM01.01, APO01.02
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2013	A.7.2.2, A.12.2.1, A.6.1.1, A.7.2.1
NIST-SP-800-53 Rev. 4	AT-2, AT-3, PM-13, PS-7, SA-9, SA-16, IR-2

Tabelle 18: Referenzen PR.AT

5.5.3 Datensicherheit – Data Security

Stellen Sie sicher, dass Informationen, Daten und Datenträger so verwaltet werden, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäss der Risikostrategie der Organisation geschützt werden.

Bezeichnung	Aufgabe
PR.DS-1	Stellen Sie sicher, dass gespeicherte Daten geschützt sind (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit).
PR.DS-2	Stellen Sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind.
PR.DS-3	Stellen Sie sicher, dass für Ihre IT-Betriebsmittel ein formaler Prozess etabliert ist, der die Daten bei Entfernung, Verschiebung oder Ersatz der Betriebsmittel schützt.
PR.DS-4	Stellen Sie sicher, dass Sie bezüglich der Verfügbarkeit der Daten über ausreichende Kapazitäts-reserven verfügen.
PR.DS-5	Stellen Sie sicher, dass adäquate Massnahmen gegen den Abfluss von Daten (Datenlecks) implementiert sind.
PR.DS-6	Etablieren Sie einen Prozess, um Firmware, Betriebssysteme, Anwendungssoftware und Daten hinsichtlich ihrer Integrität zu verifizieren.
PR.DS-7	Stellen Sie eine IT-Umgebung für das Entwickeln und Testen zur Verfügung, welche komplett unabhängig von den produktiven Systemen ist.
PR.DS-8	Etablieren Sie einen Prozess, um die eingesetzte Hardware hinsichtlich ihrer Integrität zu verifizieren.

Tabelle 19: Aufgaben PR.DS

Standard	Referenz
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06, DSS05.02, BAI09.03, APO13.01, BAI04.04, DSS05.04, DSS05.07, DSS.06.02, BAI03.08, BAI07.04, BAI03.05
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.2, SR 7.1, SR 7.2, SR 5.2, SR 3.3
ISO 27001:2013	A.13.1.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.11.2.5, A.12.1.3, A.17.2.1, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.3, A.13.2.1, A.13.2.4, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4, A.12.1.4, A.11.2.4
NIST-SP-800-53 Rev. 4	MP-8, SC-12, SC-28, SC-8, SC-11, CM-8, MP-6, PE-16, AU-4, CP-2, SC-5, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-13, SC-31, SI-4, SI-7, SC-16, CM-2, SA-10

Tabelle 20: Referenzen PR.DS

5.5.4 Informationsschutzrichtlinien – Information Protection Processes and Procedures

Stellen Sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind.

Bezeichnung	Aufgabe
PR.IP-1	Erstellen Sie eine Standardkonfiguration für die Informations- und Kommunikationsinfrastruktur sowie für die industriellen Kontrollsysteme. Stellen Sie sicher, dass diese Standardkonfiguration typische Sicherheitsprinzipien (z. B. N-1-Redundanz, Minimalkonfiguration usw.) einhält.
PR.IP-2	Etablieren Sie einen Lebenszyklusprozess für die Entwicklung von Systemen.
PR.IP-3	Etablieren Sie einen Prozess zur Kontrolle von Konfigurationsänderungen.
PR.IP-4	Stellen Sie sicher, dass Sicherungen (Backups) Ihrer Informationen regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der Backups testen).
PR.IP-5	Stellen Sie sicher, dass Sie alle (regulatorischen) Vorgaben und Richtlinien hinsichtlich den physischen Betriebsmitteln erfüllen.
PR.IP-6	Stellen Sie sicher, dass Daten gemäss den Vorgaben vernichtet werden.
PR.IP-7	Stellen Sie sicher, dass Ihre Informationsschutzprozesse kontinuierlich weiterentwickelt und verbessert werden.
PR.IP-8	Tauschen Sie sich bezüglich der Effektivität verschiedener Schutztechnologien mit Ihren Partnern aus.
PR.IP-9	Etablieren Sie Prozesse zur Reaktion auf eingetretene Vorfälle (Incident Response Planning, Business Continuity Management, Incident Recovery, Disaster Recovery).
PR.IP-10	Testen Sie die Reaktions- und Wiederherstellungspläne.
PR.IP-11	Integrieren Sie Aspekte der Cyber-Sicherheit bereits in den Personalrekrutierungsprozess (z. B. durch die Etablierung von Background-Checks/Personensicherheitsprüfungen).
PR.IP-12	Entwickeln und implementieren Sie einen Prozess zum Umgang mit erkannten Schwachstellen.

Tabelle 21: Aufgaben PR.IP

Standard	Referenz
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, BAI03.01, BAI03.02, BAI03.03, BAI06.01, BAI01.06, APO13.01, DSS01.01, DSS04.07, DSS01.04, DSS05.05, BAI09.03, DSS 05.06, APO11.06, APO12.06, DSS04.05, BAI08.04, DSS03.04, DSS04.03, DSS04.04, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05, BAI03.10, DSS05.02
ISA 62443-3:2013	SR 7.6, SR 7.3, SR 7.4, SR 4.2, SR 3.3
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, Clause 9, Clause 10, A.16.1.1, A.17.1.1, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4, A.12.6.1, A.16.1.3, A.18.2.2, A.18.2.3
NIST-SP-800-53 Rev. 4	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-11, SA-12, SA-15, SA-17, PL-8, SI-12, SI-13, SI-14, SI-16, SI-17, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, CA-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, SI-4, CP-7, CP-12, CP-13, IR-7, IR-9, PE-17, IR-3, PM-14, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21, RA-3, RA-5, SI-2

Tabelle 22: Referenzen PR.IP

5.5.5 Unterhalt – Maintenance

Stellen Sie sicher, dass Unterhalts- und Reparaturarbeiten an Komponenten des IT- und/oder des ICS-Systems gemäss den geltenden Richtlinien und Prozessen durchgeführt werden.

Bezeichnung	Aufgabe
PR.MA-1	Stellen Sie sicher, dass der Betrieb, die Wartung und allfällige Reparaturen an den Betriebsmitteln aufgezeichnet und dokumentiert werden (Logging). Stellen Sie sicher, dass diese zeitnah durchgeführt werden und nur unter Einsatz von geprüften und freigegebenen Mitteln erfolgen.
PR.MA-2	Stellen Sie sicher, dass Unterhaltsarbeiten an Ihren Systemen, die über Fernzugriffe erfolgen, aufgezeichnet und dokumentiert werden. Stellen Sie sicher, dass kein unautorisierter Zugriff möglich ist.

Tabelle 23: Aufgaben PR.MA

Standard	Referenz
COBIT 5	BAI03.10, BAI09.02, BAI09.03, DSS01.05, DSS05.04
ISA 62443-3:2013	
ISO 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.15.1.1, A.15.2.1
NIST-SP-800-53 Rev. 4	MA-2, MA-3, MA-4, MA-5, MA-6

Tabelle 24: Referenzen PR.MA

5.5.6 Einsatz von Schutztechnologie – Protective Technology

Installieren Sie technische Sicherheitslösungen, um die Sicherheit und Resilienz Ihres Systems und Ihrer Daten gemäss den Vorgaben und Prozessen zu garantieren.

Bezeichnung	Aufgabe
PR.PT-1	Definieren Sie Vorgaben zu Audits und Log-Aufzeichnungen. Erstellen und prüfen Sie die Logs regelmässig gemäss den Vorgaben und Richtlinien.
PR.PT-2	Stellen Sie sicher, dass Wechseldatenträger geschützt sind und dass sie nur gemäss den Richtlinien eingesetzt werden.
PR.PT-3	Stellen Sie sicher, dass Ihr System so konfiguriert ist, dass jederzeit eine Minimalfunktionalität gewährleistet wird (Systemhärtung).
PR.PT-4	Stellen Sie sicher, dass Ihre Kommunikations- und Steuernetzwerke geschützt sind.
PR.PT-5	Stellen Sie sicher, dass Ihre Systeme gemäss vordefinierten Szenarien funktionieren. Z. B: Funktionalität während eines Angriffs, Funktionalität in der Wiederherstellungsphase, Funktionalität in der normalen Betriebsphase.

Tabelle 25: Aufgaben PR.PT

Standard	Referenz
COBIT 5	APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01, DSS05.02, DSS05.06, APO13.01, DSS05.05, DSS06.06, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 2.3, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.2, SR 7.6
ISO 27001:2013	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, A.9.1.2, A.13.1.1, A.13.2.1, A.14.1.3, A.17.1.2, A.17.2.1
NIST-SP-800-53 Rev. 4	AU Family, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, AC-3, CM-7, AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Tabelle 26: Referenzen PR.PT

5.6 Erkennen – Detect

5.6.1 Auffälligkeiten und Vorfälle – Anomalies and Events

Stellen Sie sicher, dass Auffälligkeiten (abnormales Verhalten) und sicherheitsrelevante Ereignisse zeitgerecht erkannt werden und dass sich das Personal der potenziellen Auswirkungen solcher Vorfälle bewusst ist.

Bezeichnung	Aufgabe
DE.AE-1	Definieren Sie Standardwerte für zulässige Netzwerkoperationen und die zu erwartenden Datenflüsse für Anwender/innen und Systeme. Überprüfen Sie diese Werte fortlaufend.
DE.AE-2	Stellen Sie sicher, dass entdeckte Cyber-Sicherheitsvorfälle hinsichtlich ihrer Ziele und ihrer Methoden analysiert werden.
DE.AE-3	Stellen Sie sicher, dass Informationen zu Cyber-Sicherheitsvorfällen aus verschiedenen Quellen und Sensoren aggregiert und aufbereitet werden.
DE.AE-4	Legen Sie die Auswirkungen möglicher Vorfälle fest.
DE.AE-5	Definieren Sie die Schwellenwerte, ab denen Cyber-Sicherheitsvorfälle zu einer Alarmierung führen.

Tabelle 27: Aufgaben DE.AE

Standard	Referenz
COBIT 5	DSS03.01, DSS05.07, APO12.06, BAI08.02
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO 27001:2013	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2, A.12.4.1, A.16.1.1, A.16.1.4, A.16.1.7
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CM-2, SI-4, AU-6, CA-7, IR-4, IR-5, IR-8, SI-4, CP-2, RA-3

Tabelle 28: Referenzen DE.AE

5.6.2 Überwachung – Security Continuous Monitoring

Stellen Sie sicher, dass das IKT-System inkl. aller Betriebsmittel in regelmässigen Abständen überwacht wird, um einerseits Cyber-Sicherheitsvorfälle zu erkennen und andererseits die Effektivität der Schutzmassnahmen überprüfen zu können.

Bezeichnung	Aufgabe
DE.CM-1	Etablieren Sie ein kontinuierliches Netzwerk-Monitoring, um potenzielle Cyber-Sicherheitsvorfälle zu erkennen.
DE.CM-2	Etablieren Sie ein kontinuierliches Monitoring aller physischen Betriebsmittel und Gebäude, um Cyber-Sicherheitsvorfälle zu erkennen.
DE.CM-3	Etablieren Sie ein Monitoring der Cyber-Aktivitäten der Mitarbeitenden, um potenzielle Cyber-Sicherheitsvorfälle zu erkennen.
DE.CM-4	Stellen Sie sicher, dass Schadsoftware erkannt werden kann.
DE.CM-5	Stellen Sie sicher, dass Schadsoftware auf Mobilgeräten erkannt werden kann.
DE.CM-6	Stellen Sie sicher, dass die Aktivitäten von externen Dienstleistungsanbietern überwacht werden (Monitoring), sodass allfällige Cyber-Sicherheitsvorfälle erkannt werden.
DE.CM-7	Überwachen Sie Ihr System laufend, um sicherzustellen, dass Aktivitäten/Zugriffe von unberechtigten Personen, Geräten und Software erkannt werden.
DE.CM-8	Führen Sie Verwundbarkeits-Scans durch.

Tabelle 29: Aufgaben DE.CM

Standard	Referenz
COBIT 5	DSS05.07, DSS05.01, APO07.06, BAI03.10, DSS01.03, DSS03.05, DSS01.04, DSS01.05, APO10.05, DSS05.02, DSS05.05
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2013	A.12.4.1, A.12.2.1, A.12.5.1, A.14.2.7, A.15.2.1, A.12.6.1
NIST-SP-800-53 Rev. 4	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, AU-13, CM-10, CM-11, SI-3, SC-18, SI-4, SC-44, PS-7, SA-4, SA-9, CM-8, PE-3, PE-6, PE-20, SI-4, AU-12, RA-5

Tabelle 30: Referenzen DE.CM

5.6.3 Detektionsprozesse – Detection Processes

Prozesse und Handlungsanweisungen zur Erkennung von Cyber-Sicherheitsvorfällen werden gepflegt, getestet und unterhalten.

Bezeichnung	Aufgabe
DE.DP-1	Definieren Sie klare Rollen und Verantwortlichkeiten, so dass klar ist, wer wofür zuständig ist und wer welche Kompetenzen hat.
DE.DP-2	Stellen Sie sicher, dass die Detektionsprozesse die Vorgaben und Bedingungen erfüllen.
DE.DP-3	Testen Sie Ihre Detektionsprozesse.
DE.DP-4	Kommunizieren Sie erkannte Vorfälle an die zuständigen Stellen (Lieferanten, Kundschaft, Partner, Behörden usw.).
DE.DP-5	Verbessern Sie Ihre Detektionsprozesse kontinuierlich.

Tabelle 31: Aufgaben DE.DP

Standard	Referenz
COBIT 5	APO01.02, DSS05.01, DSS06.03, DSS06.01, MEA03.03, MEA03.04, APO13.02, DSS05.02, APO08.04, APO12.06, DSS02.05, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2013	A.6.1.1, A.7.2.2, A.18.1.4, A.18.2.2, A.18.2.3, A.14.2.8, A.16.1.2, A.16.1.3, A.16.1.6
NIST-SP-800-53 Rev. 4	CA-2, CA-7, PM-14, AC-25, SA-18, SI-3, SI-4, PE-3, PM-14, AU-6, RA-5, PL-2

Tabelle 32: Referenzen DE.DP

5.7 Reagieren – Respond

5.7.1 Reaktionsplanung – Response Planning

Erarbeiten Sie einen Reaktionsplan im Hinblick auf erkannte Cyber-Sicherheitsvorfälle. Stellen Sie sicher, dass dieser Reaktionsplan im Ereignisfall korrekt und zeitgerecht ausgeführt wird.

Bezeichnung	Aufgabe
RS.RP-1	Stellen Sie sicher, dass der Reaktionsplan während oder nach einem erkannten Cyber-Sicherheitsvorfall korrekt und zeitnah durchgeführt wird.

Tabelle 33: Aufgaben RS.RP

Standard	Referenz
COBIT 5	APO12.06, BAI01.10
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-2, CP-10, IR-4, IR-8

Tabelle 34: Referenzen RS.RP

5.7.2 Kommunikation – Communication

Stellen Sie sicher, dass Ihre Reaktionsprozesse mit den internen und externen Anspruchsgruppen abgestimmt sind. Stellen Sie sicher, dass Sie im Ereignisfall Unterstützung durch staatliche Stellen erhalten, falls notwendig und angemessen.

Bezeichnung	Aufgabe
RS.CO-1	Stellen Sie sicher, dass alle Personen ihre Aufgaben und die Reihenfolge ihrer Handlungen kennen, wenn sie auf eingetretene Cyber-Sicherheitsvorfälle reagieren müssen.
RS.CO-2	Definieren Sie Kriterien für das Reporting und stellen Sie sicher, dass Cyber-Sicherheitsvorfälle gemäss diesen Kriterien gemeldet und bearbeitet werden.
RS.CO-3	Teilen Sie Informationen und Erkenntnisse zu erkannten Cyber-Sicherheitsvorfällen gemäss den definierten Kriterien.
RS.CO-4	Koordinieren Sie sich mit all Ihren Anspruchsgruppen gemäss den vordefinierten Kriterien.
RS.CO-5	Sorgen Sie für ein gesteigertes Bewusstsein hinsichtlich Cyber-Sicherheitsvorfällen, indem Sie sich regelmässig mit Ihren Partnern austauschen.

Tabelle 35: Aufgaben RS.CO

Standard	Referenz
COBIT 5	EDM03.02, APO01.02, APO12.03, DSS01.03, DSS03.04, BAI08.04
ISA 62443-3:2013	
ISO 27001:2013	A.6.1.1, A.7.2.2, A.16.1.1, A.6.1.3, A.16.1.2, Clause 7.4, Clause 16.1.2, A.6.1.4
NIST-SP-800-53 Rev. 4	CP-2, CP-3, IR-3, IR-8, CA-2, CA-7, IR-4, IR-8, PE-6, RA-5, SI-4, PM-15, SI-5, PM-15

Tabelle 36: Referenzen RS.CO

5.7.3 Analyse – Analysis

Stellen Sie sicher, dass regelmässig Analysen durchgeführt werden, die Ihnen eine adäquate Reaktion auf Cyber-Sicherheitsvorfälle ermöglichen.

Bezeichnung	Aufgabe
RS.AN-1	Stellen Sie sicher, dass Benachrichtigungen aus Detektionssystemen berücksichtigt und Nachforschungen ausgelöst werden.
RS.AN-2	Stellen Sie sicher, dass die Auswirkungen eines Cyber-Sicherheitsvorfalls korrekt bewertet werden.
RS.AN-3	Führen Sie nach einem eingetretenen Vorfall forensische Analysen durch.
RS.AN-4	Kategorisieren Sie eingetretene Vorfälle gemäss den Vorgaben im Reaktionsplan.

Tabelle 37: Aufgaben RS.AN

Standard	Referenz
COBIT 5	DSS02.04, DSS02.07, DSS02.02, APO12.06, DSS03.02, DSS05.07, EDM03.02
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO 27001:2013	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4
NIST-SP-800-53 Rev. 4	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4, IR-4, AU-7, CP-2, IR-5, IR-8, SI-5, PM-15

Tabelle 38: Referenzen RS.AN

5.7.4 Schadensminderung – Mitigation

Handeln Sie so, dass die weitere Ausbreitung eines Cyber-Sicherheitsvorfalls verhindert und der mögliche Schaden verringert wird.

Bezeichnung	Aufgabe
RS.MI-1	Stellen Sie sicher, dass Cyber-Sicherheitsvorfälle eingegrenzt werden können und die weitere Ausbreitung unterbrochen wird.
RS.MI-2	Stellen Sie sicher, dass die Auswirkungen von Cyber-Sicherheitsvorfällen gemindert werden können.
RS.MI-3	Stellen Sie sicher, dass neu identifizierte Verwundbarkeiten reduziert oder als akzeptable Risiken dokumentiert werden.

Tabelle 39: Aufgaben RS.MI

Standard	Referenz
COBIT 5	APO12.06
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4
ISO 27001:2013	A.12.2.1, A.16.1.5, A.12.6.1
NIST-SP-800-53 Rev. 4	IR-4, CA-7, RA-3, RA-5

Tabelle 40: Referenzen RS.MI

5.7.5 Verbesserungen – Improvements

Verbessern Sie die Reaktionsfähigkeit Ihrer Organisation auf eingetretene Cyber-Sicherheitsvorfälle regelmässig, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Bezeichnung	Aufgabe
RS.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus vorangegangenen Cyber-Sicherheitsvorfällen in Ihre Reaktionspläne einfliessen.
RS.IM-2	Aktualisieren Sie Ihre Reaktionsstrategien.

Tabelle 41: Aufgaben RS.IM

Standard	Referenz
COBIT 5	BAI01.13, DSS04.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tabelle 42: Referenzen RS.IM

5.8 Wiederherstellen – Recover

5.8.1 Wiederherstellungsplanung – Recovery Planning

Stellen Sie sicher, dass die Wiederherstellungsprozesse so gepflegt und durchgeführt werden (können), dass eine zeitnahe Wiederherstellung der Systeme gewährleistet ist.

Bezeichnung	Aufgabe
RC.RP-1	Stellen Sie sicher, dass der Wiederherstellungsplan nach einem eingetretenen Cyber-Sicherheits-vorfall korrekt durchgeführt wird.

Tabelle 43: Aufgaben RC.RP

Standard	Referenz
COBIT 5	APO12.06, DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-10, IR-4, IR-8

Tabelle 44: Referenzen RC.RP

5.8.2 Verbesserungen – Improvements

Verbessern Sie Ihre Wiederherstellungsprozesse laufend, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Bezeichnung	Aufgabe
RC.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus vorangegangenen Cyber-Sicherheitsvorfällen in Ihre Wiederherstellungspläne einfliessen.
RC.IM-2	Aktualisieren Sie Ihre Wiederherstellungsstrategie.

Tabelle 45: Aufgaben RC.IM

Standard	Referenz
COBIT 5	APO12.06, BAI05.07, DSS04.08, BAI07.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tabelle 46: Referenzen RC.IM

5.8.3 Kommunikation – Communication

Koordinieren Sie Ihre Wiederherstellungsaktivitäten mit internen und externen Partnern wie Internet-Service-Providern, Cyber Emergency Response Teams (CERT), Behörden, Systemintegratoren usw.

Bezeichnung	Aufgabe
RC.CO-1	Stellen Sie sicher, dass Ihre öffentliche Wahrnehmung aktiv gemanaged wird.
RC.CO-2	Stellen Sie sicher, dass Ihre Reputation nach einem eingetretenen Cyber-Sicherheitsvorfall wiederhergestellt wird.
RC.CO-3	Kommunizieren Sie alle Ihre Wiederherstellungsaktivitäten an die internen Anspruchsgruppen, insbesondere auch an die Führungskräfte und die Geschäftsleitung.

Tabelle 47: Aufgaben RC.CO

Standard	Referenz
COBIT 5	EDM03.02, MEA03.02, APO12.06
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4

Tabelle 48: Referenzen RC.CO

6 Schlussfolgerungen

Die Versorgung der thermischen Netze ist vor allem aufgrund ihrer Vielschichtigkeit eine besonders komplexe Aufgabe. Die zur Erhitzung der thermischen Leitungen eingesetzten Energiequellen und industriellen Prozesse sind vielfältig und weisen jeweils ihre eigenen Besonderheiten auf. Bislang decken die in erster Linie zur Beheizung von Gebäuden genutzten thermischen Netze nur einen kleinen Teil des schweizerischen Wärmebedarfs ab. Dies könnte sich jedoch aufgrund des gesellschaftlichen und politischen Wandels der letzten Jahre ändern. So sollen erneuerbare Energien die fossilen Brennstoffe letztlich vollständig ersetzen, was den Ausbau der thermischen Netze klar ankurbeln könnte. Ausserdem bestehen Wechselwirkungen zwischen dieser Branche und vielen anderen Industriezweigen. Daher sollten die thermischen Netze nicht isoliert, sondern als Teil eines Ganzen betrachtet werden, das von branchenübergreifenden Synergien profitiert. Ein grosser Teil der zur Versorgung der thermischen Leitungen benötigten Wärme stammt effektiv aus anderen industriellen Tätigkeiten, was eine Abhängigkeit von der entsprechenden Tätigkeit oder dem dafür verantwortlichen Unternehmen zur Folge hat. Deshalb muss der gesamte Versorgungsprozess berücksichtigt werden und nicht nur der Prozess zur Versorgung der thermischen Netze.

Wie die meisten industriellen Tätigkeiten nutzen auch thermische Netze verschiedene IKT-Systeme, um ihre Anlagen effizient zu betreiben. Ein Ausfall dieser Systeme kann erhebliche Auswirkungen auf den reibungslosen Betrieb der thermischen Netze in der Schweiz haben und somit die Wärmeversorgung des Landes direkt beeinflussen. Um ein akzeptables Sicherheitsniveau dieser Infrastrukturen aufrechtzuerhalten, müssen diese IKT-Systeme angemessen geschützt werden. Daher wird die Umsetzung des gemeinsam vom BWL, TNS und dem SVGW erarbeiteten IKT-Minimalstandards empfohlen. Dieser verfolgt das Ziel, das Resilienzniveau der Schweizer Branche der thermischen Netze zu erhöhen und so deren Versorgung auch bei einer IKT-Störung zu gewährleisten.

Um ein angemessenes Sicherheitsniveau zu erreichen, analysiert der IKT-Minimalstandard die Zusammensetzung, den Versorgungsprozess und die kritischen branchenspezifischen Aktivitäten. Diese Analyse ermöglicht es, die kritischen Elemente der thermischen Infrastruktur zu identifizieren, um sie angemessen zu schützen. Hinsichtlich des anzuwendenden Sicherheitsprogramms basiert der IKT-Minimalstandard auf dem NIST Framework Core, das im Wesentlichen drei Aspekte vereint:

- Erstens stützt es sich auf einen risikobasierten Ansatz. Jede Organisation kann somit ihre Risikosensitivität, die zur Verringerung dieser Risiken zu ergreifenden Massnahmen und deren Priorisierung selbst definieren und ihre Cyber-Sicherheit entsprechend ihren Bedürfnissen kontrollieren und anpassen.
- Zweitens bedient es sich der Defense-in-depth-Strategie. Dank dieses auf einer Mehrebenen-Verteidigung basierenden Konzepts lassen sich mehrere Sicherheitsmassnahmen kombinieren und so die IKT-Ausrüstung wirksamer schützen.
- Der letzte Aspekt dieses Sicherheitsprogramms sind die Massnahmen des NIST Framework Core.

Dieser IKT-Minimalstandard bietet ein auf diesen Massnahmen basierendes Excel-Assessment-Tool[78], mit dem die Unternehmen der Branche der thermischen Netze die Resilienz ihrer IT-abhängigen Prozesse stärken können. Den Akteuren der Branche steht mit diesem Tool ein Werkzeug zur Verfügung, mit dem sie ihr Sicherheitsniveau systematisch bestimmen und auf ein einheitlich hohes Minimum anheben können. Die Umsetzung des IKT-Minimalstandards erfolgt mittels einer wirksamen, bewährten Methode. Andere Versorgungsbranchen wie die Strom- oder Trinkwasserbranche verwenden dieselben Verfahren, was bei Unternehmen, die in mehreren Bereichen tätig sind, Synergien ermöglicht.

Cyber-Sicherheit ist kein Zustand, sondern wird als dynamischer Prozess verstanden und gelebt. Sicherheit im Umgang mit IKT kann nie erreicht werden, sondern muss ständig angestrebt und regelmässig überprüft sowie kontinuierlich verbessert werden. Der IKT-Minimalstandard zur Sicherstellung der Versorgung der thermischen Netze dient als Leitfaden für die Umsetzung dieses Prozesses und somit die Erreichung des angestrebten Resilienzniveaus.

[78] *Zu finden unter: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html*

7 Anhang

7.1 Versorgungsprozesse der verschiedenen industriellen Prozesse

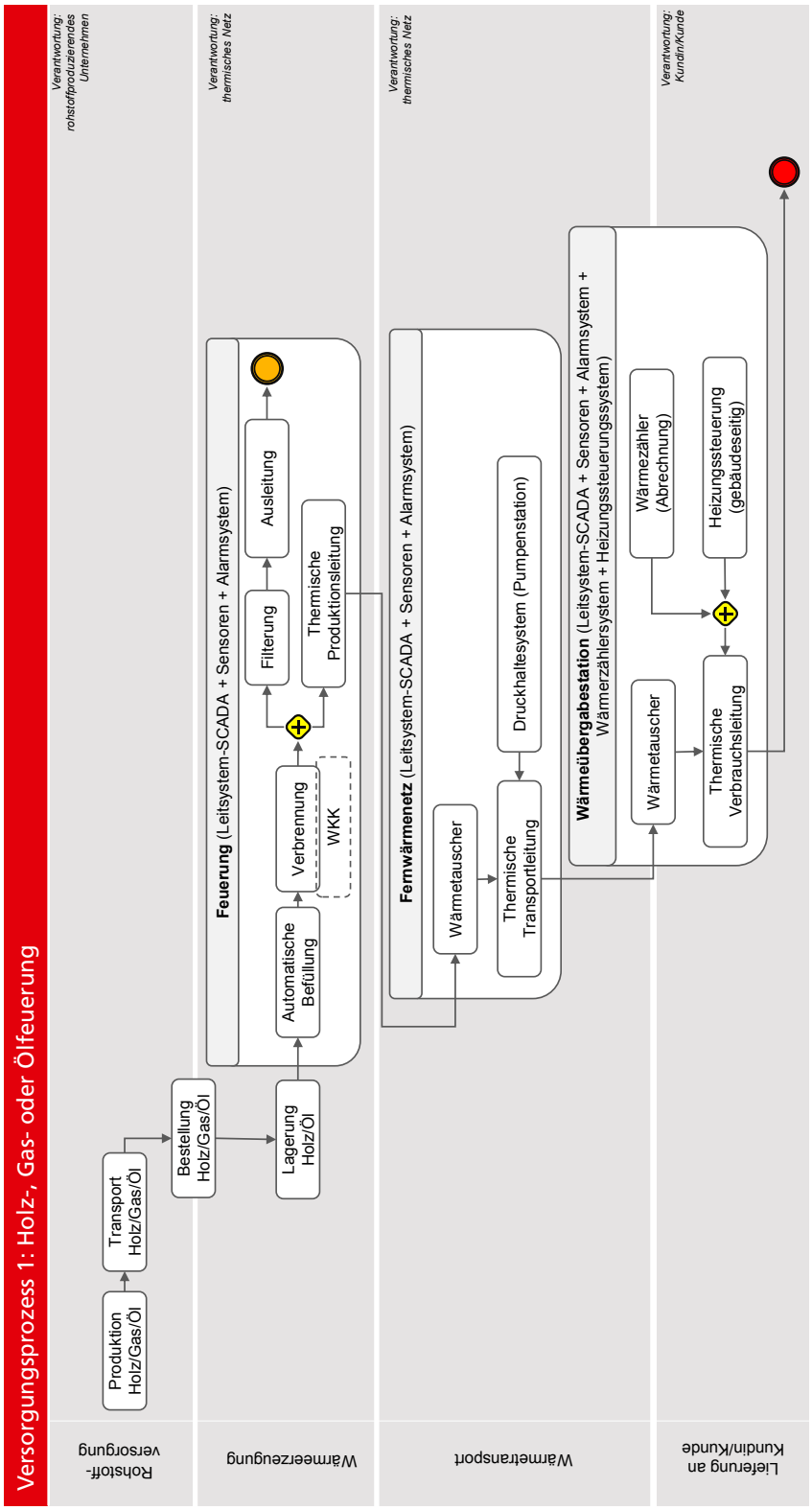

Abbildung 16: Versorgungsprozess mit Feuerungen

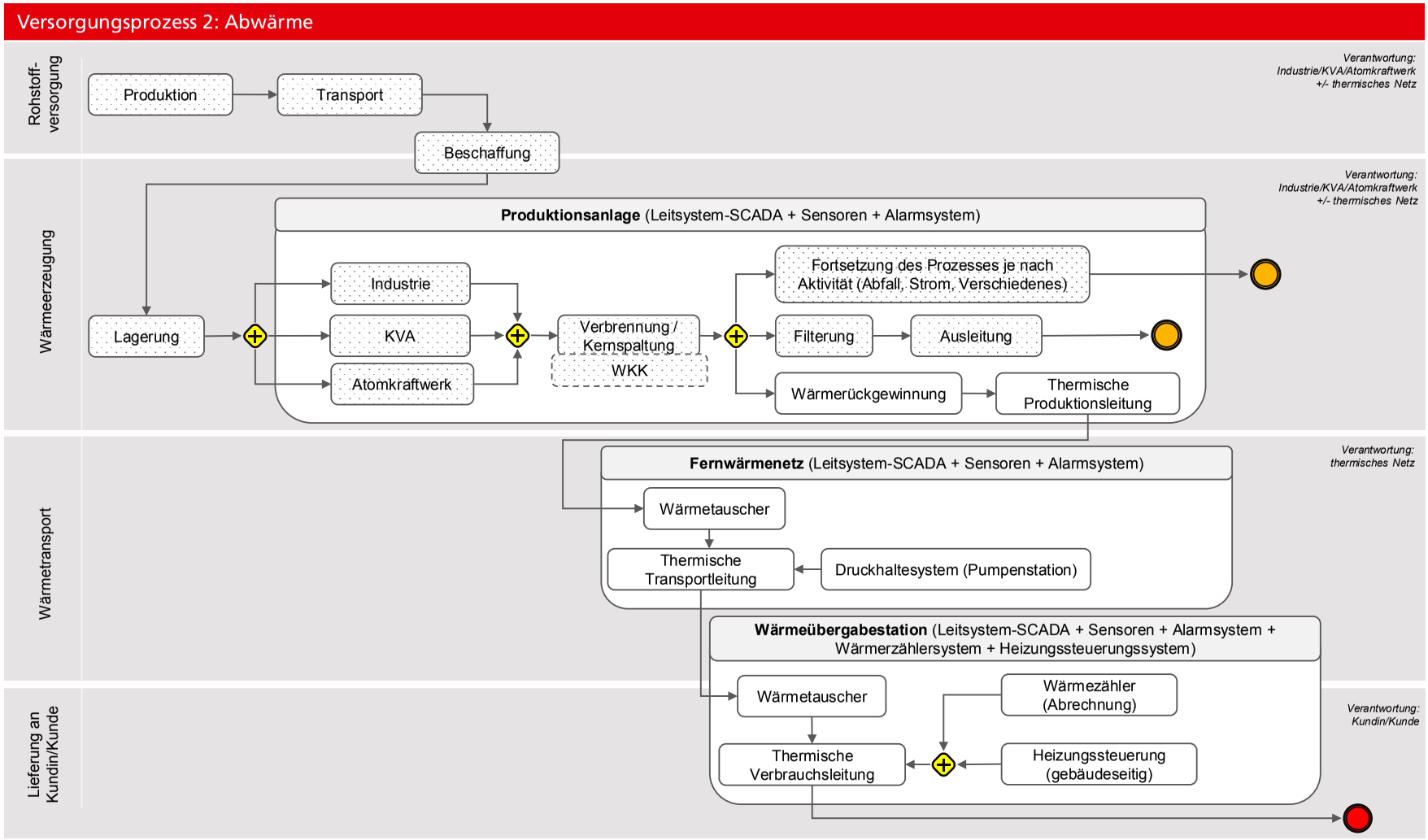

Abbildung 17: Versorgungsprozess mit Abwärme

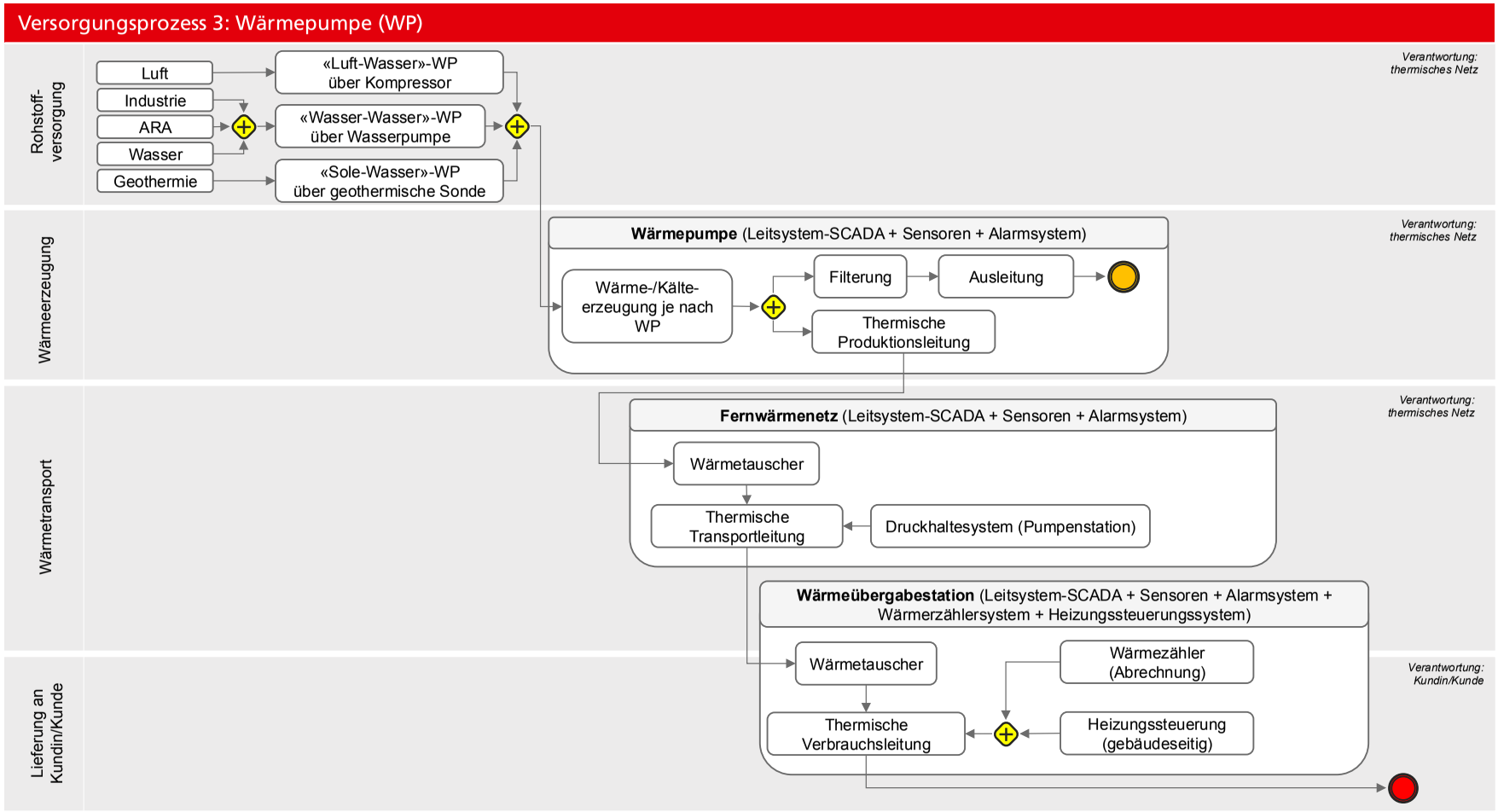

Abbildung 18: Versorgungsprozess mit Wärmepumpen

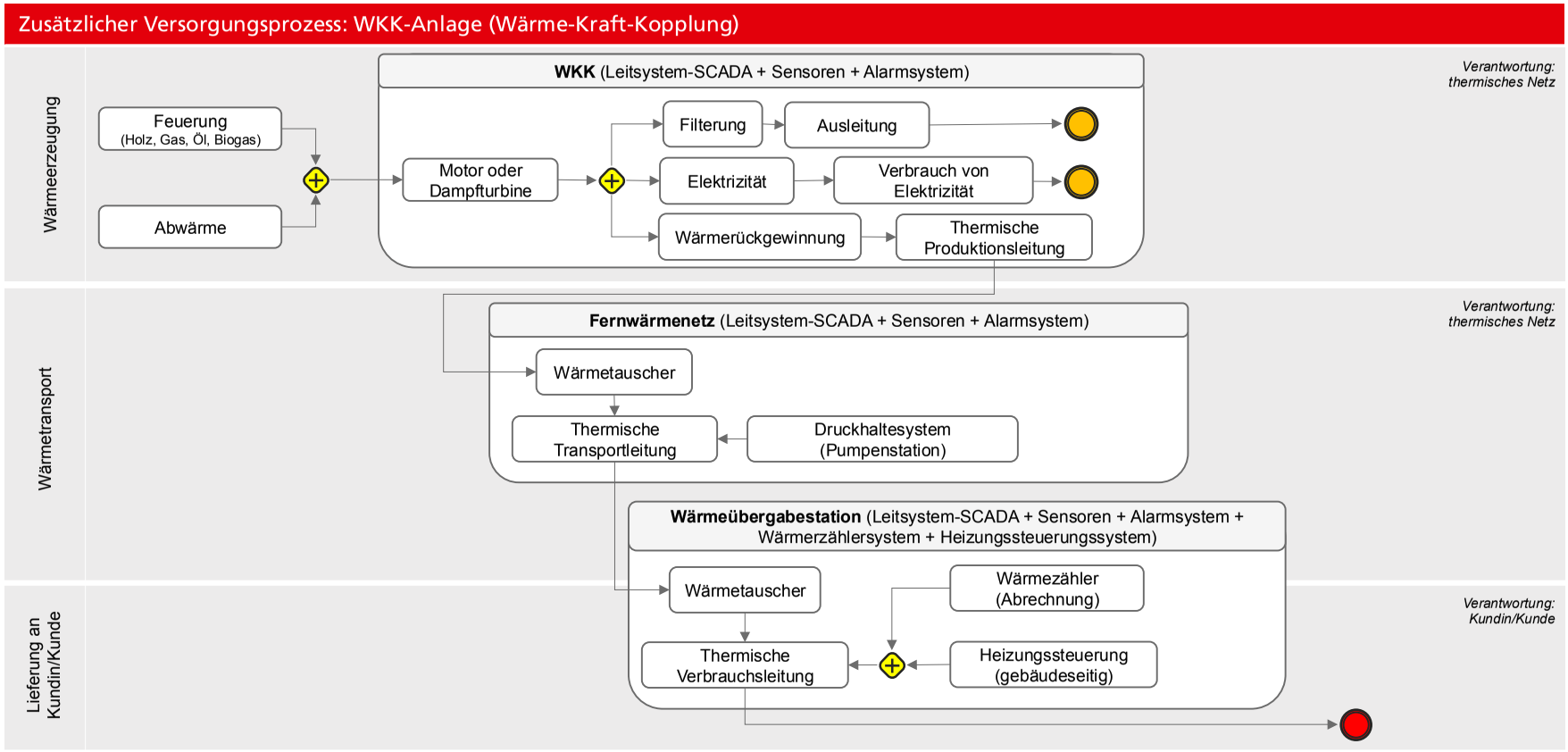

Abbildung 19: Zusätzlicher Versorgungsprozess – Wärme-Kraft-Kopplungsanlage

7.2 Abhängigkeit zwischen verschiedenen Industriezweigen

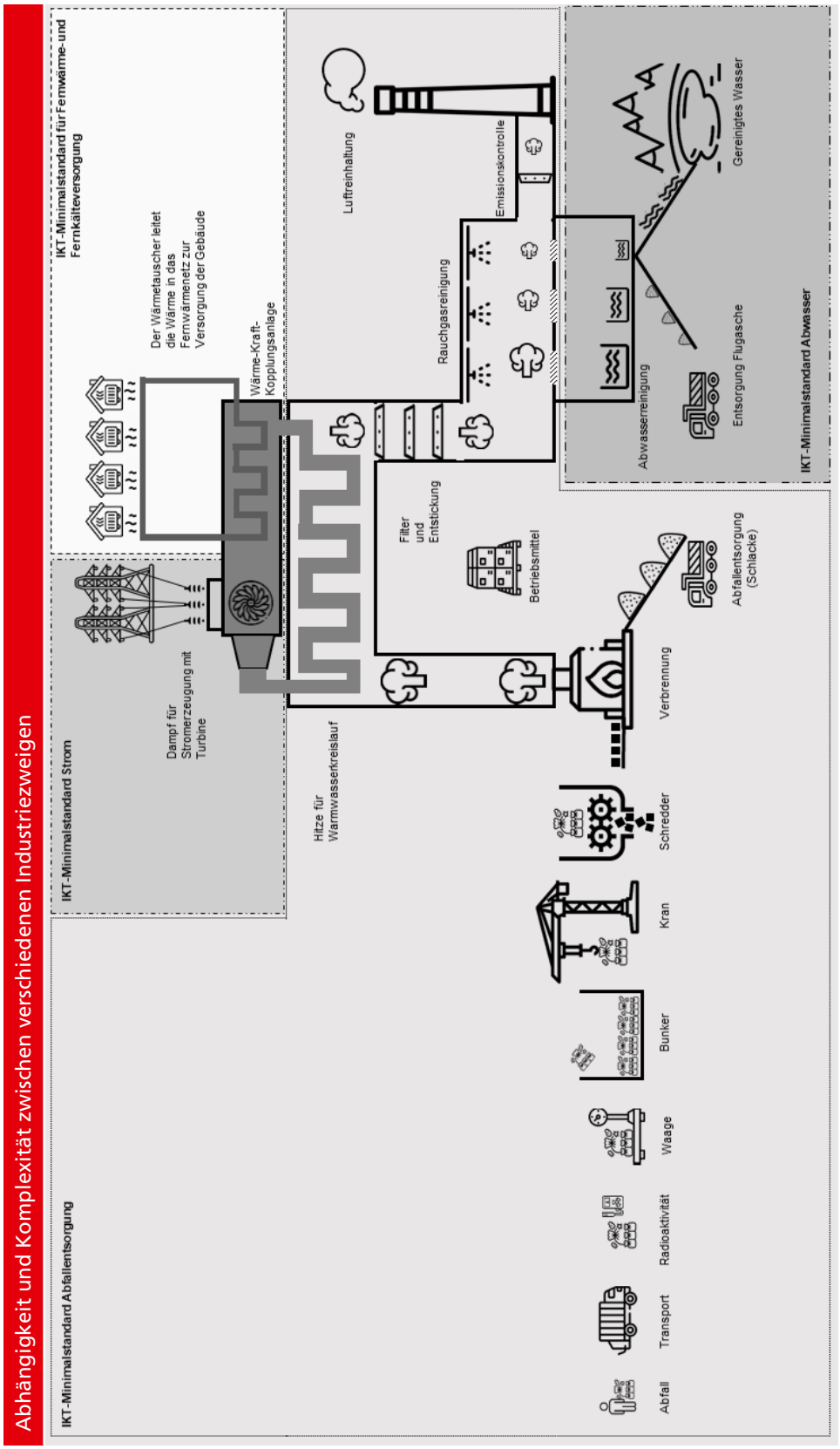

Abbildung 20: Abhängigkeiten zwischen KVA, thermischem Netz, Strom und Abwasser

Kritische Aktivitäten und zugehörige IKT-Systeme

		Kritische Aktivitäten	IKT-Systeme	*Safety*	Automatisierungs-pyramide	Bemerkungen zu den Aktivitäten
		Telekommunikationsinfrastruktur und Kommunikationsdienste	z.B. VoIP, EDI, Internet, E-Mail, mobile Komm.			Zugang zu Kommunikationsdiensten, um mit allen internen und externen Anspruchsgruppen der Organisation kommunizieren zu können
		Integrierte Verwaltung aller Geschäftsprozesse	ERP		Ebene 5 ERP	Erleichtert die Erledigung der alltäglichen Aufgaben einer Organisation, muss aber mit allen IKT-Systemen verbunden sein (zentrales Nervensystem einer Organisation)
		Faktor Mensch	Gesamtheit der IKT-Systeme			Kann auf alle Anlagen und Systeme einwirken und zu fahrlässig oder böswillig verursachten Ausfällen führen
Organisatorisch (administrativ)						
Operativ *(industriell)*	Globale Steuerung	Steuerung des gesamten operativen Prozesses der thermischen Netze	Leitsystem – ICS	*Safety*	Ebene 3 SCADA/HMI	Überwachung, Erfassung, Kontrolle und Analyse des gesamten industriellen Prozesses (Kernstück des operativen Betriebs eines Unternehmens)
		Physischer Schutz der ICS				ICS können sich über mehrere Kilometer verteilt in ungeschützten Gebäuden befinden, was den physischen Zugriff auf bestimmte Systeme oder Anlagen ermöglicht
		Übermittlung von Sensordaten			Ebene 1 Sensoren/Aktoren	Übermittlung von Daten der Industrieanlagen an das Leitsystem, damit dieses sie interpretieren kann
		Steuerung des Alarmsystems			Ebene 3 SCADA/HMI	Alarmierung der Verantwortlichen bei Störungen, damit diese reagieren, kontrollieren und korrigieren können
	Produktion	Steuerung der Wärmepumpenversorgung			Ebene 3 SCADA/HMI	Wärmeversorgung der Wärmepumpen mittels Kompressor, Wasserpumpe oder Erdsonde
		Steuerung der Wärmeerzeugung (Feuerung und Wärmepumpen)			Ebene 3 SCADA/HMI	Steuerung der Wärmeproduktionseinheiten entsprechend den industriellen Prozessen der Feuerungen und Wärmepumpen
		Steuerung der Wärmerückgewinnung			Ebene 3 SCADA/HMI	Rückgewinnung der bei einer anderen industriellen Tätigkeit erzeugten Wärme zur Versorgung des thermischen Netzes
		Steuerung der Abhängigkeit von Abwärme			Ebene 4 MES	Organisatorische und operative Abhängigkeiten von einem anderen wärmeproduzierenden Unternehmen
	Transport	Steuerung des Druckhaltesystems			Ebene 3 SACADA/HMI	Aufrechterhaltung eines optimalen Druckniveaus im gesamten thermischen Netz, damit die Wärme bis zum Verbrauchsort gelangt

Abbildung 21: Kritische Aktivitäten

7.4 Verweise, Dokumente und Standards

7.4.1 Normative Dokumente

Dieser IKT-Minimalstandard für die Fernwärme und Fernkälteversorgung berücksichtigt Konzepte, Empfehlungen und Massnahmen von verschiedenen Standards und anderen normativen Dokumenten (Tabelle).

Titel	Jahr	Herausgeber/in & Beschreibung
Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI)	2012	Hrsg.: **Bundesamt für Bevölkerungsschutz (BABS)** Die nationale SKI-Strategie definiert den Geltungsbereich, bezeichnet die kritischen Infrastrukturen und hält die übergeordneten Grundsätze beim Schutz kritischer Infrastrukturen fest. Sie richtet sich an alle Stellen, die in diesem Bereich Verantwortung tragen, insbesondere an die jeweils zuständigen Behörden, die politischen Entscheidungsträger/innen und die Betreiber/innen von kritischen Infrastrukturen.
Massnahmen zum Schutz von industriellen Kontrollsystemen (SCADA/ICS)	2013–2020	Hrsg.: **Melde- und Analysestelle Informationssicherung MELANI (2013) – Nationales Zentrum für Cybersicherheit NCSC (2020)** Diese Anleitung beschreibt basierend auf US-amerikanischen Unterlagen des Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT) sowie des National Institute of Standards and Technology (NIST) knapp und pragmatisch auf acht Seiten die wichtigsten elf Massnahmen, die SCADA- bzw. ICS-Betreiber/innen umsetzen müssen.
Leitfaden Schutz kritischer Infrastrukturen (Leitfaden SKI)	2015–2018	Hrsg.: **Bundesamt für Bevölkerungsschutz (BABS)** Der Leitfaden SKI stellt ein Instrument zur Analyse und gegebenenfalls Verbesserung der Resilienz der kritischen Infrastrukturen dar. Er wurde namentlich für die Anwendung in kritischen Teilsektoren durch Betreiber/innen, Branchenverbände und Fachbehörden konzipiert. Im Wesentlichen schlägt der Leitfaden einen möglichen Risikomanagementprozess vor: Analyse (Identifikation der Ressourcen, Verwundbarkeiten, Risiken), Bewertung, Massnahmen (Definition, Umsetzung, Überprüfung und Verbesserung). Der Prozess kann durchaus bzw. sollte sogar in bestehende Managementprozesse integriert oder darauf aufbauend ausgeführt werden.
Bundesgesetz über die wirtschaftliche Landesversorgung **(Landesversorgungsgesetz, LVG; SR 531)**	2016	Hrsg.: **Bundesversammlung der Schweizerischen Eidgenossenschaft** Das LVG regelt Massnahmen zur Sicherstellung der Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen in schweren Mangellagen, denen die Wirtschaft nicht selber zu begegnen vermag. Der Bund kann im Rahmen der bewilligten Mittel Massnahmen von privatrechtlichen und öffentlich-rechtlichen Unternehmen zur Sicherstellung der wirtschaftlichen Landesversorgung fördern, sofern die Massnahmen im Rahmen der Vorbereitung auf eine schwere Mangellage zu einer wesentlichen Stärkung lebenswichtiger Versorgungssysteme und Infrastrukturen beitragen. Eine dieser Massnahmen bildet der vorliegende IKT-Minimalstandard.

Tabelle 49: Publikationen des Bundes, von Verwaltungsstellen sowie Verbänden, die für diesen Standard als wichtige Referenzdokumente dienen.

Titel	Jahr	Herausgeber/in & Beschreibung
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)	2018	Hrsg.: **Informatiksteuerungsorgan des Bundes (ISB)** Da der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt, hat der Bundesrat das ISB mit der Erarbeitung einer nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken beauftragt. Diese Strategie soll aufzeigen, wie diese Risiken heute aussehen, wie die Schweiz dagegen gerüstet ist, wo die Mängel liegen und wie diese am wirksamsten und effizientesten zu beheben sind. Die NCS identifiziert vorhandene Strukturen, definiert Zielsetzungen mit entsprechenden Massnahmen (z. B. Risiko- und Verwundbarkeitsanalysen eines Teilsektors).

Tabelle 49: Publikationen des Bundes, von Verwaltungsstellen sowie Verbänden, die für diesen Standard als wichtige Referenzdokumente dienen.

7.4.2 Internationale Standards

Die Tabelle zeigt eine weiterführende Auswahl an internationalen Standards, die teilweise in das vorliegende Dokument eingeflossen sind.

Titel	Jahr	Herausgeber/in & Beschreibung
BSI-Standard 100-4 Notfallmanagement	2009	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Etablierung eines Notfallmanagements, die auf den in Standard 200-2 beschriebenen Vorgehensweisen basiert und diese ergänzt. Beschrieben werden sämtliche Prozesse innerhalb einer Notfallorganisation von der Business-Impact-Analyse über das Krisenmanagement bis hin zur Rückführung und zu kontinuierlichen Prozesstätigkeiten ausserhalb von Krisensituationen.
ISA/IEC 62443 ff. Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme	2009–2013	Hrsg.: **International Society of Automation (ISA)/International Electrotechnical Commission (IEC)** Serie von insgesamt 13 Sicherheitsnormen und technischen Spezifikationen für industrielle Automatisierungs- und Steuerungssysteme (Industrial Automation and Control Systems, IACS). Die IEC 61508 ff. (Sicherheitsgrundnorm für IACS) umfassen das Thema Informationssicherheit und decken das Thema industrielle Automatisierungs- und Steuerungssysteme abschliessend und unabhängig ab. Vier verschiedene Aspekte bzw. Ebenen der Informationssicherheit werden behandelt: • Allgemeine Aspekte wie Konzepte, Terminologie oder Metriken: IEC 62443-1-x • IT-Sicherheitsmanagement: IEC 62443-2-x • System-Ebene: IEC 62443-3-x • Komponenten-Ebene: IEC 62443-4-x Speziell zu erwähnen ist, dass diese Normenserie auch die Netzwerk- und Zonenarchitektur abdeckt, die in anderen Standards nicht oder nicht so detailliert zu finden sind. Aktuell entwickelt sich diese Normenserie zur grundlegenden normativen Vorgabe im Bereich der RAMS-Normen (Reliability, Availability, Maintainability, Safety, zu Deutsch etwa «Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit») des CENELEC (u.a. EN 50126).

Tabelle 50: Nationale und internationale Standards für digitale Sicherheit

Titel	Jahr	Herausgeber/in & Beschreibung
BSI ICS Security-Kompendium	2013	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Das Kompendium stellt ein Grundlagenwerk dar und soll einen einfachen Zugang zur IT-Sicherheit von SCADA-Systemen ermöglichen. Erläutert werden die notwendigen SCADA-Grundlagen, die entsprechenden Abläufe, relevante Standards und der konkrete Zusammenhang mit dem IT-Grundschutz, wobei auch Unterschiede und Lücken etablierter Standards und insbesondere des IT-Grundschutzes im Bereich SCADA-Sicherheit aufgezeigt werden.
ISA/IEC 62264 ff. Enterprise-control system integration	2013–2016	Hrsg.: **International Society of Automation (ISA)/International Electrotechnical Commission (IEC)** Eine Reihe von insgesamt fünf Normen zur Integration von Unternehmens-IT sowie Kontroll- und Leitsystemen.
ISO 27001:2013 Information technology – Security techniques – Information security management systems – Requirements + ISO 27002:2013 Information security, cybersecurity and privacy protection – Information security controls	2013–2022	Hrsg.: **Internationale Organisation für Normung (ISO)** Erläutert im Detail die Anforderungen an ein Informationssicherheitsmanagementsystem (Information Security Management System ISMS). Die Reihe ISO 2700 ff. umfasst eine Serie von Informationssicherheitsstandards. Davon sind hier folgende von besonderem Interesse: • 27000:2018 Überblick und Terminologie • 27001:2013 Anforderungen: Grundlagen mit Kontrollen und Kontrollzielen im Anhang • 27002:2022 Leitfaden für Informationssicherheitsmassnahmen • 27003:2017 Informationssicherheitsmanagementsysteme – Anleitung zur Umsetzung • 27005:2018 Informationssicherheits-Risikomanagement • 27019:2017 Informationssicherheitsmassnahmen für die Energieversorgung Die Sicherheits-Normenreihe ISO 27000 ist mittlerweile weit verbreitet und dürfte sich in den kommenden Jahren als massgebender Referenzrahmen durchsetzen. Schon heute liegt durchaus richtig, wer ISO Sicherheitsstandards befolgt. Im Gegensatz zu anderen Standards oder Frameworks sind sie nicht zu detailliert, dementsprechend flexibel anwendbar und können über eine längere Zeitspanne kontinuierlich verbessert und erweitert werden. Das ISMS sowie der Inhalt der Massnahmen müssen branchenspezifisch adaptiert und umgesetzt werden.
Framework for Improving Critical Infrastructure Cybersecurity	2014	Hrsg.: **National Institute of Standards and Technology (NIST)** Dieses Framework ist aus der Forderung im US-Präsidialerlass «Improving Critical Infrastructure Cybersecurity» (Verbesserung der Cyber-Sicherheit kritischer Infrastrukturen) aus dem Jahre 2013 hervorgegangen und ist eine Zusammenstellung verschiedener Leitlinien, um den aktuellen Status in einem Unternehmen zu ermitteln und eine Roadmap zu verbesserten Cyber-Sicherheitspraktiken unter Bezugnahme auf andere Frameworks und Standards wie ISO27001, ISA 62443, NIST 800-53 und COBIT zu definieren.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev. 2	2015	Hrsg.: **National Institute of Standards and Technology (NIST)** Dieser Leitfaden gibt eine umfassende Einführung in SCADA-Topologien und Architekturen, identifiziert Bedrohungen und Verwundbarkeiten und gibt Empfehlungen zu Gegenmassnahmen und zur Risikominderung. Zudem werden SCADA-spezifische Kontrollen basierend auf dem NIST 800-53 Framework präsentiert.

Tabelle 50: Nationale und internationale Standards für digitale Sicherheit

Titel	Jahr	Herausgeber/in & Beschreibung
Recommended Practice: Improving Industrial Control System Cyber-security with Defense-in-Depth Strategies	2016	Hrsg.: **Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** Eine erweiterte und überarbeitete Ausgabe einer früheren Veröffentlichung aus dem Jahre 2006. Umfassende Einführung in die Defense-in-depth-Sicherheitsstrategie für industrielle Kontrollsysteme.
Communication network dependencies for ICS/SCADA Systems	2017	Hrsg.: **European Union Agency for Network and Information Security (ENISA)** Dieser Bericht konzentriert sich auf die Aspekte der Kommunikationsnetze und der Interkommunikation zwischen ICS/SCADA sowie die Erkennung von Schwachstellen, Risiken, Bedrohungen und Sicherheitsauswirkungen, die durch cyber-physische Systeme verursacht werden können. Er enthält auch eine Reihe von Empfehlungen zur Minderung der identifizierten Risiken. Das wichtigste Ergebnis der vorgängigen Studie ist eine Liste von bewährten Praktiken und Richtlinien, um die Angriffsfläche von ICS/SCADA-Systemen so weit wie möglich zu begrenzen. Das Hauptziel des Dokumentes ist es, einen Einblick in die Kommunikations-netzwerkabhängigkeiten der ICS/SCADA-Systeme zu geben sowie kritische Sicherheits-ressourcen und realistische Angriffsszenarien und Bedrohungen gegen diese Kommuni-kationsnetze zu identifizieren.
BSI-Standard 200-1 Managementsysteme für Informations-sicherheit (ISMS)	2017	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Der Standard beschreibt ISMS-relevante Methoden, Aufgaben und Aktivitäten, die ein erfolgreiches ISMS ausmachen, sowie die Aufgaben der Führungsebene. Bei der Umset-zung der Empfehlungen hilft die Methodik des IT-Grundschutzes, die eine Schritt-für-Schritt-Anleitung für die Entwicklung eines ISMS in der Praxis gibt und konkrete Mass-nahmen für alle Aspekte der Informationssicherheit nennt. Der Standard 200-1 richtet sich an Verantwortliche für den IT-Betrieb, Sicherheitsbeauftragte, Sicherheitsexpertinnen und experten sowie Sicherheitsberaterinnen und berater, die mit dem Informations-sicherheitsmanagement betraut sind.
BSI-Standard 200-2 IT-Grundschutz-Methodik	2017	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein System für das Informationssicherheitsmanagement in der Praxis und mithilfe der Grundschutz-Kataloge aufgebaut und betrieben werden kann. Es wird sehr ausführlich darauf eingegangen, wie ein Sicherheitskonzept in der Praxis erstellt wird, wie angemessene Sicherheitsmass-nahmen ausgewählt werden und was bei der Umsetzung zu beachten ist.
BSI-Standard 200-3 Risikomanagement	2017	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Durchführung von Risikoanalysen, die ein bestehendes IT-Grundschutz-Sicherheitskonzept ergänzen. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen als Hilfsmittel verwendet. Ein wesentlicher Unterschied zu den meisten anderen Risikoanalysemethoden ist das gänzliche Weglassen von Eintrittswahrscheinlichkeiten von Schadensereignissen.
ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements	2019	Hrsg.: **Internationale Organisation für Normung (ISO)** Detailliert die Anforderungen an ein Business-Continuity-Management-System.

Tabelle 50: Nationale und internationale Standards für digitale Sicherheit

Titel	Jahr	Herausgeber/in & Beschreibung
BSI IT-Grundschutz-Kataloge **BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz** **BSI Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz**	2019	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Der IT-Grundschutz beschreibt mithilfe der BSI-Standards 200-1 bis 200-3 und 100-4 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Informationssicherheits-managementsystems (ISMS). Die IT-Grundschutz-Kataloge sowie das IT-Grundschutz-Kompendium beschreiben die Umsetzung der damit einhergehenden Massnahmen und Ziele. Ein auf diese Weise aufgebautes ISMS erfüllt die Anforderungen von ISO 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen von ISO 27002. Sicherheit kann nach den vom BSI entwickelten Vorgehensweisen des IT-Grundschutzes, aber auch nach den Standards der ISO-27000-Reihe eingeführt und kontrolliert werden. Beide Möglichkeiten sind vom Ansatz her kompatibel. Mit beiden lässt sich ein ISMS aufbauen und betreiben, das die Risiken im Bereich der Informationssicherheit ermittelt und durch geeignete Massnahmen auf ein akzeptables Mass reduziert. Ein wesentlicher Bestandteil eines ISMS nach ISO 27001 ist die Risikoanalyse und -bewertung, wohingegen eine Risikoanalyse beim IT-Grundschutz des BSI nur in bestimmten Fällen erforderlich ist. In den IT-Grundschutz-Katalogen des BSI wird die detaillierte Vorgehensweise zur Minimierung von Risiken beschrieben. Demnach lassen die ISO-Standards mehr Interpretation offen und sind flexibler, geben aber auch entsprechend weniger detailliert Anleitung und Unterstützung. Für den IT-Grundschutz-Ansatz gilt demnach entsprechend das Gegenteil. Dieser bietet, wie der Name sagt, einen «Grundschutz». Der Aufwand für eine ISO-basierte Zertifizierung ist geringer.
Mapping of Dependencies to International Standards (Zuordnungstabelle)	2020	Hrsg.: **European Union Agency for Network and Information Security (ENISA)** In diesem Bericht wurden die Abhängigkeiten und Zusammenhänge zwischen Betreiber/innen von essenziellen Diensten (Operators of Essential Services, OES) und Anbietern digitaler Dienste (Digital Services Providers, DSP) analysiert und diverse Indikatoren für ihre Bewertung ermittelt. Diese Indikatoren sind internationalen Standards und Rahmenbedingungen zugeordnet, nämlich ISO/IEC 27002, COBIT 5, Sicherheitsmassnahmen der NIS-Kooperationsgruppe und dem Cyber-Sicherheitsprogramm des NIST Framework.
ISA/IEC 62351 ff. Power systems management and associated information exchange – Data and communications security	2022	Hrsg.: **International Society of Automation (ISA)/International Electrotechnical Commission (IEC)** Die Normreihe IEC 62351 beschreibt den Sicherheitsstandard für Energiemanagement-systeme und den dazugehörigen Datenaustausch. Es werden Massnahmen definiert, um die vier Grundanforderungen für eine sichere Datenkommunikation/Datenverarbeitung zu erfüllen.

Tabelle 50: Nationale und internationale Standards für digitale Sicherheit

7.5 Abkürzungsverzeichnis

Abkürzung	Beschreibung
ARA	Abwasserreinigungsanlagen
BABS	Bundesamt für Bevölkerungsschutz
BFE	Bundesamt für Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
BWL	Bundesamt für wirtschaftliche Landesversorgung
CEO-Betrug	Hacker senden eine angeblich dringende, jedoch gefälschte Zahlungsaufforderung im Namen eines Geschäftsleitungsmitglieds, für das sie sich ausgeben und das zu diesem Zeitpunkt oft nicht erreichbar ist.
DCS	Distributed Control System
DDC	Direct Digital Control
DMZ	Demilitarized Zone, IT-Netzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten (wird oft benutzt, um eine logische Trennung zwischen zwei Netzwerkzonen sicherzustellen).
EDI	Electronic Data Interchange
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Ressource Planning
EWS	Engineering Workstations
Fake Sextortion	Erpresser drohen mit der Veröffentlichung kompromittierender Bilder oder Informationen.
FINMA	Eidgenössische Finanzmarktaufsicht
HMI	Human Machine Interface, Stelle oder Handlung, durch die ein Mensch mit einer Maschine in Kontakt tritt.
ICS	Industrial Control System (dt. industrielles Kontrollsystem)
IDS	Intrusion Detection System (dt. Eindringungserkennungssystem)
IKT	Informations- und Kommunikationstechnologie (elektronische Datenverarbeitung EDV)
IP	Internet Protocol
ISA	International Society of Automation
ISB	Informatiksteuerungsorgan des Bundes
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
IT	Informationstechnologie (Information Technology), hier insbesondere Büro-IT/Büroautomation. Alles, was nicht OT betrifft.
KVA	Kehrichtverwertungsanlagen
MELANI	Melde- und Analysestelle Informationssicherung (Informatiksteuerungsorgan des Bundes)
MES	Manufacturing Execution System

Tabelle 51: Abkürzungsverzeichnis

Abkürzung	Beschreibung
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NCSC	Nationales Zentrum für Cybersicherheit
NIST	National Institute of Standards and Technology
OT	Operational Technology (insbesondere SCADA-Systeme)
Phishing	Opfer werden verleitet, ihre Passwörter und weitere persönliche Informationen anzugeben.
PLC	Programmable Logic Controller (dt. speicherpogrammierbare Steuerung)
Ransomware	Daten auf einem Gerät werden verschlüsselt und sind für deren Eigentümerinnen bzw. Eigentümer nicht mehr zugänglich.
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition, zur Überwachung und Steuerung technischer Prozesse. Zum SCADA-System gehören neben der Steuerung und Überwachung auch die Sensoren, Leitungen, Computer und die Leitstelle des (Produktions-)Systems. Gemeint sind insbesondere Kommissioniersysteme, Produktionssteuerungssysteme der Verarbeiter sowie Kassensysteme im Detailhandel.
SVGW	Schweizerischer Verein des Gas- und Wasserfaches
Thermische Netze	Bezeichnung, die sowohl die Fernwärme- als auch die Fernkälteversorgung umfasst
TNS	Thermische Netze Schweiz (vormals Verband Fernwärme Schweiz, VFS)
TWh	Terawattstunde
VFS	Verband Fernwärme Schweiz (ab 2023 Thermische Netze Schweiz, TNS)
VoIP	Voice-over-IP
WAN	Wide Area Network
WK	Wärmepumpe
WKK	Wärme-Kraft-Kopplung
WL	Wirtschaftliche Landesversorgung

Tabelle 51: Abkürzungsverzeichnis

7.6 Tabellenverzeichnis

7.7 Abbildungsverzeichnis

Autoren/Autorin der Erstausgabe

Name	Firma	Funktion
Sven Peter	BWL	Hauptautor/Projektleitung
Stefan Güpfert	SVGW	Co-Autor/Fachexperte/ Quality Assurance
Andreas Hurni	TNS	Co-Autor/Fachexperte/ Quality Assurance
Hans-Peter Käser	BWL	Fachexperte/Quality Assurance
Karsten Reichart	SVGW	Fachexperte/Quality Assurance
Stéphane Henry	BFE	Fachexperte/Quality Assurance
Giorgio Ravioli	BABS	Fachexperte/Quality Assurance
Alicia Kayser	ESB	Fachexpertin/Quality Assurance
Andreas Willen	EBL	Fachexperte/Quality Assurance
Boris Wächter	Primeo Energie	Fachexperte/Quality Assurance
Marcel Kränzlin	AEW	Fachexperte/Quality Assurance
Michael Gauer	IWB	Fachexperte/Quality Assurance
Patrick Steiger	SWL	Fachexperte/Quality Assurance
Philippe Roten	ERZ	Fachexperte/Quality Assurance
Reto Schär	Localnet AG	Fachexperte/Quality Assurance
Dominik Noger	EASZ	Fachexperte/Quality Assurance

Chronologie

Datum	Kurzbeschreibung
Februar 2021	Kontaktaufnahme mit dem SVGW zur Erstellung des IKT-Minimalstandards für die Fernwärme- und Fernkälteversorgung
März 2021	Kontaktaufnahme mit TNS zur Erstellung des IKT-Minimalstandards für die Fernwärme- und Fernkälteversorgung
Juni 2021	Erste Sitzung der Arbeitsgruppe
Dezember 2021	Identifizierung der kritischen Aktivitäten des Sektors
April–Mai 2022	Erarbeitung der Betaversion des französischen Dokuments und Übersetzung ins Deutsche
Juli 2022	Freigabe der Betaversion und Hinzufügen von Expertenkommentaren
September 2022	Endgültiges Korrekturlesen des Dokuments
Dezember 2022	Erstellung des endgültigen Designs des Dokuments
Februar 2023	Veröffentlichung des IKT-Minimalstandards für den Fernwärme- und Fernkältesektor

Das Dokument wurde unter Einbezug und Mithilfe des Bundesamtes für wirtschaftliche Landesversorgung (BWL), des Schweizerischen Vereins des Gas- und Wasserfaches (SVGW), Thermische Netze Schweiz (TNS) sowie von Fachexpertinnen und Fachexperten thermischer Netze erarbeitet.

Haftungsausschluss

Das vorliegende Dokument mit Empfehlungen zur Verbesserung der Cyber-Sicherheit der Informations- und Kommunikationssysteme in der Branche der thermischen Netze wurde von den beteiligten Personen und Stellen nach bestem Wissen und Gewissen erstellt. Das Bundesamt für wirtschaftliche Landesversorgung (BWL), Thermische Netze Schweiz (TNS), der Schweizerische Verein des Gas- und Wasserfaches (SVGW) sowie die involvierten Fachleute und Unternehmen übernehmen keine Gewähr, weder ausdrücklich noch implizit. Die Haftung und Verantwortung für mögliche Schäden sowie für den reibungslosen Betrieb obliegt einzig den Anwenderinnen und Anwendern.

Impressum und Kontakt

Herausgeber
Bundesamt für wirtschaftliche Landesversorgung BWL
Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Telefon +41 58 462 21 71

Konsultierte Verbände
Thermische Netze Schweiz (TNS) – vormals Verband Fernwärme Schweiz (VFS)
Schweizerischer Verein des Gas- und Wasserfaches (SVGW)

Bilder der Titelseite:
Brugg Rohrsystem AG, SIG – Services Industriels de Genève, EBL (Genossenschaft Elektra Baselland)