Erstellung eines IT-Grundschutz-Profils für ein Referenzunternehmen

(kleines/mittelständisches Unternehmen, KMU)

mit automatisierter Prozesssteuerung

(Industrial Control System, ICS)

Oder:

ICS-Security für kleine Unternehmen machbar machen

Vorgelegt als:	Masterarbeit
Bei:	Research Group IT-Security, RWTH Aachen
Von:	Sarah Fluchs
Matr.-Nr.	301450
Datum:	18. Juni 2017

1. Prüferin:
Prof. Dr.-Ing. Ulrike Meyer
Research Group IT-Security, RWTH Aachen

2. Prüfer:
Prof. Dr.-Ing. Ulrich Epple
Lehrstuhl für Prozessleittechnik, RWTH Aachen

Betreuer:
Dipl.-Inf. Holger Schildt
Bundesamt für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorbemerkungen und Danksagung

Im vorliegenden Dokument werden alle Überlegungen, Hintergründe und Entscheidungen dargelegt, die während der Erstellung des IT-Grundschutz-Profils eine Rolle gespielt haben. Damit ist die Arbeit als Hintergrundlektüre zu dem IT-Grundschutz-Profil zu verstehen, das ihr eigentliches Ergebnis ist.

Das IT-Grundschutz-Profil in der Version 1.0 trägt den Titel „IT-Grundschutz-Pilotprofil bzw. IT-Grundschutz-Profil für die Wasserwirtschaft“ und ist frei erhältlich. Es besteht aus einem Hauptprofil und perspektivisch fünf Unterprofilen. Das Hauptprofil sowie das Unterprofil Architektur (AR) wurden im Rahmen dieser Arbeit erstellt.

Als **IT-Grundschutz-Pilotprofil** ist das Dokument frei erhältlich und soll als Blaupause für die Erstellung weiterer IT-Grundschutz-Profile dienen. Es enthält keine komplette Maßnahmenempfehlung, sondern zeigt die Struktur und Grundideen eines Profils an einigen Beispielen auf.

Das **IT-Grundschutz-Profil für die Wasserwirtschaft** besteht aus dem frei verfügbaren Pilotprofil und einem kostenpflichtigen Anhang. Es enthält Empfehlungen für eine Informationssicherheitskonzeption für Institutionen der Wasserwirtschaft und basiert auf dem branchenspezifischen Sicherheitsstandard Wasser / Abwasser (B3S WA) gemäß § 8a (2) BSIG [BSIG16].

Der B3S WA wurde von den Branchenverbänden DWA[1] und DVGW[2] zur Feststellung der Eignung beim BSI eingereicht. Nach Feststellung der Eignung durch das BSI können durch die Anwendung des B3S WA auf den Sektor Wasser die Mindestanforderungen für IT-Sicherheit gemäß § 8a (1) BSIG erfüllt werden. Da sich der der B3S WA während der Niederschrift dieser Masterarbeit noch in der Prüfungsphase beim BSI befand, steht auch für das Profil für die Wasserwirtschaft die Genehmigung noch aus.

Auch der IT-Grundschutz befand sich zur Zeit der Niederschrift dieser Arbeit im Umbruch. Das IT-Grundschutz-Profil ist ein Konzept des modernisierten IT-Grundschutzes; allerdings war der Modernisierungsprozess zum Zeitpunkt der Niederschrift noch nicht abgeschlossen. Wo möglich, werden Begrifflichkeiten, Konzepte und Inhalte des modernisierten IT-Grundschutzes verwendet. Jedoch muss das Profil die bisherigen, noch nicht modernisierten IT-Grundschutz-Bausteine zurückgreifen, um Maßnahmen zu empfehlen.

Sobald die modernisierten Bausteine zur Verfügung stellen, sollten die bisherigen Bausteine mit Hilfe von Migrationstabellen ersetzt werden. Damit geht auch eine Anpassung der Begrifflichkeiten einher: Statt Maßnahmen werden in den modernisierten Bausteinen Anforderungen empfohlen.

[1] Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall

[2] Deutscher Verein des Gas- und Wasserfachs

Als Universitätsabsolventin im „Elfenbeinturm“ war die Autorin dieser Arbeit auf Unterstützung aus der Praxis angewiesen. Schließlich sollte als Ergebnis nicht nur ein theoretisch gutes Konzept für ein Pilotprofil, sondern auch ein praktisch brauchbares Profil für Anwender der Wasserwirtschaft entstehen.

Die Autorin dankt deshalb einer Vielzahl von Vertretern aus der automatisierungstechnischen Praxis und der Wasserwirtschaft für deren Aufgeschlossenheit und die geduldige Beantwortung sämtlicher Fragen – allen voran Rolf Tenner von den Stadtentwässerungsbetrieben Köln und Dr. Ludger Terhart von der Emschergenossenschaft / Lippeverband.

1 Einleitung

„For many complex IACS networks, there is no longer any single person who fully understands the system, […] and neither is there accurate documentation.“

Ralph Langner in seinem Buch
Robust Control System Networks — How To Achieve Reliable Control After Stuxnet [Lan12]

1.1 Problemstellung und Zielsetzung

Das vorangestellte Zitat lässt auf den ersten Blick den Bezug zur IT-Security vermissen. Was haben Systemkenntnis und Dokumentation mit Informationssicherheit zu tun? Die Antwort ist: Es ist sind Grundvoraussetzungen. Ihr Fehlen lässt in vielen Unternehmen mit automatischer Prozesssteuerung (Industrial Automation and Control System, IACS oder kurz ICS) die Erstellung einer Sicherheitskonzeption für ihre ICS-Netze als unüberschaubare Aufgabe erscheinen.

Leider wird diese Aufgabe aber immer wichtiger. Die Erfolgsgeschichte des Internets und der dazugehörigen Protokolle hat auch die industriellen Netze nicht unberührt gelassen: Ursprünglich physisch abgeschottet („air-gapped“), mit proprietären Protokollen und zu herkömmlichen Büro-Netzen völlig inkompatibler Hardware, gleicht sich nun die verwendete Technik von ICS-Netzen der von Büronetzen an. Die massenhafte Verbreitung von Ethernet- und IP-kompatibler Technik macht diese unschlagbar günstig – und der Effizienz- und Planungsgewinn durch die Vernetzung von Maschinensteuerung und Firmenverwaltung ist zu groß, um ihn nicht zu nutzen. Die Folge: ICS-Netze sind aus dem Internet potenziell genauso zugänglich wie Büro-Netze, mit allen Vorteilen für die Flexibilität und allen Nachteilen für die Sicherheit.

Es mangelt nicht an Regelwerken für die Informationssicherheit; eines davon ist der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Wie in vielen Regelwerken kamen ICS-Netze darin bislang nicht explizit vor. Die Absicherung von ICS-Netzen erfordert jedoch andere Prioritäten als die Absicherung von Büronetzen: Informationssicherheit in Büronetzen hat vor allem den Schutz sensibler Dateninhalte zum Ziel, während Informationssicherheit in ICS-Netzen vor allem schädliche Auswirkungen der Daten auf die physische Welt, also die gesteuerten Anlagen, verhindern soll. Im Zuge der Modernisierung des IT-Grundschutzes, innerhalb derer auch diese Arbeit entstanden ist, wird das Regelwerk deswegen explizit auf ICS-Netze erweitert.

Das Problem mit der ICS-Security ist jedoch nicht der Mangel an Regelwerken, die sinnvolle Sicherheitsmaßnahmen empfehlen. Das Problem ist, dass auch das beste Regelwerk individuell an die Anwenderinstitution angepasst werden muss – und dieser Aufwand ist nicht zu unterschätzen. Anwender müssen zunächst einmal den genauen Aufbau ihrer ICS-Netze kennen: Hardware, Software, Protokolle, Schnittstellen nach außen. Dies ist – hier deckt sich die Beobachtung des Eingangszitats mit den Erfahrungen der Autorin dieser Arbeit – weder trivial noch selbstverständlich. Auf die scheinbar harmlose Frage „wie sieht denn Ihr ICS-Netz aus?“

erhielt die Autorin mehr als einmal eine Antwort, deren Informationsgehalt sich mit „historisch gewachsen“ zusammenfassen lässt.

Das Problem verschärft sich noch, wenn man die Situation speziell in kleinen und mittelständischen Unternehmen (KMU) betrachtet. Während die ICS-Sicherheit für Konzerne mit eigener IT-Abteilung schon eine Herausforderung darstellt, haben kleinere Unternehmen in der Regel nicht einmal eine IT-Abteilung: Nur etwa 6% der KMU mit weniger als 250 Mitarbeitern haben nach Angaben des Statistischen Bundesamtes eigene IT-Fachkräfte, während es bei Unternehmen mit mindestens 250 Mitarbeitern 77% sind. Für IT-*Sicherheits*-Fachkräfte sind keine Zahlen bekannt [Destatis15a; Destatis17a].

Das Ziel dieser Arbeit ist deswegen die **Entwicklung eines Konzepts, mit dessen Hilfe besonders kleine Unternehmen (beispielsweise KMU) mit wenig Ressourcen und Know-How den IT-Grundschutz auf ihre ICS-Netze anwenden können**. Die Anwendung des Konzepts soll für den Anwender so wenig Aufwand und technische Fachkenntnis wie möglich erfordern und trotzdem in einer zweckdienlichen Absicherung münden.

So ein Konzept ist im modernisierten IT-Grundschutz als **IT-Grundschutz-Profil** vorgesehen. Ein solches Profil soll die Anwendung des IT-Grundschutzes für eine möglichst homogene Anwendergruppe („Referenzunternehmen“) demonstrieren. Damit ist es eine Art Schablone für ein Informationssicherheitskonzept, die dem Anwender einen möglichst großen Teil der Anpassungsarbeit des Regelwerks an seine eigene Institution abnimmt.

Da es bislang kein solches Profil gibt, wird das im Zuge dieser Arbeit entwickelte Profil den Status eines Pilotprofils annehmen, nach dessen Vorbild Profile für weitere Anwendergruppen erstellt werden können. Neben dem Pilotprofil soll dementsprechend eine Methodik entwickelt werden, die bei der Erstellung weiterer Profile unterstützt.

Gerade weil solide Systemkenntnis und Dokumentation so elementar für die Informationssicherheit und in der Praxis oft mangelhaft sind, soll das in dieser Arbeit entwickelte Pilotprofil das Kunststück vollbringen, aus minimaler Systemkenntnis des Anwenders neben sinnvollen Sicherheitsmaßnahmen einen möglichst genauen Plan von dessen ICS-Netzes zu generieren.

Ein so anwendernahes Vorhaben ist nicht umsetzbar, ohne eng mit einer konkreten Anwendergruppe zusammenzuarbeiten. Das explizite zweite Ziel dieser Arbeit ist es deswegen, mit dem Pilotprofil zugleich ein praktisch brauchbares IT-Grundschutz-Profil für eine konkrete Anwendergruppe auf den Weg zu bringen. Das erste Teilziel der vorliegenden Arbeit ist deswegen die Identifikation einer geeigneten Anwendergruppe für das Pilotprofil.

Die gesamte Vorgehensweise zur Erreichung der Ziele dieser Masterarbeit wird im folgenden Abschnitt 1.2 skizziert.

1.2 Vorgehensweise

Abb. 1.1. gibt einen Überblick über die Vorgehensweise, mit der die Problemstellung bearbeitet wird. Sie wird im Verlauf der Arbeit zu Beginn jedes Kapitels in Erinnerung gerufen, um eine Einordnung der Kapitelinhalte in das große Ganze zu erleichtern.

Die Vorgehensweise ist geteilt in die Erarbeitung von Inhalten (linke Seite, blau) und die Entwicklung von Methoden (rechte Seite, grün). Das Ziel der methodischen Arbeit ist die Entwicklung einer Methode für die Erstellung weiterer IT-Grundschutz-Profile. Das Ziel der inhaltlichen Arbeit ist die Entwicklung eines IT-Grundschutz-Profils für eine konkrete Branche, die Wasserwirtschaft. (Die Auswahl dieser Branche ist Teil der Arbeit und wird im weiteren Verlauf noch begründet.) Das resultierende IT-Grundschutz-Profil soll sowohl als „Wasser-Profil“ als auch als Pilotprofil genutzt werden können.

Der IT-Grundschutz ist so konzipiert, dass er auf konkrete Institutionen angewendet werden kann, um eine Sicherheitskonzeption für deren spezifischen Bedürfnisse zu erarbeiten. Für die Erstellung eines Profils muss der IT-Grundschutz ebenfalls angewendet werden – jedoch nicht auf eine konkrete Institution, sondern auf eine verallgemeinerte Institution, die stellvertretend für die Zielgruppe des Profils steht. Diese Institution wird Referenzinstitution genannt und die Gesamtheit ihrer abzusichernden Objekte Referenzarchitektur.

Somit sind auch die ersten Schritte in der Vorgehensweise dieser Arbeit schnell erklärt: Nachdem einige **Grundlagen** zu ICS-Netzen und zum IT-Grundschutz erläutert wurden, geht es an die Festlegung von Referenzinstitution und Referenzarchitektur.

Auf methodischer Seite werden Eingrenzungskriterien für die **Referenzinstitution** sowie Kriterien für die Bestimmung des Schutzbedarfs von Geschäftsprozessen festgelegt. Auf inhaltlicher Seite werden diese Eingrenzungskriterien genutzt, um eine geeignete Referenzinstitution – eine Institution der Wasserwirtschaft – und die dazugehörigen Geschäftsprozesse und Anlagen zu ermitteln. Auch die grundlegende ICS-Netzstruktur der Anlagen wird dafür berücksichtigt. Die Schutzbedarfskriterien werden für die Schutzbedarfsfeststellung der Geschäftsprozesse herangezogen.

Die **Referenzarchitektur** konkretisiert die abzusichernden Objekte der Referenzinstitution und ihre Verknüpfungen. Da die ICS-Architekturen der betrachteten Institutionen sich erheblich unterscheiden können, wird eine Methode entwickelt, um im Profil Variationen in der Referenzarchitektur abbilden zu können. Zusätzlich soll diese Methode eine möglichst anwenderfreundliche Ermittlung der passenden Variationen ermöglichen.

Für die Wasserwirtschaft wird die Methode mit Inhalten gefüllt, sodass am Ende eine Referenzarchitektur steht, die möglichst genau die möglichen Varianten in den ICS-Architekturen der Branche abbildet.

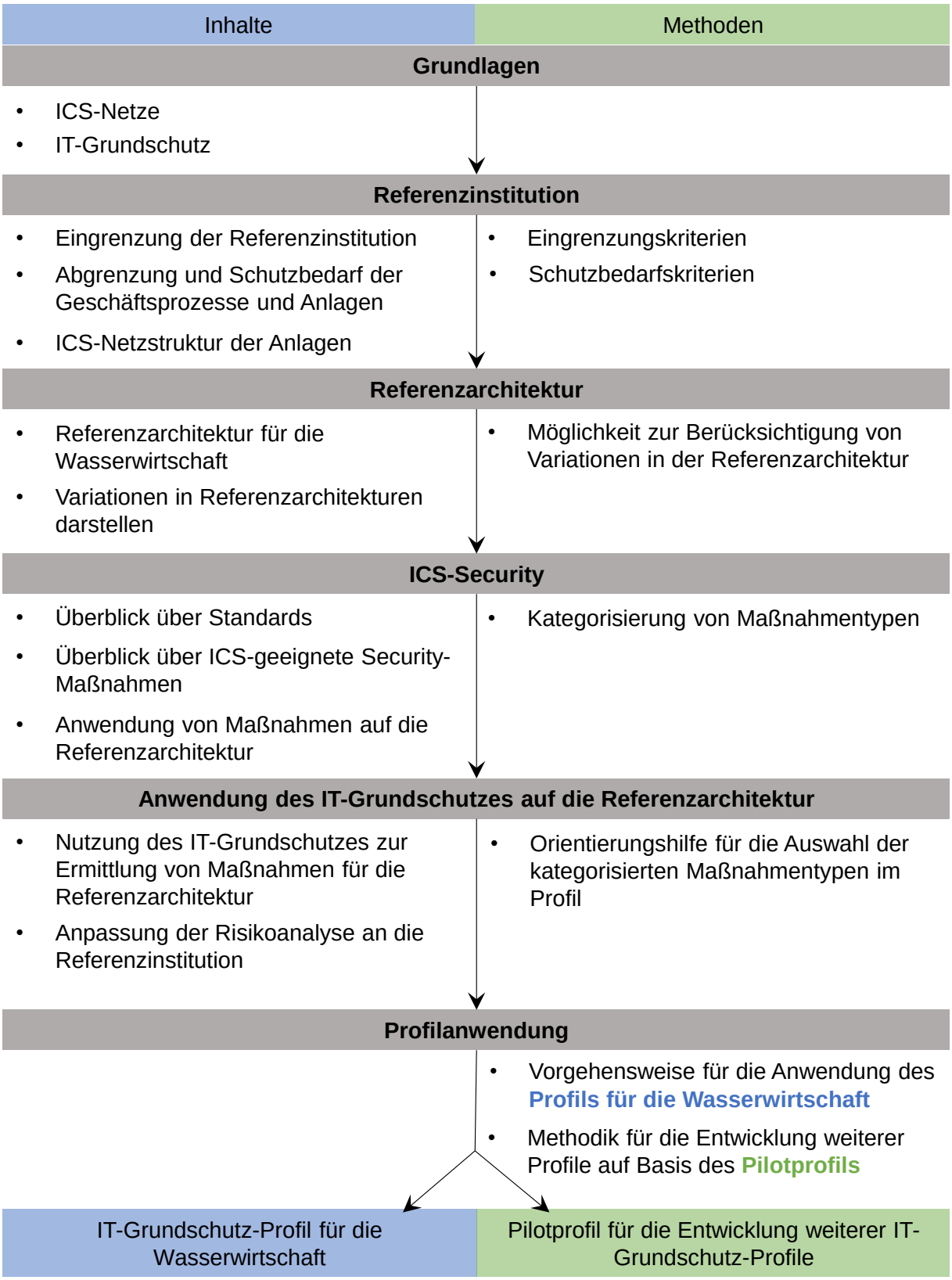


Abb. 1.1: Vorgehensweise der Masterarbeit

Nachdem die Betrachtungsgegenstände für die Erstellung des Sicherheitskonzeptes feststehen, widmet sich das folgende Kapitel der **ICS-Security**. Sein Ziel ist ein Überblick über relevante Standards und ICS-geeignete Security-Maßnahmen. Die Maßnahmentypen werden kategorisiert und die Maßnahmen, die die grundlegende Architektur von ICS-Netzen betreffen, werden auf die Referenzarchitektur angewendet.

Danach folgt die **Anwendung des IT-Grundschutzes auf die Referenzarchitektur** auf der inhaltlichen Seite: Der Schutzbedarf einzelner Objekte wird festgestellt und der IT-Grundschutz wird auf diese Objekte angewendet, um Maßnahmen zu ermitteln. Auch die Risikoanalyse, ebenfalls ein Teil des IT-Grundschutzes, wird an die Branche der Referenzinstitution angepasst. Die Methodenseite enthält in diesem Schritt eine Orientierungshilfe für die Zuordnung von Maßnahmen zu Zielobjekten, die auf der zuvor erfolgten Kategorisierung beruht.

Der letzte Schritt vollendet die Erarbeitung des IT-Grundschutz-Profils für die Wasserwirtschaft auf der inhaltlichen und des Pilotprofils auf der methodischen Seite, indem Methoden zur **Profilanwendung** für beide Fälle erarbeitet werden.

1.3 Begriffsdefinitionen

In diesem Abschnitt werden einige wesentliche Begriffe geklärt, die in der vorliegenden Arbeit häufig verwendet werden. Weitere Begrifflichkeiten werden im weiteren Verlauf der Arbeit erläutert. Alle Definitionen der in dieser Arbeit verwendeten Begriffe sind im Glossar und Abkürzungsverzeichnis (Kapitel 10, am Ende dieses Dokuments) zusammengestellt. Auch häufig verwendete Abkürzungen finden sich dort.

Der Begriff **Institution** wird in dieser Arbeit dann benutzt, wenn Unternehmen und Behörden gemeint sind. Konsequenterweise wird auch der Begriff *Referenzunternehmen* aus dem Titel und der in Abschnitt 1.1 dargelegten Problemstellung dieser Arbeit durch **Referenzinstitution** ersetzt.

Der Begriff **KMU** steht für kleine und mittlere Unternehmen. Es gibt dafür verschiedene Definitionen. Laut der Europäischen Union sind KMU Unternehmen mit weniger als 250 Mitarbeitern und höchstens 50 Mio. € Jahresumsatz. Das englische Kürzel SME steht für *small and medium-sized enterprises* [EU17]. Das Institut für Mittelstandsforschung (IfM) in Bonn zählt bei ebenfalls nicht mehr als 50 Mio. € Jahresumsatz Unternehmen mit weniger als 500 Mitarbeitern zu den KMU [IfM16].

Im Rahmen dieser Arbeit ist die genaue KMU-Definition nicht relevant. Da die Zielgruppe KMU unter dem Gesichtspunkt der oft geringeren personellen Ressourcen und des folglich geringeren IT-Know-Hows in kleineren Unternehmen ausgewählt wurde, reicht eine Definition nach Mitarbeiterzahlen aus. In dieser Arbeit sollen demnach Unternehmen mit weniger als 500 Mitarbeitern zu den KMU gezählt werden. Auch Behörden dieser Größe sollen zu den KMU zählen.

ICS (manchmal auch **IACS**) steht für **Industrial (Automation** and**) Control Systems** und bezeichnet Systeme zur Fertigungs- und Prozessautomatisierung im industriellen Umfeld. Unter den Begriff fallen in dieser Arbeit alle technischen Systeme, die für die automatisierte Steuerung eines Prozesses und die menschliche Überwachung dieser automatisierten Steuerung zuständig sind.

OT (Operational Technology) ist ein Oberbegriff für ICS und weitere Automationslösungen, die nicht im industriellen Umfeld verortet sind, etwa Gebäudeleittechnik oder Internet-of-Things-Geräte. In dieser Arbeit stehen jedoch speziell ICS im Fokus. Der Begriff *OT* wird nur zur allgemeinen Abgrenzung von der **IT (Information Technology)** verwendet.

Es gibt einen Unterschied zwischen Informationssicherheit und IT-Sicherheit: Während das Ziel von I**nformationssicherheit** der Schutz von Informationen jeglicher Art ist, will die **IT-Sicherheit** ausschließlich elektronisch gespeicherte Informationen schützen [BSI08c]. **ICS-Sicherheit** wiederum befasst sich mit auf ICS-Geräten elektronisch gespeicherten Informationen. Das Ziel der ICS-Sicherheit ist jedoch nicht nur der Schutz der Informationen, sondern insbesondere des Prozesses und der Anlagen, die diese Informationen steuern.

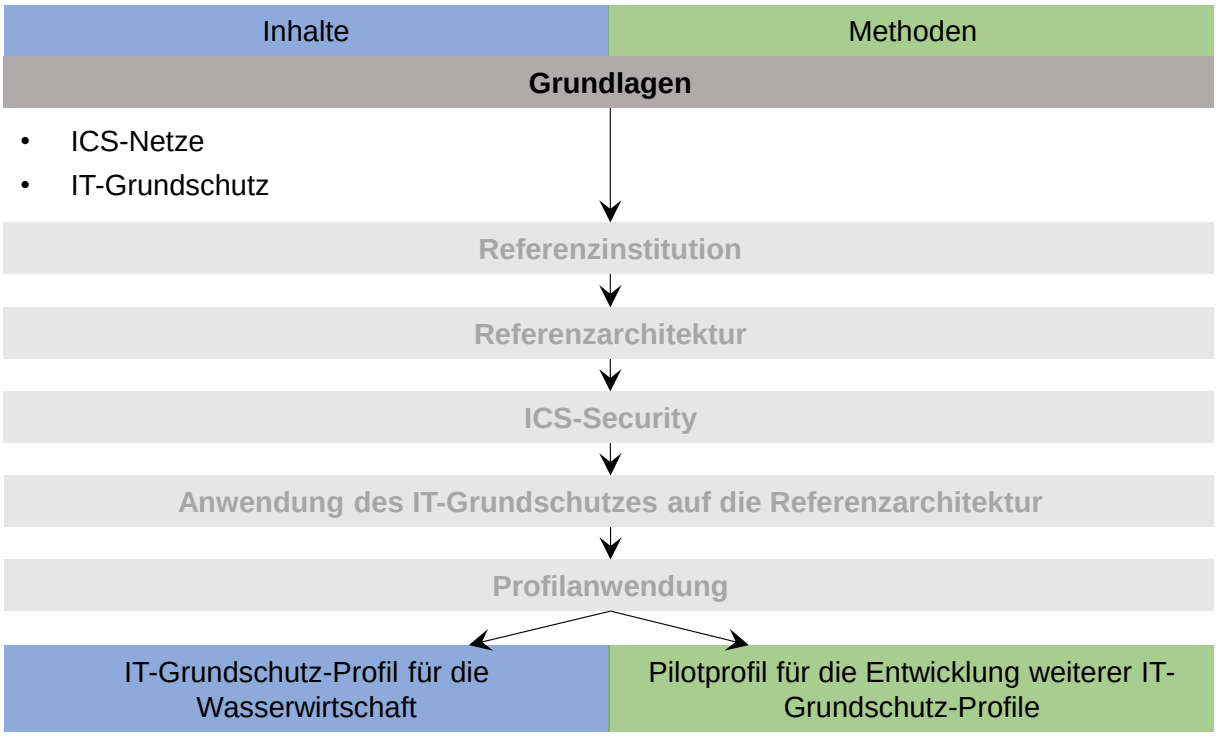
Der IT-Grundschutz hat die Zielsetzung der Informationssicherheit. Diese Arbeit arbeitet mit den Vorgehensweisen des IT-Grundschutzes, legt jedoch den Fokus auf die ICS-Sicherheit und damit einen Teilbereich der Informationssicherheit.

Es gibt in der Automatisierungstechnik weiterhin einen Unterschied zwischen den englischen Begriffen *Safety* und *Security*, die im Deutschen beide mit *Sicherheit* übersetzt werden. Mit **Security** ist die IT-Sicherheit bzw. ICS-Sicherheit der automatisierungstechnischen Komponenten gemeint. Der Begriff der (Functional) **Safety** wird häufig mit *funktionaler Sicherheit* übersetzt und hat zum Ziel, dass Maschinen oder Geräte funktionieren, ohne für ihre Umwelt gefährliche Zustände einzunehmen. Um dies sicherzustellen, sind spezielle Steuereinheiten, sogenannte Safety Instrumented Systems (SIS) aktiv, die gefährliche Maschinenzustände verhindern sollen [IEC15].

Der Unterschied zwischen Safety und Security ist gerade für ICS äußerst relevant. Aus diesem Grund werden in der vorliegenden Arbeit häufig die englischen Begriffe zur klareren Unterscheidung verwendet. Die ICS-Sicherheit wird durchgängig als **ICS-Security** bezeichnet, um sie von der *Safety* abzugrenzen. *Safety* ist nicht Betrachtungsgegenstand der vorliegenden Arbeit.

In der vorliegenden Arbeit wird ein IT-Grundschutz-Profil am Beispiel der Wasserwirtschaft entwickelt. Unter dem Begriff **Wasserwirtschaft** werden in der vorliegenden Arbeit Institutionen zusammengefasst, die Dienstleistungen innerhalb der Branchen „Öffentliche Wasserversorgung“ und „Öffentliche Abwasserbeseitigung“ erbringen.

2 Grundlagen



2.1 ICS-Netze

2.1.1 Automatisierungspyramide

Die Grundlage für die logische Struktur des verallgemeinerten ICS-Netzes bildet die Automatisierungspyramide (Abb. 2.1).

Auf der untersten Ebene, der **Feldebene**, befinden sich die Sensoren und Aktoren (Feldgeräte). Sie stellen die Schnittstelle zwischen der physischen Welt, also des zu steuernden Prozesses, und der digitalen Welt, also dem Automatisierungssystem, dar.

Die **Steuerungsebene** darüber ist für die direkte Ansteuerung der Aktoren auf Basis der Daten der Sensoren zuständig. Auf dieser Ebene läuft die Regelung oder Steuerung komplett automatisch, in der Regel ohne menschliche Eingriffe ab.

Im Gegensatz dazu werden auf der dritten Ebene mit der Bezeichnung **Prozessleitebene** die einzelnen Steuergeräte auf der darunterliegenden Ebene von Menschen überwacht, koordiniert und bedient.

Die **Betriebsleitebene**, ist die Schnittstelle zum unternehmerischen Teil der Anlage. Hier ist die Produktionsplanung und Qualitätssicherung verortet.

Die **Unternehmensleitebene** schließlich bildet die Spitze der Automatisierungspyramide. Hier werden die unternehmensweite Ressourcenplanung, das Controlling und die Optimierung der Wertschöpfungskette erledigt.

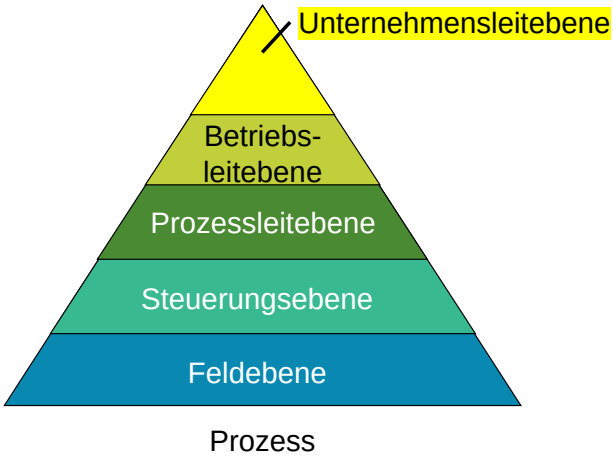


Abb. 2.1: Automatisierungspyramide (angelehnt an [Aut12])

2.1.2 Netzstruktur

Die Struktur des ICS-Netzes variiert stark. Beispielsweise können verschiedene Branchen, Unternehmenstypen, Rahmenbedingungen und Unternehmensgrößen unterschiedliche Netzstrukturen haben.

Das verallgemeinerte Netz in Abb. 2.2 ist das Resultat einer Recherche in Lehrbüchern, ([KL15], Kapitel 2 und 5; [VDI2182-3.1], Abb. 4; [VDI2182-3.2], Abb.2) Normen und Richtlinien ([NIST15a], Kapitel 2), Herstellerinformationen ([Sie06], [Sie10], [ABB13]) sowie mehrerer Telefonate mit Herstellern von Automatisierungstechnik. Es kann die Variantenvielfalt der realen ICS-Netze nicht erschöpfend abbilden. Jedoch soll das Netz den grundlegenden Netzaufbau erläutern und mögliche Unterschiede zwischen ICS-Netzen vermitteln.

In den folgenden Abschnitten werden die dargestellten Geräte, Software und Kommunikationstechnik in Abb. 2.2 näher erläutert. Der Bezug zur Automatisierungspyramide ist durch die farbliche Kennzeichnung analog zu Abb. 2.1 gegeben.

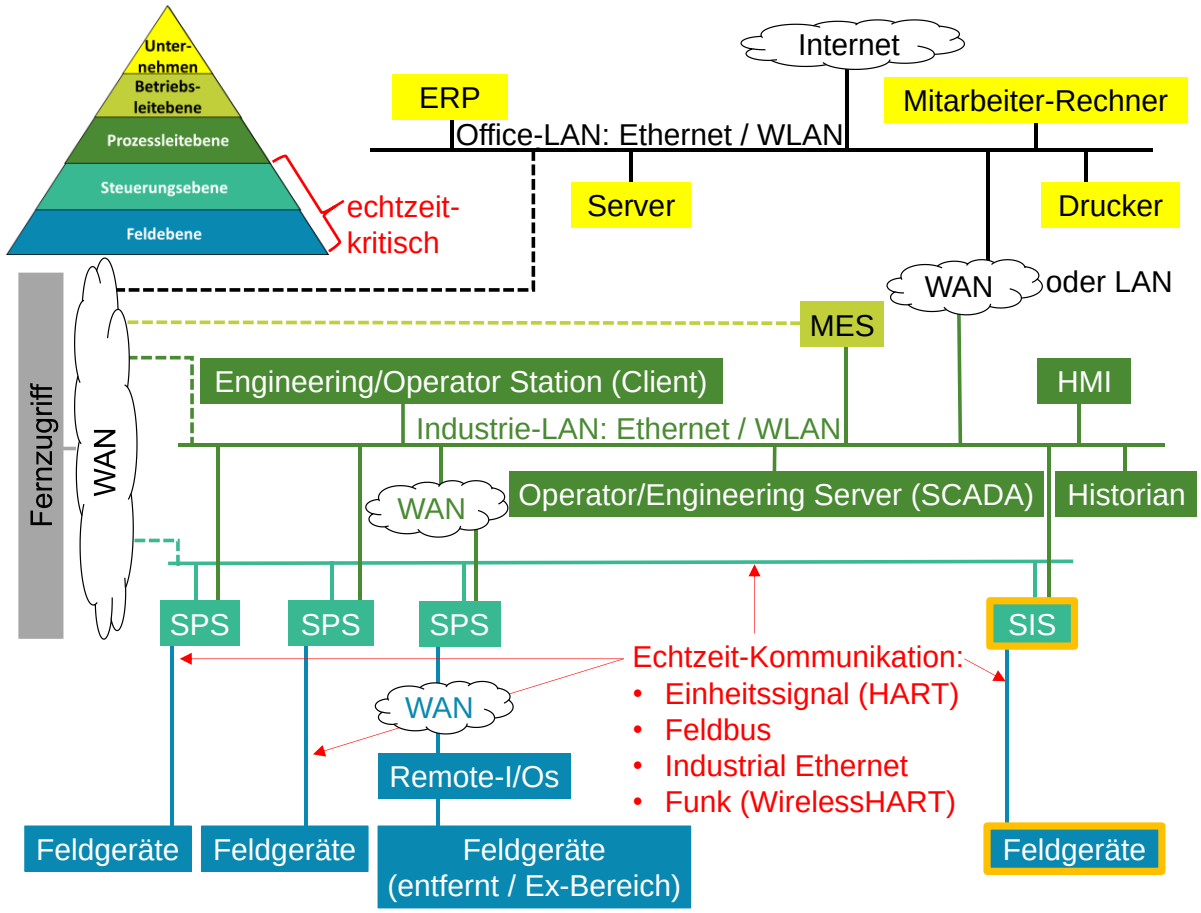


Abb. 2.2: Struktur eines ICS-Netzes

2.1.2.1 ICS-Geräte und Software

Die Aufgabe der technischen Geräte auf der Feldebene (**Feldgeräte**) ist der Input und Output (I/O): Sensoren wandeln Messungen aus der physischen Welt in elektronische Signale um, Aktoren umgekehrt. Für Sensoren und Aktoren, die weit entfernt von den Steuergeräten sind oder in besonders anspruchsvollen Umgebungen wie explosionsgefährdeten Bereichen arbeiten, können auch Remote-I/Os verwendet werden. Oft sind diese auch schlicht kostengünstiger, weil auf diese Weise nicht jedes einzelne Feldgerät an den Feldbus angeschlossen werden muss, sondern der Anschluss gebündelt über die Remote-I/O erfolgen kann. Remote-I/Os können Ein- und Ausgaben für mehrere Sensoren und Aktoren zusammenfassen und wenn nötig vorverarbeiten [Pep17].

Die Steuerungsebene umfasst alle Geräte, die automatisch einen Prozess steuern oder regeln können. Das bekannteste Beispiel sind **speicherprogrammierbare Steuerungen (SPS; auch bekannt unter dem englischen Begriff Programmable Logic Controller oder PLC)**: spezialisierte Computer, auf denen die nötigen Regelalgorithmen oder Steuerbefehle ausgeführt werden. Jedoch gibt es auch eine Vielzahl anderer Bezeichnung für Geräte mit leicht abweichender Funktionalität, wobei die Grenzen zunehmend verwischen. Beispiele sind Remote Terminal Units (RTUs) oder Programmable Automation Controllers (PAC) [Con15].

In Systemen mit besonderen Anforderungen an die Anlagensicherheit (Safety) finden sich häufig noch sogenannte **Safety Instrumented Systems (SIS)**. Diese Systeme werden in [IEC61511] definiert. Technisch gesehen sind sie nichts Anderes als Systeme aus normalen Steuergeräten, Sensoren und Aktoren, jedoch sind sie unabhängig vom restlichen System und sorgen beispielsweise dafür, dass die Anlage im Notfall abgeschaltet wird. SIS sind nur in der Prozesstechnik verbreitet [MBS11]. Für weitere Unterschiede zwischen Prozesstechnik und Fertigungstechnik siehe Kapitel 3.2.1: Automatisierungstechnische Domäne.

Auf der Prozessleitebene gibt es verschiedene Funktionen. Sie sind nicht zwingend alle vorhanden, und wenn sie es sind, dann können auch mehrere Funktionen auf demselben Rechner vereint sein. Oft sind die notwendigen Systeme in einem Raum bzw. einer Funktionseinheit, dem **Leitstand**, zusammengefasst.

Ein **SCADA-System (Supervisory Control And Data Acquisition)** erfüllt die Aufgabe eines Control Servers, auf dem alle Daten und Programme zusammenlaufen, um eine übergeordnete Prozesssteuerung auf Basis der unterlagerten SPSen zu ermöglichen. Ähnliche Funktionen hat auch ein **Prozessleitsystem (PLS, englisch: Process Control System, PCS oder Distributed Control System, DCS)**. Die ICS-Komponenten der Prozessleitebene machen von diesen zentralisierten Daten Gebrauch: **Engineering-Workstations** sind Rechner, auf denen Mitarbeiter Steuergeräte programmieren. Das **Human Machine Interface (HMI)** liefert aktuelle Anlagenzustände, meist in Form einer leserfreundlichen Grafik, auf der alle Anlagenteile erkennbar sind. Zudem ermöglicht es das Bedienen des Prozesses, etwa durch Setzen von Sollwerten. Prozessdaten werden zudem längerfristig in einem sogenannten **Historian** gespeichert [NIST15a; KL15].

Die Funktionen der Betriebsleitebene werden in größeren Unternehmen oft von einer Software mit dem Namen **Manufacturing Execution System (MES)** erfüllt. Auch für die Unternehmensleitebene gibt es dedizierte Software, das **Enterprise Resource Planning (ERP)**. In dieser Arbeit soll die Unternehmensleitebene auch das Office-Netz repräsentieren und damit sogenannte **Office-Komponenten**, die in jedem Büro zu finden sind: Computer für Mitarbeiter, Drucker, Datei- und Anwendungsserver [NIST15a].

2.1.2.2 Kommunikationstechnik

Die Feld- und Steuerungsebenen sind echtzeitkritisch; die Kommunikationsmedien auf diesen Ebenen müssen also eine Echtzeitkommunikation ermöglichen [Sie16]. Echtzeitkommunikation bedeutet, dass Signale zeitdeterministisch, also innerhalb eines garantierten Zeitfensters, ankommen müssen. Ethernet-Anschlüsse, wie sie für normale Büro-Internetanbindungen verwendet werden, können dies nicht leisten. Ethernet ist eine Standardfamilie (IEEE 802.3), die neben der physischen Übertragung auf Schicht 1 des ISO/OSI-Referenzmodells auch Funktionen der zweiten OSI-Schicht übernimmt. Dazu gehört die Medienzugriffskontrolle (Medium Access Control, MAC), die maßgeblich dafür verantwortlich ist, ob die Kommunikation deterministisch und somit echtzeitfähig ablaufen kann oder nicht.

Eine Lösung, um Echtzeitkommunikation zu gewährleisten, sind Point-to-Point (P2P)-Verbindungen, auf denen Daten in **Einheitssignale**n übertragen werden. Beispiele für Einheitssignale sind 4…20 mA oder 0…10 V. Oft wird das HART-Protokoll verwendet. Für P2P-Verkabelung ist ein einzelnes Kabel für jede Verbindung notwendig. Da auf diese Weise in komplexen Systemen schnell eine Vielzahl an Kabeln notwendig wird, wurden Feldbussysteme entwickelt. Ein **Feldbus** ist ein Bussystem, an das mehrere Teilnehmer angeschlossen werden können. Jeder Teilnehmer erhält alle über den Bus versendeten Daten, verarbeitet jedoch nur die für ihn bestimmten Daten. Feldbusse verwenden in der Regel proprietäre Protokolle, die sich von Hersteller zu Hersteller unterscheiden. Bekannte Beispiele für Feldbussysteme sind das amerikanische System Modbus und die deutsche Alternative PROFIBUS [KL15].

In den letzten Jahren hat sich aufgrund der Popularität des Internets Ethernet-Netztechnik immer mehr durchgesetzt, was sie überall verfügbar und günstig in der Anschaffung macht. Auch das Problem der proprietären, untereinander inkompatiblen Protokolle ist mit der Verwendung des Ethernet-Standards passé. Aus diesem Grund gibt es vielfältige hardware- oder softwareseitige Modifikationen des Ethernet-Standards, um ihn echtzeitfähig zu machen. Diese Kommunikationslösungen werden oft unter den Namen **Industrial Ethernet** oder Echtzeit-Ethernet zusammengefasst. Beispiele sind PROFINET, eine Weiterentwicklung von PROFIBUS, oder EtherCAT, das von der deutschen Firma Beckhoff entwickelt wird [KL15].

Auch Funknetze werden vermehrt für Echtzeitkommunikation genutzt. Weit verbreitet ist **WirelessHART**, eine drahtlose Implementierung des HART-Protokolls, die auf dem Funkstandard IEEE 802.15.4 basiert [KL15].

Local Area Networks (LAN) auf den darüberliegenden Ebenen, die nicht echtzeitkritisch sind, werden in der Regel mit **Ethernet**- oder **WLAN**-Technik gebildet. Dabei kann das Industrie-LAN auf der Prozessleitebene vom Office-LAN auf der Unternehmensebene getrennt sein. Ob die beiden Netze getrennt sind und welchem der beiden das MES der Betriebsleitebene zugeordnet ist, variiert.

Die Kommunikationstechnik *zwischen* den Ebenen kann ebenfalls stark variieren. Wird LAN-Technik verwendet, ist diese in der Regel ethernetbasiert. Liegen die Geräte auf den Ebenen nicht mehr in demselben Gebäudekomplex, wird **Wide Area Network (WAN)**-Technik notwendig. Solche weiteren Entfernungen können theoretisch auf allen automatisierungstechnischen Ebenen des Netzes vorliegen: Die Feldgeräte können von den Steuergeräten entfernt sein (zum Beispiel Messstellen in einem Kanalnetz), die Steuergeräte vom Industrie-LAN (zum Beispiel, wenn von einer Zentrale aus die Energietechnik mehrerer geografisch verteilter Gebäude gesteuert wird) und das Industrie-LAN vom Office-LAN (zum Beispiel, wenn ein Konzern mehrere lokale Produktionsanlagen vom Hauptstandort aus verwaltet). Verschiedene Arten der WAN-Technik werden in Kapitel 4.1 erläutert.

Aus dem Office-LAN heraus besteht in aller Regel eine Verbindung zum Internet. Dies muss aber nicht die einzige Verbindung nach außen bleiben: In ICS-Netzen sind häufig **Fernzugriff**e, beispielsweise für die Wartung durch Hersteller von ICS-Geräten, implementiert. Häufig sind diese Fernzugriffe zeitlich beschränkt. Das Netz oder das Gerät, auf das zugegriffen werden kann, variiert.

2.2 IT-Grundschutz

Der IT-Grundschutz ist eine Dokumentensammlung, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird. Das Werk soll Behörden und Unternehmen eine einfache Methode bieten, ihre Informationen und digitalen Systeme zu schützen. Erstmalig erschienen im Jahr 1994, drei Jahre nach der Gründung des BSI [BSI16f] wird der IT-Grundschutz laufend aktualisiert. Das ist nötig, um in der schnelllebigen Welt der Informationstechnik (IT) auf neue Techniken und damit verbundene neue Bedrohungen zu reagieren.

Diese Arbeit entsteht im Zuge einer grundlegenden Überarbeitung und Modernisierung des IT-Grundschutz. Die Modernisierung hat drei dominierende Gründe:

Der erste Grund ist die Erkenntnis, dass das mittlerweile mehr als 5000 Seiten umfassende Standardwerk nicht flexibel genug ist, um auf die immer kürzer werdenden Innovationszyklen in der IT reagieren zu können. Eine **Verschlankung** des IT-Grundschutz soll ihn flexibler und aktueller machen.

Ein zweiter Modernisierungsgrund ist die zunehmende Zahl vernetzter Geräte: Industrieanlagen im Zuge der „Industrie 4.0" und Alltagsgegenstände im Zuge des „Internet of Things" gehören mittlerweile auch zur IT und müssen in den IT-Grundschutz aufgenommen werden; eine umfassende **Umstrukturierung und Ausdehnung auf neue Technologien** ist also nötig.

Der dritte Grund ist eine Konsequenz der zunehmenden Vernetzung: Immer mehr Unternehmen und Behörden (in dieser Arbeit unter dem Oberbegriff Institution zusammengefasst) werden zunehmend abhängig von ihrer IT und die Auswirkungen eines möglichen IT-Versagens werden gravierender — gerade kleine und mittelständische Unternehmen (KMU) haben jedoch weder Ressourcen noch Know-How für ein durchdachtes Sicherheitskonzept. Der IT-Grundschutz soll im Rahmen der Modernisierung deswegen **näher an den Anforderungen der Anwender, vor allem von KMU**, ausgerichtet werden [Mün16; BSI16h].

Der IT-Grundschutz besteht aus mehreren Dokumenten. In den vier BSI-Standards ([BSI08a], [BSI08c] bzw. [BSI16e], [BSI08b], [BSI09]) wird die Methodik erläutert, nach der der IT-Grundschutz anzuwenden ist. Das IT-Grundschutz-Kompendium füllt die Methodik mit Inhalten. Es ist modular aufgebaut, um unterschiedlichen Anwendern die Anpassung an ihre Institution zu erleichtern, und enthält konkrete Sicherheitshinweise: Welche Infrastruktur in meiner Institution ist auf welche Art gefährdet und wie kann ich sie schützen?

Im Folgenden werden die Ideen und die wichtigsten Dokumente des IT-Grundschutz näher erläutert; insbesondere auch die Rolle der IT-Grundschutz-Profile. Einige Strukturen und Begrifflichkeiten haben sich innerhalb der Modernisierung verändert. In diesen Fällen werden in dieser Arbeit bevorzugt die Begriffe und Strukturen des modernisierten IT-Grundschutzes verwendet. Am Ende der Abschnitte 2.2.1 und 2.2.2 findet sich jeweils eine Vergleichstabelle (Tab. 2.1 und Tab. 2.2), um Änderungen des IT-Grundschutzes in der Modernisierung hervorzuheben und die Entsprechungen modernisierter Dokumente und Begriffe im bisherigen IT-Grundschutz zu verdeutlichen.

Da die in den folgenden Abschnitten eingeführten IT-Grundschutz-Begrifflichkeiten im Verlauf der Arbeit immer wieder verwendet werden, sind die wichtigsten Begriffe auch im Glossar und Abkürzungsverzeichnis am Ende dieser Arbeit nachzulesen.

2.2.1 BSI-Standards

Die vier BSI-Standards 100-1, 100-2, 100-3 und 100-4 beinhalten grundlegende Informationen über das Informationssicherheitsmanagementsystem, die Methodik zur Erarbeitung einer Sicherheitsstrategie, die Risikoanalyse und das Notfallmanagement nach IT-Grundschutz. Im Zuge der Modernisierung werden die Standards 100-1 bis 100-3 überarbeitet zu Standards 200-1 bis 200-3. Zum Zeitpunkt der Niederschrift dieser Arbeit waren jedoch nur die Standards 200-2 und 200-3 fertiggestellt.

2.2.1.1 Standard 100-1 (200-1)

Der **Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)** definiert allgemeine Anforderungen an ein ISMS. Der Begriff *ISMS (Information Security Management System)* bezieht sich dabei auf die in der internationalen Norm zur Informationssicherheit ISO/IEC 27001 gegebene Definition: Ein ISMS legt fest, mit welchen Instrumenten und Methoden das Management einer Institution deren Informationssicherheit sicherstellt [ISO27001]. Die ISO 27001 enthält allerdings nur allgemeine Hinweise und keine konkrete Empfehlung zur Umsetzung eines ISMS. Das BSI füllt diese Lücke: Der IT-Grundschutz ist die BSI-Empfehlung für ein ISMS nach ISO 27001 [BSI08a].

Der BSI-Standard 100-1 gibt eine Einführung in die Inhalte des Standards ISO 27001 und der dazugehörigen ISO 2700x-Standardfamilie. Diese Einführung ist zunächst unabhängig von der Methode, mit der das ISMS umgesetzt werden soll. Ihre Gliederung ist jedoch mit der Gliederung der IT-Grundschutz-Vorgehensweise kompatibel [BSI08a].

Die Norm ISO/IEC 27001 ermöglicht Institutionen, ihr ISMS zertifizieren zu lassen — das ist wichtig für Unternehmen, die gegenüber Kunden ihre Kompetenzen im Bereich Informationssicherheit nachweisen wollen [BSI08a]. Die Kompatibilität des IT-Grundschutzes mit ISO/IEC 27001 und die Möglichkeit der Zertifizierung auf Basis von IT-Grundschutz ist eine wichtige Eigenschaft des IT-Grundschutzes, die auch im Zuge der Modernisierung beibehalten werden soll [BSI16h].

2.2.1.2 Standard 200-2 (100-2)

Der **Standard 200-2: IT-Grundschutz-Methodik** ist eine Anleitung, wie das ISMS des BSI, also der IT-Grundschutz, auf eine konkrete Institution anzuwenden ist.

Im Zuge der Modernisierung soll die Vorgehensweise aus dem Standard 100-2 flexibler an Bedürfnisse verschiedener Institutionen in unterschiedlichen Situationen angepasst werden. Deswegen werden im modernisierten Standard 200-2 mehrere Varianten eingeführt, die in Abb. 2.3 grafisch dargestellt sind [BSI16h]:

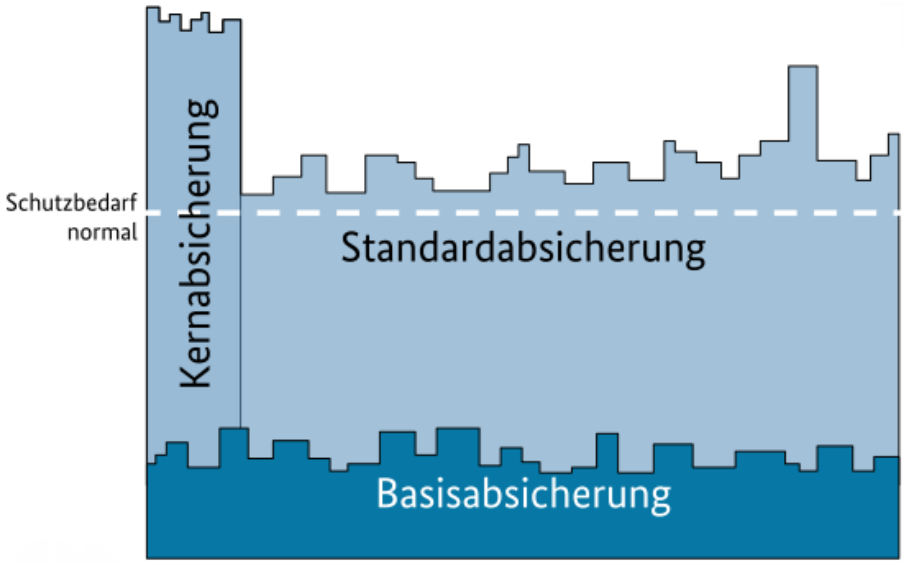


Abb. 2.3: Vorgehensweisen nach IT-Grundschutz (aus [BSI16h])

Die Basisabsicherung sorgt für eine grundlegende Absicherung aller Geschäftsprozesse und Ressourcen einer Institution und soll schnellstmöglich die größten Risiken senken, um dann eine gründlichere Absicherung darauf aufzubauen. Sie wird speziell mit Blick auf KMU entwickelt [BSI16h].

Die Kernabsicherung hingegen konzentriert sich zunächst auf einen kleinen, aber sehr wichtigen Teil eines Unternehmens und sichert diesen gründlich ab, bevor der Schutz auf andere Unternehmensbereiche ausgedehnt wird [Mün16].

Beide Vorgehensweisen sollten in der Standardabsicherung münden, die in den Grundzügen der Vorgehensweise nach Standard 100-2 entspricht [Mün16; BSI08c].

Für diese Arbeit ist vor allem die Standardabsicherung von Interesse, da auf ihrer Basis das IT-Grundschutz-Profil erstellt werden wird. Kapitel 8 des Standards 200-2 erläutert die konkreten Schritte, die zur Erstellung einer Sicherheitskonzeption nach der IT-Grundschutz-Vorgehensweise *Standard-Absicherung* notwendig sind [BSI17b].

1. **Festlegung des Informationsverbunds**: Der Informationsverbund definiert die Geschäftsprozesse, die im Rahmen des Sicherheitskonzepts erfasst werden sollen und ordnet ihnen die infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu, die für die Erbringung der Geschäftsprozesse nötig sind.
2. **Strukturanalyse:** Im Rahmen der Strukturanalyse wird der Informationsverbund zerlegt in *Zielobjekte*, also abzusichernde Prozesse, Anwendungen und IT. Außerdem wird das Zusammenspiel der Zielobjekte analysiert und dokumentiert. Das Resultat ist eine Liste aller Zielobjekte und eine grafische Darstellung der Vernetzung der Objekte in einem Netzplan.
3. **Schutzbedarfsfeststellung:** Für jedes Zielobjekt wird ein qualitativer Grad des Schutzbedarfs bezüglich der Grundwerte Integrität, Vertraulichkeit und Verfügbarkeit festgelegt. Empfohlene Schutzbedarfskategorien sind normal, hoch und sehr hoch; sie können bei Bedarf angepasst werden. Dasselbe gilt für die Grundwerte.

4. **Modellierung des Informationsverbunds**: Für jedes Zielobjekt wird mindestens ein passender IT-Grundschutz-Baustein ausgewählt. Da IT-Grundschutz-Bausteine Anforderungen enthalten, impliziert die Modellierung zugleich eine Auswahl von Anforderungen. Für die Erfüllung der Anforderungen müssen geeignete Maßnahmen gefunden werden.
5. **IT-Grundschutz-Check:** Der IT-Grundschutz-Check soll einen schnellen Überblick über das vorhandene Sicherheitsniveau bieten. Für den bereits modellierten Informationsverbund wird dabei erfasst, welche Anforderungen bereits erfüllt werden. Der IT-Grundschutz-Check wird in zwei Schritten durchgeführt: Einmal vor, einmal nach der Risikoanalyse. Für genauere Informationen zur Risikoanalyse siehe Abschnitt 2.2.1.3 zum Standard 200-3.
6. **Ergänzende Risikoanalyse:** Für Zielobjekte mit (sehr) hohem Schutzbedarf ist eine Risikoanalyse (vor der Modernisierung: ergänzende Sicherheitsanalyse und ergänzende Risikoanalyse) notwendig. Die Vorgehensweise dazu wird im Standard 200-3 (vor der Modernisierung: 100-3) beschrieben. Siehe dazu Abschnitt 2.2.1.3.

2.2.1.3 Standard 200-3 (100-3)

Der Standard **200-3: Risikoanalyse auf der Basis von IT-Grundschutz** beschreibt die Risikoanalyse, die nach Schritt 5 (IT-Grundschutz-Check) der Vorgehensweise in Standard 200-2 durchgeführt werden soll. Abb. 2.4 zeigt, wie die Risikoanalyse sich in die IT-Grundschutz-Vorgehensweise einfügt [BSI16e].

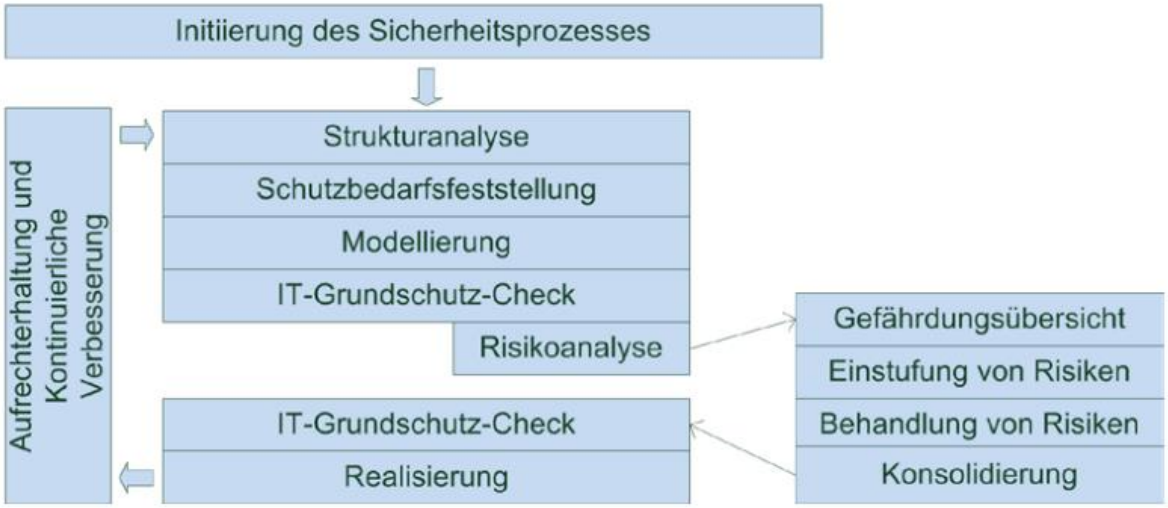


Abb. 2.4: Integration der Risikoanalyse in den IT-Grundschutz-Prozess (aus [BSI16e])

Eine explizite Analyse ist nur nötig, wenn

- einzelne Zielobjekte einen hohen oder sehr hohen Schutzbedarf zugewiesen bekommen haben,
- einzelne Zielobjekte durch existierende Bausteine nicht ausreichend modelliert werden können, oder wenn

- einzelne Zielobjekte in Einsatzszenarien verwendet werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Trifft keines der genannten Kriterien zu, ist keine explizite Risikoanalyse mehr nötig, da bei der Erstellung der einzelnen Bausteine durch das BSI bereits Risikoanalysen durchgeführt wurden.

Notwendige Arbeitsschritte der Risikoanalyse nach Standard 200-3 sind

1. **Gefährdungsübersicht:** Für jedes Zielobjekt (und das zusätzliche Zielobjekt „gesamter Informationsverbund") alle relevanten *elementaren* Gefährdungen aus den betreffenden Bausteinen auflisten. Dabei zusätzliche Gefährdungen für Grundwerte mit hohem/sehr hohem Schutzbedarf ermitteln.
2. **Risikoeinstufung:** Die betrachteten Gefährdungen auf Basis von Eintrittswahrscheinlichkeit und potentieller Schadenshöhe qualitativ bewerten. Aus diesen beiden Werten ergibt sich die Risikoeinstufung. Bei der Bewertung wird angenommen, dass die Basis- und Standard-Anforderungen aus den relevanten Bausteinen erfüllt werden. Risiken sind verbleibende Gefährdungen, die durch diese Standardanforderungen nicht ausreichend abgemildert werden.
3. **Behandlung von Risiken:** Für als Risiko eingestufte Gefährdungen eine Behandlungsmethode festlegen. Möglichkeiten sind Reduktion des Risikos durch ergänzende Sicherheitsmaßnahmen, Vermeidung durch Umstrukturierung des Informationsverbundes, Transfer durch Versicherungen oder Outsourcing, Akzeptanz eines vertretbaren Risikos oder Beobachtung des Risikos, falls es zwar jetzt akzeptabel ist, in Zukunft aber voraussichtlich steigen wird. Nach Festlegung der zusätzlichen Maßnahmen wird Schritt 2 unter Berücksichtigung dieser Maßnahmen wiederholt, um ihre Wirksamkeit einschätzen zu können.
4. **Konsolidierung des Sicherheitskonzepts:** Falls neue Anforderungen zu den in den Bausteinen üblichen hinzugefügt wurden, muss jedes Zielobjekt erneut geprüft werden. Prüfkriterien sind das Zusammenwirken der Maßnahmen, ihre Benutzerfreundlichkeit und Angemessenheit und natürlich ihre Eignung zur Gefährdungsabwehr.

Nach diesen Schritten folgt der Wiedereinstieg in die Vorgehensweise nach Standard 200-2 bei Schritt 5: IT-Grundschutz-Check (vgl. Abb. 2.4) [BSI08b].

2.2.1.4 Standard 100-4

Standard 100-4: Notfallmanagement beschreibt ein eigenes Managementsystem für die Geschäftsfortführung bei Notfällen und Krisen. Das Notfallmanagement eines Unternehmens legt den Fokus auf kritische Geschäftsprozesse, während das Managementsystem für die Informationssicherheit (ISMS) den Schutz der Informationen in den Mittelpunkt stellt. Zwischen dem IT-Grundschutz als ISMS und dem Notfallmanagementsystem bestehen aber viele Schnittmengen. Deswegen beschreibt der Standard 100-4, wie die Ergebnisse der IT-Grund-

schutz-Vorgehensweisen und Risikoanalyse auch als Input für das Notfallmanagement verwendet werden können. Eine Überführung des Standards 100-4 in eine modernisierte Version 200-4 war zum Zeitpunkt der Niederschrift dieser Arbeit kurzfristig nicht geplant [BSI09].

Tab. 2.1 gibt abschließend einen Überblick über die Änderungen von Konzepten und Begrifflichkeiten in IT-Grundschutz-Standards zwischen dem bisherigen und dem modernisierten IT-Grundschutz. Änderungen sind rot markiert. Die Informationen in der Tabelle stammen aus den bisherigen IT-Grundschutz-Standards [BSI08a; BSI08c; BSI08b; BSI09] und den Community Drafts der modernisierten Standards 200-2 und 200-3 [BSI17b; BSI16e].

Tab. 2.1: Änderungen von Konzepten und Begriffen in IT-Grundschutz-Standards zwischen dem bisherigen und dem modernisierten IT-Grundschutz

Bisheriger IT-Grundschutz		Modernisierter IT-Grundschutz	
Standard 100-1: ISMS		**Standard 200-1: ISMS**	
Standard 100-2: Vorgehensweise		**Standard 200-2: Vorgehensweise** - Basisabsicherung - Kernabsicherung - Standardabsicherung (entspricht 100-2)	
1. Definition des Geltungsbereichs	→ Informations-verbund	**1 .Definition des Geltungs-bereichs**	→ Informations-ver-bund
2. Strukturana-lyse	→ Zielobjekte	**2. Strukturana-lyse**	→ Zielobjekte
3. Schutzbedarfs-feststellung	für alle Zielobjekte	**3. Schutzbe-darfsfeststel-lung**	für alle Zielobjekte
4. Modellierung mit Bausteinen	für alle Zielobjekte → Maßnahmen-aus-wahl	**4. Modellierung mit Bausteinen**	für alle Zielobjekte → Anforderungs-aus-wahl
5. Basis-Sicher-heitscheck	Welche Standardmaß-nahmen nach IT-Grund-schutz sind bereits um-gesetzt?	**5. IT-Grund-schutz-Check**	Welche Standardanfor-derungen nach IT-Grundschutz sind be-reits erfüllt?
6 . Ergänzende Risikoanalyse		**6. Risikoana-lyse**	
Standard 100-3: Ergänzende Sicherheitsanalyse, ergänzende Risikoanalyse		**Standard 200-3: Ergänzende Risikoanalyse**	
für jedes Zielobjekt:		für jedes Zielobjekt:	
1. Gefährdungs-übersicht:	aus Bausteinen über-nommen; ggf. zusätzli-che Gefährdungen	**1. Gefähr-dungsüber-sicht:**	auf elementaren Ge-fährdungen und Bau-steinen basierend; ggf. zusätzliche Gefährdun-gen
2. Gefährdungs-bewertung	Risiko = unzureichend behandelte Gefährdung	**2. Risiko-einstufung**	Risiko = Gefährdung oben rechts in Risiko-matrix
3. Risikobehand-lung		**3. Risikobe-handlung**	
4. Konsolidierung		**4. Konsolidie-rung**	
Standard 100-4: Notfallmanagement		**Standard 100-4: Notfallmanagement** (vorerst keine Überarbeitung vorgesehen)	

2.2.2 IT-Grundschutz-Kompendium

Die IT-Grundschutz-Standards erklären die Methodik des IT-Grundschutzes; das Kompendium füllt die Methodik mit Inhalten. Vor der Modernisierung haben die IT-Grundschutz-Kataloge die Aufgabe des jetzigen IT-Grundschutz-Kompendiums erfüllt (s. Tab. 2.2).

Das IT-Grundschutz-Kompendium besteht aus drei Teilen:

- **Einführung** in die IT-Grundschutz-Standards (vor allem in die für die Anwendung des Kompendiums besonders relevante Modellierung mittels Bausteinen, siehe Abschnitt 2.2.1)
- **IT-Grundschutz-Bausteine**
- **Elementare Gefährdungen**

2.2.2.1 Bausteine

Die Bausteine sind unterteilt in Prozessbausteine und Systembausteine. Prozessbausteine modellieren einen Prozess oder Teilprozess eines Unternehmens (zum Beispiel Organisation und Personal oder Identitäts- und Berechtigungsmanagement), Systembausteine eine Komponente der Systemarchitektur (zum Beispiel Windows-Server) [BSI17c].

Sowohl Prozess- als auch Systembausteine sind noch weiter in Kategorien unterteilt. Bei den Systembausteinen ist im modernisierten IT-Grundschutz eine eigene Kategorie für Industrielle IT vorgesehen; die Bausteine tragen das Kürzel IND. Zum Zeitpunkt der Erstellung dieser Arbeit sind als IND-Bausteine vorgesehen:

- IND.1: ICS-Betrieb (Betriebs- und Steuerungstechnik / Operational Technology (OT))
- IND.2: ICS-Komponenten
    - IND.2.1: SPS
    - IND.2.2: HMI
    - IND.2.3: Maschine
    - IND.2.4: Feldgeräte
    - IND.2.5: Engineering-Workstation
    - IND.2.6: Leitstand
    - IND.2.7: Safety-System
    - IND.2.8: Historian

- IND.3: Produktionsnetze
    - IND.3.1: ERP/MES-Anbindung von ICS
    - IND.3.2: Industrielle Fernwartung
    - IND.3.3: Feldbus
    - IND.3.4: Steuerungsnetz

Auch unter den Bausteinen, die nicht explizit für die industrielle IT vorgesehen sind, finden sich für die industrielle IT relevante Bausteine – zum Beispiel der Prozess-Baustein OPS.2.4: Fernwartung. Die Identifikation aller relevanten Bausteine für das in dieser Arbeit erstellte IT-Grundschutz-Profil erfolgt in Abschnitt 6.3 [BSI17c].

Die Bausteine werden sich auf jeweils etwa 10 Seiten beschränken und damit deutlich schlanker sein als vor der Modernisierung. Konkrete Sicherheitsmaßnahmen stehen nicht in den Bausteinen im IT-Grundschutz-Kompendium, sondern in **Umsetzungshinweisen**, die in gesonderten Dokumenten veröffentlicht werden und somit flexibler aktualisiert werden können [BSI16h].

Bestandteile der Bausteine sind [BSI16b]

1. **Beschreibung:** Abgrenzung des behandelten Prozesses oder Systemelements, Zielsetzung des Bausteins.
2. **Gefährdungslage:** Aufzählung der spezifischen Bedrohungen und Schwachstellen für den Baustein sowie der für den Baustein relevanten elementaren Gefährdungen.
3. **Anforderungen und Zuständigkeiten:** Anforderungen sind Ziele, die mit konkreten Schutzmaßnahmen erreicht werden sollen, z.B. „Schutz vor Schadprogrammen“. Wie die Anforderungen konkret erfüllt werden sollen, steht in den Umsetzungshinweisen. Für normalen Schutzbedarf sind die Basis- und Standardanforderungen ausreichend. Darüber hinaus gibt es Anforderungen für erhöhten Schutzbedarf. Zuständigkeiten klären, wer in einer Institution für die Erfüllung der Anforderungen verantwortlich ist.
4. **Weiterführende Informationen:** Literaturhinweise o.ä.

   Anlage: U.a. eine Kreuzreferenztabelle, in der die für den Baustein zutreffenden Kombinationen aus elementaren Gefährdungen und jenen Anforderungen, die sie abmildern.

2.2.2.2 Elementare Gefährdungen

Die elementaren Gefährdungen sind eine Liste von (zum Erstellungszeitpunkt dieser Arbeit) 46 Gefährdungen, die für sehr viele Bausteine relevant sind, etwa Feuer oder Diebstahl. Die Liste soll die effiziente Durchführung eigener Risikoanalysen ermöglichen. Deswegen sind die elementaren Gefährdungen

- produktneutral und – soweit möglich – technikneutral,
- kompatibel mit vergleichbaren internationalen Katalogen und Standards,
- keine indirekten Gefährdungen, die durch das Fehlen von Sicherheitsmaßnahmen entstehen [BSI16e].

Gefährdungen bedrohen mindestens einen der **Grundwerte der Informationssicherheit**, die auch unter dem Kürzel CIA bekannt sind:

- **Vertraulichkeit (Confidentiality, C):** Informationen gelangen nicht an Dritte, für die sie nicht bestimmt sind.
- **Integrität (Integrity, I):** Es ist gesichert, dass Informationen unverfälscht sind.
- **Verfügbarkeit (Availability, A):** Alle Informationen, die ein System zur Erfüllung seiner Aufgaben benötigt, sind vorhanden [BSI16e].

Tab. 2.2 gibt abschließend einen Überblick über die Änderungen von Konzepten und Begrifflichkeiten für das IT-Grundschutz-Kompendium und die Umsetzungshinweise gegenüber den bisherigen IT-Grundschutz-Katalogen. Änderungen sind rot markiert. Die Informationen in der Tabelle sind den bisherigen IT-Grundschutz-Katalogen [BSI16a] und einem BSI-Vortrag zur Modernisierung [MSW16] entnommen.

Tab. 2.2: Änderungen von Konzepten und Begriffen für das IT-Grundschutz-Kompendium (bisher: Kataloge) zwischen dem bisherigen und dem modernisierten IT-Grundschutz

Bisheriger IT-Grundschutz		Modernisierter IT-Grundschutz	
Katalog		**Kompendium**	
1. Einführung in die Methodik		**1. Einführung in die Methodik**	
2. Modellierung mit Bausteinen		**2. Modellierung mit Bausteinen**	
3. Bausteinkataloge		**3. Bausteine**	
Bausteinaufbau:		Bausteinaufbau:	
	1. Kurzbeschreibung		1. Beschreibung, Abgrenzung, Zielsetzung
	2. Gefährdungslage		2. Gefährdungslage: elementare/spezifische Gefährdungen
	3. Maßnahmenempfehlungen		3. Anforderungen und Zuständigkeiten (Rollen)
	3. Kreuzreferenztabelle: Maßnahmen ↔ Gefährdungen		3. Kreuzreferenz-tabelle: Anforderungen ↔ elementare Gefährdungen
	4. Hinweise		4. Literatur, Hinweise
4. Gefährdungskataloge		**4. Elementare Gefährdungen**	
5. Maßnahmenkataloge		**Nicht Teil des Kompendiums!**	
Auflistung aller IT-Grundschutz-Maßnahmen. Oft ist eine einzelne Maßnahme für mehrere Bausteine relevant.		**Umsetzungshinweise:** Für viele Bausteine: konkrete, bausteinspezifische Maßnahmen für die Erfüllung der Anforderungen	

2.2.3 IT-Grundschutz-Profile

IT-Grundschutz-Profile sind ein neues Konzept des modernisierten IT-Grundschutzes. Die Idee der Profile folgt aus der Beobachtung, dass es viele Gruppen von Institutionen gibt, die sowohl in technischer als auch organisatorischer Hinsicht sehr ähnlich aufgebaut sind — beispielsweise Krankenhäuser oder Online-Händler. Besonders zeitaufwendige Teile der IT-Grundschutz-Vorgehensweise sind somit innerhalb dieser Gruppen sehr ähnlich: die Strukturanalyse, die Schutzbedarfsfeststellung und die Baustein-Modellierung der eigenen Institution.

Profile sollen Anwendern eine Schablone an die Hand geben, wie der IT-Grundschutz konkret auf die eigene Institution angewendet werden kann. Dazu führen sie für eine homogene Gruppe von Institutionen (bzw. eine Referenzinstitution) und für einen in dieser Gruppe übliche Architektur des Informationsverbunds (Referenzarchitektur) die IT-Grundschutz-Vorgehensweise exemplarisch durch.

Mithilfe von Profilen kann der IT-Grundschutz individuell an die Bedürfnisse einer einzelnen Branche angepasst werden. Aus diesem Grund sollen sie auch von Branchenvertretern selbst und nicht vom BSI erstellt werden [MSW16; MS16].

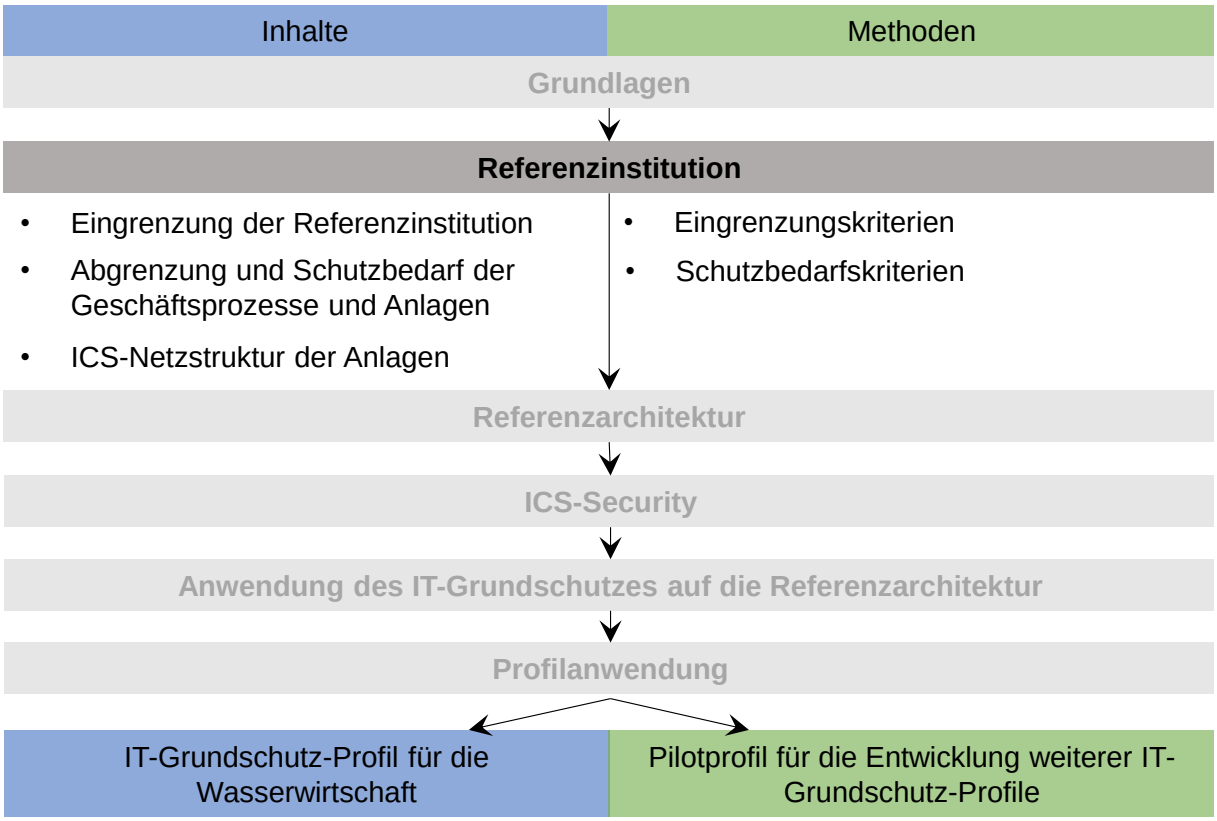
Das in dieser Masterarbeit entstehende Profil nimmt die Rolle eines Pilotprofils ein, denn zu Beginn der Arbeit gibt es noch keine fertigen IT-Grundschutz-Profile. Aus diesem Grund sind die Inhalte des Profils nicht fest vorgegeben; vielmehr ist der Vorschlag einer sinnvollen Profilstruktur ein Teilziel dieser Arbeit.

Die Struktur des in dieser Arbeit erstellten IT-Grundschutz-Profils zeigt Tab. 2.3. Sie ist an die – bislang nicht veröffentlichte – Strukturbeschreibung des IT-Grundschutz-Referats des BSI für ein IT-Grundschutz-Profil angelehnt [BSI16d; BSI17a].

Tab. 2.3: Struktur des IT-Grundschutz-Profils

1		**Formale Aspekte**
	1.1	Titel
	1.2	Autor, Verantwortliche/r
	1.3	Versionsstand, Revisionszyklus
	1.4	Vertraulichkeit
	1.5	Status der BSI-Anerkennung
2		**Management Summary**
	2.1	Zielgruppe
	2.2	Zielsetzung
	2.3	Inhalte
3		**Anwendung des Profils**
	3.1	Begriffsklärung
	3.2	Anwendungsfälle
	3.3	Hauptprofil und Unterprofile
	3.4	Vorgehensweise
	3.5	Integration in das Gesamtsicherheitskonzept
4		**Geltungsbereich**
	4.1	Zielgruppe (Referenzinstitution)
	4.2	Rahmenbedingungen
	4.3	IT-Grundschutz-Vorgehensweise, Schutzniveau
	4.4	ISO-27001-Kompatibilität
5		**Abgrenzung des Informationsverbunds**
	5.1	Organisationsstruktur
	5.2	Geschäftsprozesse und Anlagen
	5.3	Schutzbedarf der Anlagen
	5.4	ICS-Netzstruktur
6		**Referenzarchitektur**
	6.1	Zielobjektliste
	6.2	Netzpläne
	6.3	Schutzbedarf der Zielobjekte
7		**Anforderungen und Maßnahmen**
	7.1	Modellierung der Zielobjekte
	7.2	Auswahl der Anforderungen
	7.3	ggf. Umsetzungsvorgaben
8		**Risikobehandlung**
	8.1	Integration und Realitätsabgleich der Gesamt-Referenzarchitektur
	8.2	Vorgehensweise bei Abweichungen
	8.3	Hilfestellungen zur ergänzenden Risikoanalyse
9		**Anhang**
	10.1	Glossar
	10.2	Literaturverzeichnis
	10.3	Tabellen

3 Eingrenzung der Zielgruppe (Referenzinstitution)



Die Referenzinstitution für das in dieser Arbeit erstellte IT-Grundschutz-Profil muss einen Spagat leisten: Einerseits soll sie abstrakt sein, damit sich eine möglichst große Anwendergruppe darin wiederfinden kann. Andererseits muss sie aber auch so konkret sein, dass die Anwender die Empfehlungen des Profils möglichst direkt auf ihre eigene Institution anwenden können.

Aus diesem Grund soll für die Referenzinstitution eine Gruppe von Institutionen gewählt werden, die hinsichtlich der wesentlichen Eingrenzungskriterien in sich so homogen wie möglich ist. Als eine sehr gut geeignete Zielgruppe hat sich die Wasserwirtschaft herauskristallisiert. In diesem Kapitel wird die Eingrenzung auf die Wasserwirtschaft anhand der **organisatorischen Eingrenzungskriterien** Unternehmensstruktur und Rahmenbedingungen und der **technischen Eingrenzungskriterien** Automatisierungstechnische Domäne und ICS-Netzstruktur begründet.

Technisches und organisatorisches Wissen über die Wasserwirtschaft wurde, wann immer möglich, durch Fachliteratur, Regelwerke und Normen belegt. Branchenwissen, das nicht explizit durch eine Quellenangabe belegt ist, stammt aus im Rahmen dieser Masterarbeit geführten Gesprächen mit Branchenexperten.

3.1 Organisatorische Eingrenzungskriterien

Bei organisatorischen Eingrenzungskriterien ist nicht nur wichtig, dass die betrachtete Unternehmensgruppe homogen ist. Organisationsstruktur und Rahmenbedingungen können auch Auswirkungen auf weitere Profilinhalte wie Schutzbedarf und rechtliche Anforderungen haben.

3.1.1 Unternehmensstruktur

3.1.1.1 Größe

Die Größe der Referenzinstitution ist in der Problemstellung dieser Arbeit in Abschnitt 1.1 umrissen: Die Zielgruppe sollen kleine und mittelständische Unternehmen sein, also Unternehmen mit weniger als 500 Mitarbeitern (Definition siehe Abschnitt 1.3). Die meisten Unternehmen der Wasserwirtschaft erfüllen dieses Kriterium.

In Deutschland gibt es etwa 16 000 Unternehmen, die zu diesem Sektor zählen, darunter etwa 6000 in der Wasserversorgung und etwa 10 000 in der Abwasserbeseitigung [Destatis15b]. Mit etwa 75 000 Beschäftigten in der Wasserwirtschaft haben die Unternehmen der Branche im Durchschnitt gerade einmal fünf Mitarbeiter [Destatis11]. Laut einer Recherche der Dienstleistergewerkschaft ver.di, bei der 854 deutsche Unternehmen der Wasser- und Abwasserversorgung erfasst wurden, **haben 92% der Unternehmen höchstens 500 Mitarbeiter**. Ver.di hat dabei jedoch nur Unternehmen ab 20 Beschäftigte berücksichtigt — mit Berücksichtigung dieser Kleinstbetriebe dürfte der Anteil also noch höher ausfallen [Verdi15].

Die wenigen großen Betriebe in der Wasserwirtschaft sind entweder in der Hand großer Städte (zum Beispiel Berlin, Hamburg, München, Köln oder Frankfurt), großer privater Unternehmen (zum Beispiel die Gelsenwasser AG, Veolia Wasser GmbH oder Thüga AG) oder großer Zweckverbände (zum Beispiel der Zweckverband Bodensee-Wasserversorgung oder Emschergenossenschaft / Lippeverband) [BSI15].

3.1.1.2 Betriebsform

Die Ursache für die große Anzahl kleiner Unternehmen liegt in den rechtlichen Rahmenbedingungen: In Deutschland sind nach Grundgesetz Art. 28 Abs. 2 und diversen Landesverfassungen die **Kommunen für die Wasserversorgung und Abwasserbeseitigung verantwortlich** [DWA15].

Der überwiegende Teil der Unternehmen in der Wasserwirtschaft haben **öffentlich-rechtliche Betriebsformen**: In der Wasserversorgung waren es im Jahr 2008 56%, in der Abwasserentsorgung 2011 sogar mehr als 90%. Öffentliche Betriebsformen umfassen dabei Eigenbetriebe, Regiebetriebe, Zweckverbände und Anstalten öffentlichen Rechts (AöR). Sind die Betriebe privatrechtlich, also als GmbH oder AG organisiert, dann meist in Form von Eigengesellschaften oder öffentlichen Gesellschaften. Eine Mischform stellen die Öffentlich-Privaten-Partnerschaften (ÖPP) dar [BSI15].

Wenn privatrechtliche Betriebsformen gewählt werden, besitzt die Kommune trotzdem die Handlungshoheit — zumeist, weil sie genügend Anteile an den Betrieben und/oder Stimmrechte erhält [BSI15].

3.1.1.3 Organisationsstruktur

Die **Organisationsstruktur der Betriebe ist heterogen**, abhängig von ihrer Größe und ihrem Aufgabenspektrum. Oft sind die Betriebe nicht ausschließlich in der Wasserwirtschaft tätig, sondern Mehrfachdienstleister. Darunter fallen die meisten Stadtwerke. Die Dienstleistungen Wasserversorgung und Abwasserbeseitigung sind dann nur ein Teilbereich neben anderen Dienstleistungen wie Strom, Gas, Wärme, Telekommunikation und Mobilität. Die Abwasserbeseitigung ist zudem häufig direkt bei der Stadtverwaltung angesiedelt. Auch in diesem Fall kann das Personal oft nicht klar einer Dienstleistung zugeordnet werden [Verdi15].

Dementsprechend sind die Abteilungsstrukturen schwierig zu verallgemeinern. Wasserversorgung und Abwasserbeseitigung sind in der Regel getrennt verantwortet. Bei kleineren Anlagen, die von Stadtwerken oder der Stadtverwaltung mitbetrieben werden, gibt es oft nur eine einzige Abteilung für den Betrieb der Anlage oder er ist Teilaufgabe einer übergeordneten Abteilung [Her16; Kar14; Stei17]. Größere, auf die Wasserwirtschaft spezialisierte Dienstleister haben mehrere Abteilungen, zumindest eine kaufmännische und eine technische.

Wenn es eine IT- oder EDV-Abteilung gibt, so kann diese auch der kaufmännischen statt der technischen Abteilung unterstellt sein [StEB14; Nor16]. Dies birgt Herausforderungen für die Informationssicherheit, weil sie abteilungsübergreifend verantwortet werden muss. Die technische Abteilung kann noch weiter unterteilt sein. Häufig wird die Verantwortung für Kanalnetze und Aufbereitungsanlagen oder Kläranlagen getrennt, was auch den Kategorien aus automatisierungstechnischer Sicht entspricht (siehe Abschnitt 3.2.1, [Sch13; Fle17]).

Zusammenfassend ist die Wasserwirtschaft ist bei Betrachtung des Eingrenzungskriterium *Unternehmensgröße* als Zielgruppe dieser Arbeit gut geeignet, weil der Großteil der Betriebe wie in der Aufgabenstellung der Masterarbeit gefordert weniger als 500 Mitarbeiter hat.

Betrachtet man die Betriebsform, so ist die Wasserwirtschaft ebenfalls eine relativ homogene Branche mit überwiegend öffentlich-rechtlichen Betriebsformen, die stets kommunal verantwortet werden.

Die Organisationsstrukturen innerhalb der Betriebe sind heterogen; für die im Fokus dieser Arbeit stehende Informationssicherheit ihrer Automatisierungstechnik ist jedoch die Homogenität der technischen Strukturen wichtiger — und diese ist gegeben, wie in Abschnitt 3.2.2 gezeigt werden wird.

3.1.2 Rahmenbedingungen

Rahmenbedingungen, also für eine bestimmte Unternehmensgruppe geltende Gesetze, Richtlinien und Normen, sind wichtige Eingrenzungskriterien: Sie können spezielle Anforderungen,

Reglementierungen und Schutzbedarfe für die betrachteten Anlagen der Referenzinstitution nach sich ziehen.

3.1.2.1 EU-Richtlinien und deutsche Verordnungen

Da die Wasserversorgung und Abwasserbeseitigung zu der grundlegenden Daseinsvorsorge eines Staates gehören, unterliegen sie zahlreichen Rahmenbedingungen auf unterschiedlichen Verwaltungsebenen.

Die EU-Trinkwasserrichtlinie (98/83/EG, [TWRL98]) und die EU-Kommunalabwasserrichtlinie (91/271/EWG, [AWRL91]) legen Mindeststandards zur Trinkwasserqualität und zur Abwasserreinigung fest. Mit der Trinkwasserverordnung (TrinkwV 2001, [TrinkwV01]) und der Abwasserverordnung (AbwV, [AbwV97]) sind sie in deutsches Recht umgesetzt.

Die EU-Wasserrahmenrichtlinie (2000/60/EG, [WRRL00]) macht Zielvorgaben für die Qualität der Gewässer, die die Wasserwirtschaft als Quellen nutzt und in die sie die gereinigten Abwässer einleitet. Ihre Umsetzung in nationales Recht findet sich im Wasserhaushaltsgesetz (WHG, [WHG09]).

Die Umsetzung aller erwähnten deutschen Verordnungen liegt in der Verantwortung der Kommunen [DWA15].

Das im Rahmen dieser Arbeit erstellte Profil muss demnach hinsichtlich des Schutzbedarfs und der Risikobewertung die besondere Stellung der Wasserwirtschaft als **EU-weit reglementierte Versorgungsleistung** berücksichtigen.

3.1.2.2 Regelwerke der Verbände

Die Interessen der Wasserwirtschaft werden durch mehrere Verbände repräsentiert. Hier sind vor allem die Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) und der Deutsche Verein des Gas- und Wasserfaches (DVGW) zu nennen, die jeweils über 10 000 Mitglieder haben. Beide Verbände geben Regelwerke heraus, in denen sie branchenweite Qualitäts- und Sicherheitsstandards definieren [BSI15].

Einige dieser Standards regeln Gesichtspunkte, die auch in den Umfang des in der dieser Arbeit erstellten Profils fallen. In diesen Punkten sollte das Profil mit **bestehenden Anforderungen der Verbands-Regelwerke** konform sein, um für die Anwender keinen Interessenskonflikt zu erzeugen.

3.1.2.3 IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen

Zusätzlich zu der EU-weiten Reglementierung der Wasserwirtschaft als Versorgungsleistung zählt der Sektor Wasserwirtschaft zu den kritischen Infrastrukturen (KRITIS).

Das Bundesministerium des Innern (BMI) definiert in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen Kritikalität als ein „relatives Maß für die Bedeutsamkeit einer Infrastruk-

tur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat" [BMI09]. Dementsprechend werden Kritische Infrastrukturen (KRITIS) in derselben Publikation umschrieben als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden" [BMI09].

KRITIS unterliegen in größerem Maße staatlicher Kontrolle und Kooperationsverpflichtungen. Seit Juli 2015 gilt das IT-Sicherheitsgesetz, kurz IT-SiG, das KRITIS-Betreiber verpflichtet, ihre kritischen Dienstleistungen nach dem Stand der Technik angemessen abzusichern und dies mindestens alle zwei Jahre überprüfen zu lassen. Auch die Meldung von IT-Sicherheitsvorfällen schreibt das Gesetz vor [IT-SiG15].

Mitglieder einer KRITIS-Branche können gemäß § 8a (2) BSIG [BSIG16] selbst branchenspezifische IT-Sicherheitsstandards (B3S) entwickeln, um die vorgeschriebene Absicherung nach dem Stand der Technik für ihre Mitglieder zu erleichtern [BSI16g]. Das BSI kann dabei auf Anfrage beratend tätig sein. Die Verbände DWA und DVGW erarbeiten zum Zeitpunkt der Erstellung dieser Arbeit bereits einen B3S Wasser / Abwasser (B3S WA). Er wird als Informationsgrundlage für diese Arbeit genutzt.

Welche Anlagenbetreiber innerhalb der KRITIS-Branchen genau unter das IT-SiG fallen, legt nicht das Gesetz selbst fest — dies geschieht in der Verordnung zur Bestimmung kritischer Infrastrukturen, kurz BSI-KritisV [KritisV16]. Danach gelten die Bestimmungen des IT-Sicherheitsgesetzes für

- Abwasserkanalisation ab 500 000 angeschlossenen Einwohnern
- Kläranlagen mit einer Ausbaugröße ab 500 000 Einwohnerwerten[3]
- Abwasserbeseitigungs-Leitzentralen mit einer Ausbaugröße der gesteuerten und überwachten Anlagen ab 500 000 Einwohnerwerten
- Trinkwassergewinnungsanlagen mit gewonnener Wassermenge ab 22 Mio. m³/Jahr
- Wasserwerke mit Wasseraufkommen ab 22 Mio. m³/Jahr
- Aufbereitungsanlagen mit aufbereiteter Trinkwassermenge ab 22 Mio. m³/Jahr
- Wasserverteilungssystemen mit verteilter Wassermenge ab 22 Mio. m³/Jahr
- Wasserversorgungs-Leitzentralen, deren gesteuerte und überwachte Anlagen mindestens 22 Mio. m³/Jahr Wasser verarbeiten.

[3] Der Einwohnerwert ist ein Vergleichswert für die in Abwässern enthaltenen Schmutzfrachten. Er ergibt sich aus Summe der Anzahl angeschlossener Einwohner und eines Vergleichswerts, mit dessen Hilfe sich die Schmutzfracht gewerblicher Abwässer in Einwohnerzahlen ausdrücken lässt [DIN16323].

Diesen Kriterien entsprechen mit etwa 230 Anlagen nur 1,4% der etwa 16 000 vorhandenen Anlagen [Bor16].

Das in dieser Arbeit erstellte IT-Grundschutz-Profil soll die Übernahme der Sicherheitsmaßnahmen nicht nur für KRITIS-Betreiber, sondern gerade auch **für die große Mehrheit der kleineren Anlagenbetreiber** ermöglichen. Auch wenn diese bislang nicht gesetzlich zur Einhaltung der Informationssicherheit verpflichtet sind, so haben sie doch — wenn auch in kleineren Maßstäben — dieselben technischen Infrastrukturen und damit dieselben IT-Sicherheitsprobleme wie die KRITIS-Betreiber.

3.2 Technische Eingrenzungskriterien

3.2.1 Automatisierungstechnische Domäne

In der Automatisierungstechnik haben sich zwei Domänen herausgebildet: die Prozesstechnik und die Fertigungstechnik. Zwischen beiden bestehen signifikante Unterschiede, die sich auch im Aufbau des ICS-Netzes niederschlagen.

Der Prozesstechnik werden Betriebe zugeordnet, die formlose **Produkte** wie Gase, Flüssigkeiten und Schüttgüter hervorbringen — klassische Branchen sind Chemie- und Pharmaindustrie, Öl- und Gasraffinerien, aber auch große Teile der Lebensmittelindustrie. Zur Fertigungstechnik gehören solche Betriebe, deren Produkte diskrete Werkstücke, also Festkörper mit eigener Form oder einen Verbund von Festkörpern, sind. Branchenbeispiele sind die Automobilindustrie und ihre Zulieferer sowie weite Teile des Maschinenbaus. Es gibt aber auch hybride Anlagen, die Merkmale aus beiden Domänen besitzen. Die Darstellung der Unterschiede in den folgenden Absätzen beruht – soweit nicht anders gekennzeichnet – auf [MBS11].

Die **Anlagensicherheit (Safety)** spielt in der Prozesstechnik eine größere Rolle. Die Ursache dafür liegt in der Natur der zugrundeliegenden Prozesse: In der Prozesstechnik werden die physikalischen und chemischen Eigenschaften eines Produkts verändert. Aktoren können darauf einwirken, indem sie die richtigen Bedingungen für einen physikalischen oder chemischen Prozess schaffen. Der Prozess selbst aber läuft eigenständig und kann nicht beliebig ein- und ausgeschaltet werden; ein Herunterfahren der Anlage führt somit nicht zwangsläufig zu einem sicheren Zustand.

In der Fertigungstechnik hingegen gibt es meistens zumindest einen sicheren Zustand: den energielosen Zustand, wenn alle Anlagen abgeschaltet sind. Um die Anlagensicherheit im eingeschalteten Zustand sicherzustellen, reichen meist einfache physische Maßnahmen wie das Umzäunen des Bewegungsbereichs eines Roboterarms.

In der Prozesstechnik muss die Safety aufwendiger gewährleistet werden: Oft gibt es dedizierte Steuergeräte, die unabhängig sicherstellen, dass der chemische oder physikalische Prozess nie seinen sicheren Zustand verlässt. Diese Steuergeräte werden Sicherheitssysteme

oder Safety Instrumented Systems (SIS) genannt und in den Normen IEC 61508 und IEC 61511 definiert [IEC61508; IEC61511]. Sie agieren auf der Steuerungsebene und sind im Beispiel-ICS-Netz in Abb. 2.2 (wie auch häufig in der Industrie) orangefarben markiert. In der Fertigungstechnik sind solche Systeme nicht üblich.

Auch bei den ICS-Komponenten wie Steuergeräten, Sensoren und Aktoren und Engineering Stations, die grundsätzlich in beiden Domänen vorkommen, gibt es grundlegende Unterschiede. Der Grund: In der Fertigungstechnik liegt das **Prozess-Know-How** tendenziell beim Hersteller, nicht beim Betreiber der Anlage; in der Prozesstechnik ist es umgekehrt.

In der Prozesstechnik werden häufig komplette Fertigungsstraßen an Betreiber verkauft. Dabei können durchaus verschiedene Fertigungsstraßen von verschiedenen Herstellern stammen — nicht immer gibt es bereichsübergreifende, übergeordnete Leitsysteme. In der Prozesstechnik hingegen haben sich solche übergeordneten Leitsysteme etabliert [ZVEI10].

Ein weiterer Unterschied ist die Andersartigkeit der **Aktoren** in beiden Domänen: Während sie in der Prozesstechnik nur Rahmenbedingungen für einen Prozess schaffen können, verursachen sie in der Fertigungstechnik oft direkt als Werkzeug die nötige Produktveränderung. Als eine Folge ist der Zustand der Aktoren und somit die Qualitätskontrolle in der Fertigungstechnik deutlich relevanter.

Eine weitere Folge betrifft die **Echtzeitanforderungen** der Steuergeräte und Datenübertragung: Zwar sind Automatisierungssysteme sowohl in der Fertigungs- als auch in der Prozesstechnik echtzeitkritisch, die Zykluszeiten der Steuergeräte in der Fertigungstechnik sind jedoch tendenziell geringer [FA09] (S.159).

Ein letzter Punkt und nicht ganz unwichtig für die Erstellung eines Profils, das als praxisnahe Richtlinie für Anwender dienen soll: Die Prozess- und Fertigungstechnik haben unterschiedliche **Verbände**, nutzen unterschiedliche **Modelle und Begrifflichkeiten** und folgen teils unterschiedlichen **Normen** [MBS11].

Aufgrund der Vielzahl der Unterschiede zwischen den beiden Domänen muss das Tätigkeitsfeld der Referenzinstitution für diese Arbeit entweder auf die Prozess- oder auf die Fertigungstechnik begrenzt werden. Sowohl die Wasserversorgung als auch die Abwasserbeseitigung sind gänzlich der Prozesstechnik zuzuordnen und somit hinsichtlich des Eingrenzungskriteriums *Automatisierungstechnische Domäne* homogen.

3.2.2 ICS-Netzstruktur

Die Homogenität der automatisierungstechnischen Netzstruktur ist vor allem deswegen wichtig, weil ein grundlegendes Element eines IT-Grundschutz-Profils die Referenzarchitektur ist, in der möglichst viele Anlagenbetreiber ihre eigene Architektur wiederfinden sollen.

Die Wasserwirtschaft eignet sich hinsichtlich dieses Eingrenzungskriteriums sehr gut, da die technische Infrastruktur für alle automatisierten Geschäftsprozesse in der Wasserversorgung und Abwasserentsorgung ausgesprochen homogen ist.

Abb. 3.1 und Abb. 3.2 zeigen den grundlegenden Netzaufbau der ICS-Komponenten einer Anlage in der Wasserwirtschaft. Sie übertragen Netzinformationen aus der KRITIS Sektorstudie des BSI [BSI15] und des DWA-Merkblattes M 253 [DWA11] auf die grundlegende ICS-Netzstruktur, die in Abschnitt 2.1 eingeführt wurde. Die Grundstruktur der Anlagen ist an einer Stelle variabel: Bei der **räumlichen Verteilung** der Steuer- und Feldgeräte.

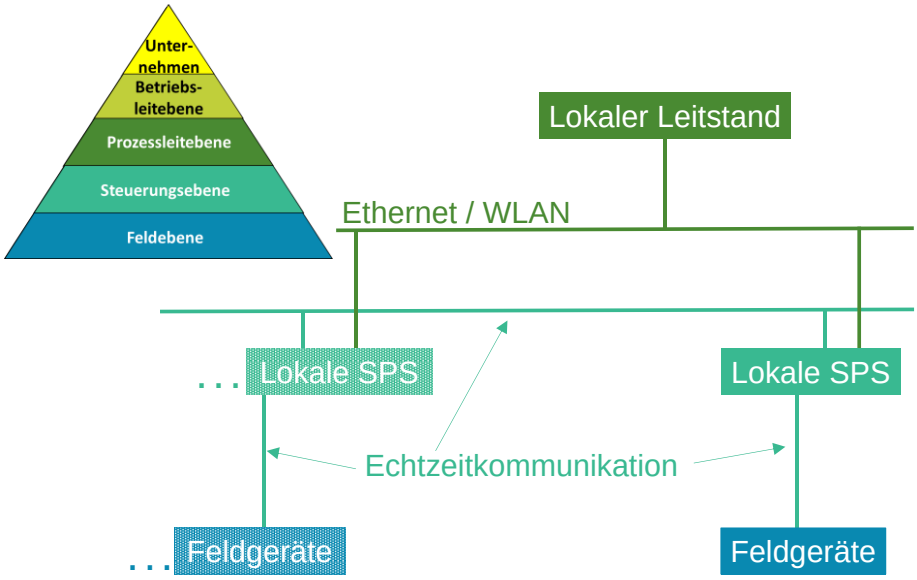


Abb. 3.1: Konzentrierte ICS-Netzstruktur

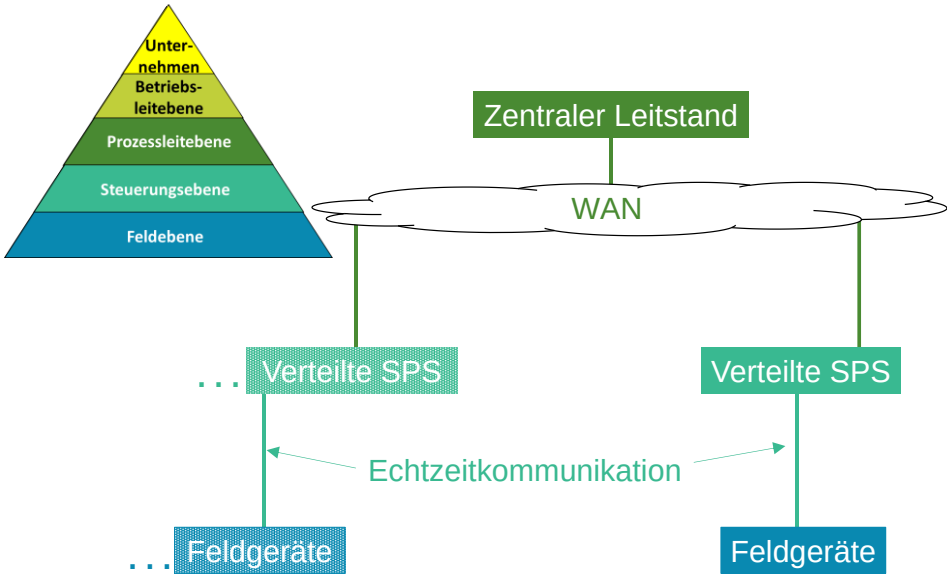


Abb. 3.2: Verteilte ICS-Netzstruktur

Lokale Steuergeräte sind in einem LAN mit dem lokalen Leitstand und untereinander verbunden (siehe Abb. 3.1) – die Struktur solcher Anlagen wird im Folgenden **konzentrierte ICS-Netzstruktur** genannt. Verteilte Steuergeräte sind durch ein WAN mit dem zentralen Leitstand und untereinander nicht verbunden (siehe Abb. 3.2) – dies entspricht der **verteilten ICS-Netzstruktur**.

Die lokale Architektur ist in Wasserwerken und Kläranlagen zu finden, die verteilte Architektur immer dann, wenn Klappen, Schieber Ventile und Pumpen in Rohrnetzen oder Kanalnetzen gesteuert werden müssen. Der Leitstand repräsentiert in beiden Fällen die Überwachungs- und Bedienfunktionen der Prozessleitebene. Für eine genauere Beschreibung der Anlagentechnik in der Wasserwirtschaft siehe Abschnitt 3.3.1; für eine genauere Beschreibung der automatisierungstechnischen Komponenten siehe Abschnitt 2.1.2. Es gibt zudem durchaus eine **Mischform** zwischen zentrierter und verteilter Netzstruktur; diese wird in Abschnitt 3.3.2 beleuchtet.

Abb. 3.1 und Abb. 3.2 zeigen deutlich, dass die Automatisierungstechnik in der Wasserwirtschaft nicht nur sehr homogen, sondern auch relativ einfach ist: Die wichtigsten Komponenten sind der Leitstand, von dem aus die SPSen überwacht und geführt werden, die Steuergeräte selbst und die Feldgeräte. Es wird **keine außergewöhnliche Geräte- oder Kommunikationstechnik** verwendet. Das ist für ein Pilotprofil, wie es in dieser Arbeit entsteht, eine wünschenswerte Eigenschaft. Auf diese Weise lenken weniger Branchenspezifika von der Adaptierbarkeit des Profils für andere Branchen ab.

3.3 Abgrenzung des Informationsverbunds

Die Eingrenzung der Referenzinstitution auf die Wasserwirtschaft legt eine Zielgruppe von Unternehmen fest. Für das IT-Grundschutz-Profil muss zusätzlich abgegrenzt werden, welche Geschäftsprozesse innerhalb dieser Unternehmen Gegenstand der Betrachtung sein sollen und welche technische Infrastruktur zur Erbringung dieser Geschäftsprozesse notwendig ist. Im IT-Grundschutz-Vokabular entspricht dies der Abgrenzung des *Informationsverbunds* (siehe Abschnitt 2.2).

3.3.1 Geschäftsprozesse

Wasser- und Abwassernetze stehen durch den Wasserkreislauf in direkter Abhängigkeit zueinander: Das gereinigte Abwasser dient als Rohwasser für die Trinkwasseraufbereitung, das benutzte Trinkwasser tritt in die Abwasserkanalisation ein. Aus diesem Grund (und wegen ihrer technischen Ähnlichkeit, wie in Abschnitt 3.2.2 beschrieben) werden im IT-Grundschutz-Profil die Wasserversorgung und Abwasserbeseitigung zusammengefasst.

3.3.1.1 Geschäftsprozesse und Anlagen

Die betrachteten Geschäftsprozesse und Anlagen orientieren sich an der Verordnung zur Bestimmung kritischer Infrastrukturen (BSI-KritisV, [KritisV16]). Die Abwasserbeseitigung umfasst die **Geschäftsprozesse** Siedlungsentwässerung sowie Abwasserbehandlung und Gewässereinleitung (Tab. 3.1). Bei der Wasserversorgung sind es Gewinnung, Aufbereitung und Verteilung (Tab. 3.2) [KritisV16].

Tab. 3.1: Geschäftsprozesse und Anlagen der Abwasserbeseitigung

Geschäftsprozess	**Siedlungsentwässerung**	**Abwasserbehandlung und Gewässereinleitung**
Anlage	**Kanalisation mit Leitstand**	**Kläranlage mit Leitstand**
ICS-Netzstruktur	verteilt	konzentriert
Anlagenbestandteile für Teilprozesse (potenziell Aktoren)		
Transport	Kanalnetz, Armaturen (Schieber, Ventile, Klappen)	Einlaufbauwerk, Versickerungsanlage
Förderung	Pumpen, Druckbehälter	Pumpen
Wasserstandskontrolle	Wehr, Speicherbecken bei Mischsystemen: Mischwasserüberlauf	
Mechanische Aufbereitung	Regenklärbecken	Mazerator, Filter, Rechen, Sieb, Sandfang, Fettabscheider
Biologische Aufbereitung		Belebungsbecken, Belüftung, Biofilmreaktor
Chemische Aufbereitung		Fällung, Flockung, Chlorung
Sensoren	Durchfluss, Druck, Füllstand, Konzentration	Durchfluss, Druck, Füllstand, Konzentration

Tab. 3.2: Geschäftsprozesse und Anlagen der Wasserversorgung

Geschäftsprozess	**Gewinnung**	**Aufbereitung**	**Verteilung**
Anlage	**Gewinnungsanlage (Wasserwerk) mit Leitstand**	**Aufbereitungsanlage (Wasserwerk) mit Leitstand**	**Wasserverteilungssystem mit Leitstand**
ICS-Netzstruktur	konzentriert	konzentriert	verteilt
Anlagenbestandteile für Teilprozesse (potenziell Aktoren)			
Gewinnung	aus Grundwasser: Brunnen, Sickerleitung, Sickerstollen aus Oberflächenwasser: Entnahmebauwerk aus Niederschlagswasser: Zisterne		
Mechanische Aufbereitung		Siebung, Sedimentation, Filtration	
Biologische und chemische Aufbereitung		Fällung, Flockung, Flotation, Begasung, Belüftung, Enthärtung, Chlorung	
Förderung	Pumpen, Druckbehälter	Pumpen, Förderschnecken, Überläufe	Pumpen, Druckbehälter
Speicherung	Durchlaufbehälter	Durchlaufbehälter	Hochbehälter, Tiefbehälter
Transport und Verteilung			Rohrnetz, Armaturen (Schieber, Ventile, Klappen)
Sensoren	Durchfluss, Druck, Füllstand	Durchfluss, Druck, Füllstand, Konzentration	Durchfluss, Druck, Füllstand

In Tab. 3.1 und Tab. 3.2 und werden den fünf berücksichtigten Geschäftsprozessen die dafür notwendigen Anlagen zugeordnet. Die **ICS-Netzstruktur** bezieht sich auf die in Abschnitt 3.2.2 erläuterten Unterschiede in der räumlichen Lage der SPSen: Bei verteilten Strukturen sind die Steuergeräte räumlich verteilt, bei konzentrierten Netzen sind die Steuergeräte im selben Gebäude- beziehungsweise Anlagenkomplex wie der Leitstand der Anlage.

Für die Geschäftsprozesse Siedlungsentwässerung und Verteilung sind Kanalnetze notwendig: Die Kanalisation bzw. das Wasserverteilungssystem, jeweils inklusive Leitstand. Beides sind also Anlagen mit verteilter ICS-Netzstruktur (*verteilte Anlagen*) gemäß Abb. 3.2. Größere Kanalbauwerke, etwa Pumpstationen, können durchaus einen lokalen Leitstand besitzen; in diesem Fall wird dem Bauwerk eine konzentrierte ICS-Netzstruktur gemäß Abb. 3.1 zugeordnet.

Für die Geschäftsprozesse Gewinnung, Aufbereitung und Abwasserbehandlung sind Gewinnungsanlagen, Aufbereitungsanlagen und Kläranlagen notwendig — allesamt mit konzentrierter ICS-Netzstruktur entsprechend Abb. 3.1. Als Wasserwerke werden Betriebseinheiten bezeichnet, „die aus Anlagen zur Gewinnung, Aufbereitung, Förderung und Speicherung von Wasser“ bestehen können [DIN4046]. Damit kann ein Wasserwerk alle Teilprozesse außer Transport und Verteilung beinhalten – in der Regel wird dafür eine konzentrierte ICS-Netzstruktur verwendet. Deswegen wird in dieser Arbeit der Begriff *Wasserwerk* übergreifend für die Anlagen mit konzentrierter ICS-Netzstruktur (*konzentrierte Anlagen*) in der Wasserversorgung gebraucht.

Bei der Abwasserbeseitigung gibt es noch einen weiteren Geschäftsprozess: die Klärschlammbehandlung. Klärschlamm fällt als Nebenprodukt der Abwasserbehandlung an. Eine Behandlung kann ihn besser verwertbar machen: Klärschlamm kann als Düngemittel oder zur Gewinnung von Wärme und Strom genutzt werden. Die Klärschlammbehandlung hat jedoch keinen direkten Einfluss auf die Verfügbarkeit der Dienstleistung Abwasserbeseitigung [BSI15]. In der BSI-Kritisverordnung wird sie bei der Auflistung der kritischen Geschäftsprozesse nicht berücksichtigt [KritisV16]. Dementsprechend findet sie auch in dem in dieser Arbeit erstellten IT-Grundschutz-Profil keine Beachtung.

3.3.1.2 Typische Anlagen, Aktoren und Sensoren

In Tab. 3.1 und Tab. 3.2 werden ergänzend Beispiele für typische **Anlagenbestandteile** aufgelistet. Diese Anlagenbestandteile sind für die genannten Geschäftsprozesse, manchmal jedoch auch nur für **Teilprozesse** davon zuständig. Je nach Digitalisierungsgrad der Anlage können viele dieser Anlagenbestandteile automatisiert gesteuert werden, sind also potenziell **Aktoren**. Auch typische **Sensoren** sind aufgelistet. Die Begrifflichkeiten für Teilprozesse sowie Anlagenbestandteile sind für die Wasserversorgung der Norm DIN 4046 sowie für die Abwasserbeseitigung den Normen DIN 4045 und DIN EN 16323 entnommen [DIN4046; DIN4045; DIN16323].

Es wird an dieser Stelle betont, dass die genannten Anlagenbestandteile keinen Anspruch auf Vollständigkeit erheben, sondern nur eine Vorstellung typischer von der Leit- und Automatisierungstechnik in der Wasserwirtschaft gesteuerten Anlagen vermitteln soll. Für genauere Beschreibungen der Anlagen wird auf die oben genannten Normen sowie auf die KRITIS-Sektorstudie des BSI verwiesen [BSI15].

Bei verteilten Netzen, also dem Wasserverteilungssystem für die Wasserversorgung und der Kanalisation für die Abwasserbeseitigung, sind die vorherrschenden Teilprozesse **Wassertransport und -verteilung sowie Wasserförderung**. Für die Förderung aus tiefer gelegenen Quellen sind Pumpen nötig, liegt die Quelle erhöht, reichen die Armaturen (Schieber, Ventile und Klappen) im Rohrnetz [BSI15]. Einlaufbauwerke leiten Wasser in Kanäle oder Kläranlagen ein, Versickerungsanlagen sind für die kontrollierte Versickerung in den Boden zuständig [DIN4045]. Sensoren können Durchfluss, Druck und / oder Füllstand des Wassers in den Rohren beziehungsweise Kanälen messen [BSI15].

Bei den Kanalnetzen der Abwasserbeseitigung kommt noch der Teilprozess der **Wasserstandskontrolle**, also unter anderem die Vermeidung von Überflutungen, hinzu. Dafür werden Wehre oder Speicherbecken verwendet [DIN16323].

Bei einem Mischsystem, das im Gegensatz zum Trennsystem Regen- und Abwasser in gemeinsamen Kanälen führt, ist eine Überflutung besonders schwerwiegend: Die betroffenen Gebiete würden dann nicht nur mit Regenwasser, sondern auch mit Mischwasser, bestehend aus Abwasser und Regenwasser, überflutet. Um das zu verhindern, sind bei Mischsystemen mehr Speicher- und Behandlungssysteme wie Mischwasserüberläufe notwendig. Auch zusätzliche Hochwasserpumpen können vorgesehen sein [BSI15].

In den Anlagen, die für die Wasserreinigung zuständig sind — Aufbereitungs- und Kläranlagen — ist neben der Förderung der wichtigste Teilprozess die **Wasseraufbereitung**. Die mechanische Aufbereitung sorgt beispielsweise mittels Mazeratoren (Zerkleinerern), Rechen, Sieben, Filtern, Fettabscheidern und Sandfängen für die Entfernung gröberen Schmutzes. Die biologische und chemische Reinigung eliminieren ungewünschte Zusatzstoffe im Wasser durch Belüftung und Beimischung biologischer oder chemischer Substanzen [MS11]. Für die biologische Aufbereitung werden Anlagen wie Belebungsbecken, Belüftungen, Biofilmreaktoren und für die chemische Aufbereitung Anlagen für Fällung oder Flockung (Absetzen oder Koagulation gelöster Wasserbestandteile durch Zugabe einer Chemikalie), Entgasung (Entfernung gelöster Gase), Enthärtung (Verminderung der Calcium-Ionenkonzentration) und Chlorung (Zugabe von Chlor) verwendet [DIN4045; DIN16323; DIN4046].

Dabei kommen in Aufbereitungsanlagen für Trinkwasser und Kläranlagen für Abwasser grundsätzlich dieselben Verfahren und damit ähnliche Anlagen zum Einsatz; lediglich die Intensität der nötigen Behandlung unterscheidet sich. Für die Förderung des Klärschlammes werden zusätzlich zu Pumpen Förderschnecken und Absaugvorrichtungen verwendet. Als Sensoren kommen zu Durchfluss-, Druck- und Füllstandsmessern noch Konzentrationssensoren hinzu [BSI15].

Für die **Wassergewinnung** werden unterschiedliche Anlagen verwendet, je nachdem, woher das Wasser gewonnen wird. Brunnen, Sickerleitungen und Sickerstollen können Grundwasser aus dem Boden holen, Entnahmebauwerke leiten Wasser aus Oberflächenwasser wie Seen, Flüssen oder Talsperren und Zisternen können Niederschlagswasser sammeln. Für die **Wasserspeicherung** zwischen Wasserwerken und Versorgungsgebieten werden Durchlaufbehälter verwendet; außerdem kommen im Wasserverteilungssystem zur Speicherung und Druckerhöhung Hochbehälter (z.B. Wassertürme) und zur Speicherung ohne Druckerhöhung Tiefbehälter zum Einsatz [DIN4046].

3.3.2 Abgrenzung des ICS-Netzes

Die grundlegende ICS-Netzstruktur mitsamt der Unterteilung in verteilte und konzentrierte ICS-Netze wurde in Abb. 3.1 und Abb. 3.2 bereits vorgestellt. Zusätzlich sind auch Mischformen dieser beiden Strukturtypen möglich: Etwa eine konzentrierte Anlage mit lokalem Leitstand, die zusätzlichen an einen entfernten, zentralen Leitstand angeschlossen ist. Um die Abgrenzung des Informationsverbunds an einem möglichst generischen Netz zu verdeutlichen, wird in Abb. 3.3 eine **gemischte ICS-Netzstruktur** vorgestellt, die im weiteren Verlauf der Arbeit die Grundlage für die Referenzarchitektur bildet.

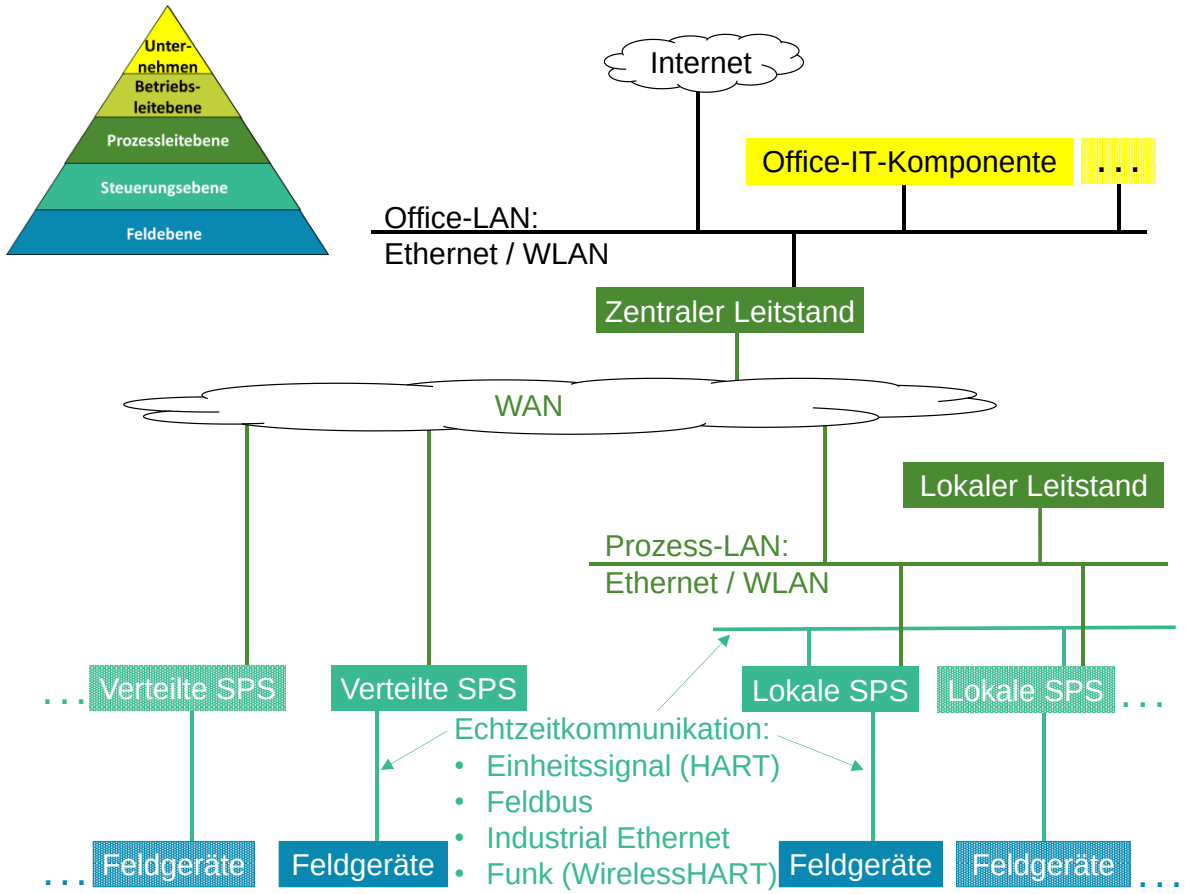


Abb. 3.3: Gemischte ICS-Netzstruktur

Die gemischte ICS-Netzstruktur setzt voraus, dass sowohl verteilte als auch lokale Anlagen vorhanden sind. Jede verteilte Anlage hat einen zentralen und jede konzentrierte Anlage einen lokalen Leitstand, in denen die Steuerungsprozesse auf den unteren Ebenen koordiniert und überwacht werden.

Der zentrale Leitstand steuert über ein WAN eine Vielzahl verteilter Anlagen mit ihren jeweiligen Steuergeräten – gegebenenfalls für eine ganze Region. Diese verteilte Struktur ist in der linken Hälfte der Abb. 3.3 dargestellt.

Die lokalen Leitstände steuern über ein LAN die Steuergeräte einer einzelnen konzentrierten Anlage. Um alle verteilten und konzentrierten Anlagen einer Region vom zentralen Leitstand aus im Blick zu behalten, können die konzentrierten Anlagen zusätzlich noch über das WAN an den zentralen Leitstand angebunden sein, wie in der rechten Hälfte von Abb. 3.3 zu sehen. Diese Verbindung muss aber nicht zwangsläufig bedeuten, dass die Anlagen vom zentralen Leitstand aus steuerbar sind; sie können auch lediglich Überwachungsdaten liefern. Die Daten helfen, ein vollständigeres Bild des Kanalnetzes zu erhalten, weil sie Informationen über die Schnittstellen der konzentrierten Anlagen zum Kanalnetz liefern, zum Beispiel: Wie viel Wasser nimmt die Kläranlage gerade auf?

In Abb. 3.3 stehen die Leitstände stellvertretend für die Funktionen von HMI, Engineering-Workstation und Historian (für eine Erläuterung dieser ICS-Komponenten siehe Abschnitt 2.1.2.1 oder Glossar und Abkürzungsverzeichnis). Im Leitstand werden somit SCADA- bzw. PLS-Funktionen umgesetzt, die zentrale Datenhaltung, zentrales Programmieren der SPSen und übergeordnete Prozesssteuerungen mit einer Sollwertführung der unterlagerten SPS ermöglichen [DWA11]. Die genannten Funktionen können physisch durchaus auf mehrere Geräte verteilt sein.

Der zentrale Leitstand befindet sich meist am Hauptsitz des Wasserversorgungs- oder Abwasserbeseitigungsdienstleisters. Dort werden außer der Überwachung des Kanalnetzes auch Verwaltungs- und Managementtätigkeiten ausgeführt, wie sie in der Automatisierungspyramide auf den oberen beiden Ebenen angesiedelt sind.

Dafür gibt es ein Office-Netz (in der Regel ein Ethernet-LAN oder WLAN), das ERP- und MES-Software und einen Internetanschluss, aber auch normale Bürogeräte wie Server, Rechner für Mitarbeiter und Drucker beinhaltet. In dieser Arbeit werden diese Komponenten unter dem Begriff *Office-IT-Komponenten* zusammengefasst. Wenn eine Verbindung des Office-LAN zum Prozess-LAN des Leitstands besteht, kann die IT-Sicherheit der Office-IT-Komponenten einen Einfluss auf die Informationssicherheit der Geschäftsprozesse in der Wasserwirtschaft haben [DWA07].

Die ICS-Netzstruktur in Abb. 3.3 stellt den grundlegenden Aufbau der technischen Infrastruktur für die betrachteten Geschäftsprozesse des in dieser Arbeit erstellten IT-Grundschutz-Profils dar. Gemeinsam mit den näheren Beschreibungen der Anlagen und Steuereinheiten in Abschnitt 3.3.1 bildet sie den *Informationsverbund*, dessen Festlegung in den IT-Grundschutz-Standards (siehe Kapitel 2.2) gefordert wird.

Für die zum Informationsverbund gehörigen Geschäftsprozesse und wasserwirtschaftlichen Anlagen erfolgt im folgenden Abschnitt noch die Schutzbedarfsfeststellung, bevor in Kapitel 4 der Informationsverbund um Netztechnik, Software und Variationsmöglichkeiten ergänzt wird.

3.4 Schutzbedarf der Geschäftsprozesse und Anlagen

Die Schutzbedarfsfeststellung für die Wasserwirtschaft erfolgt nach BSI-Standard 200-2 (Standard-Absicherung, Kapitel 8.2) in mehreren Schritten [BSI17b]. Im ersten Schritt wird der Schutzbedarf für die berücksichtigten Geschäftsprozesse und die dazugehörigen Anlagen festgelegt. Dies geschieht in Abschnitt 3.4.2 dieses Kapitels.

Der Schutzbedarf für einzelne Zielobjekte kann vom Schutzbedarf der Gesamtanlage abweichen. Diese Problematik wird in einem späteren Kapitel (Abschnitt 6.1) behandelt.

Bevor Schutzbedarfe den einzelnen Geschäftsprozessen und Zielobjekten zugeordnet werden können, müssen zunächst geeignete Kriterien für die Zuweisung festgelegt werden. Dies erfolgt im folgenden Abschnitt 3.4.1.

3.4.1 Festlegung der Schutzbedarfskategorien

Die Kategorien für den Schutzbedarf orientieren sich ebenfalls an BSI-Standard 200-2; jedoch werden einige Anpassungen für die Wasserwirtschaft vorgenommen.

Im Standard 200-2 sind drei Schutzbedarfskategorien vorgesehen [BSI17b]:

- **Normal**: Die Schadensauswirkungen sind begrenzt und überschaubar.
- **Hoch**: Die Schadensauswirkungen können beträchtlich sein.
- **Sehr hoch**: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Für die Einschätzung der Schadensauswirkungen schlägt der Standard 200-2 sechs Schadenskategorien vor [BSI17b]:

1. **Verstoß gegen Gesetze / Vorschriften / Verträge**,
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts,
3. Beeinträchtigung der persönlichen Unversehrtheit,
4. **Beeinträchtigung der Aufgabenerfüllung,**
5. negative Innen- oder Außenwirkung und
6. finanzielle Auswirkungen.

In dieser Arbeit wird die Wasserwirtschaft in ihrer Funktion als potenziell kritische Infrastruktur betrachtet. Die Betrachtung der Schadenskategorien für die Wasserwirtschaft wird deswegen auf zwei Kategorien beschränkt: Kategorie 1: Verstoß gegen Gesetze / Vorschriften / Verträge und Kategorie 4: Beeinträchtigung der Aufgabenerfüllung.

Die Kategorie „Verstoß gegen Gesetze / Vorschriften / Verträge“ ist für die Wasserwirtschaft deswegen relevant, weil für Wasserversorger und Abwasserbeseitiger ab einer bestimmten

Größe als Betreiber kritischer Infrastrukturen das IT-Sicherheitsgesetz [IT-SiG15] gilt (siehe Abschnitt 3.1.2.3).

Im Rahmen des Gesetzes müssen Betreiber nun mit Bußgeldern von bis zu 50.000 € rechnen, falls sie Störungen nicht melden, Kontaktstellen nicht benennen, Auditergebnisse nicht an das BSI übermitteln oder keine angemessenen Sicherheitsvorkehrungen treffen und mit einer Buße von bis zu 100.000 €, wenn sie vom BSI angemahnte Sicherheitsmängel nicht beseitigen.

Die Bußgelder sind jedoch für einen durchschnittlichen Betreiber als eher geringfügige Konsequenzen einzustufen, wenn man Zahlen des Statistischen Bundesamt zu Grunde legt. Es wurden unter anderem Beschäftigtenzahlen, Umsätze und Nettowertschöpfungen von Unternehmen aus der Wasserwirtschaft mit mindestens 20 Mitarbeitern erhoben [Destatis17b]. Die durchschnittlichen jährlichen Nettowertschöpfungen pro Betrieb betrugen 2014 etwa 6,1 Mio. € in der Wasserversorgung sowie etwa 11,7 Mio. € in der Abwasserbeseitigung. Bei durchschnittlich 80 Mitarbeitern bei Betrieben der Wasserversorgung beziehungsweise 119 Mitarbeitern bei Betrieben der Abwasserbeseitigung ist das maximale Bußgeld von 100.000€ etwa das Äquivalent der Nettowertschöpfung von etwas mehr als einem Mitarbeiter oder etwa 0,9 % bis 1,6 % der gesamten Nettowertschöpfung [Destatis17b].

Obwohl die Schadensauswirkungen objektiv gesehen und im Durchschnitt betrachtet eher gering sind, hat das IT-Sicherheitsgesetz das Bewusstsein der Anlagenbetreiber für die Notwendigkeit eines Informationssicherheitskonzepts entscheidend geschärft. Beispielsweise führte es zu der Erarbeitung des branchenspezifischen Sicherheitsstandards Wasser / Abwasser (B3S WA), auf dem auch Teile der vorliegenden Arbeit basieren. In dieser Arbeit soll jedoch für die Festlegung der Schutzbedarfskategorien das Hauptaugenmerk auf die objektiv gesehen größten Auswirkungen gelegt werden – und diese sind in der Schadenskategorie 4: Beeinträchtigung der Aufgabenerfüllung zu erwarten.

Zur Begründung wird noch einmal an die Definition einer kritischen Infrastruktur aus Abschnitt 3.1.2.3 erinnert: Kritische Infrastrukturen sind demnach „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, **bei deren Ausfall oder Beeinträchtigung** [Hervorhebung der Verfasserin] nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden" [BMI09].

Während also andere Schadenskategorien durchaus kleinere Schäden nach sich ziehen können, sind objektiv gesehen die höchsten Schäden bei **Beeinträchtigung der Aufgabenerfüllung** zu erwarten. Da für die Schutzbedarfskategorie immer der höchste zu erwartende Schaden die Kategorie festlegt („Maximumsprinzip", [BSI17b]), ist diese Beschränkung zielführend.

Sind in einer weiteren Kategorie (beispielsweise Beeinträchtigung der persönlichen Unversehrtheit oder Verstoß gegen Gesetze / Vorschriften / Verträge) dennoch hohe Schäden zu erwarten, so sind diese in der Wasserwirtschaft in der Regel als Folge einer Beeinträchtigung der Aufgabenerfüllung zu werten und somit durch die Betrachtung dieser Kategorie schon ab-

gedeckt. Beispiele sind hygienische Beeinträchtigungen durch einen längeren Ausfall der Abwasserbeseitigung oder ein Verstoß gegen Gesetze für die Trinkwasserqualität durch einen Ausfall einer Aufbereitungsanlage.

Ein weiterer Grund für die Beschränkung auf die Schadenskategorie „Beeinträchtigung der Aufgabenerfüllung“ ist die Schwerpunktsetzung dieser Arbeit auf die OT bzw. ICS. Bei diesen Systemen hat die Verfügbarkeit einen sehr viel höheren Stellenwert als etwa Vertraulichkeit von Daten. Auch werden in den Datenbanken des Leitsystems in der Regel keine personenbezogenen Daten gespeichert und verarbeitet [DWA11], sodass etwa eine Beeinträchtigung des informationellen Selbstbestimmungsrechts zwar für die gesamte Wasserwirtschaft eine Rolle spielen mag, für den Fokus dieser Arbeit jedoch nicht.

Für die Schadenskategorie „Beeinträchtigung der Aufgabenerfüllung“ definiert der BSI-Standard 200-2 die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ wie in Tab. 3.3 dargestellt [BSI17b].

Tab. 3.3: Definitionen von Schutzbedarfskategorien

Schutzbedarfs-kategorie	"Normal"	"Hoch"	"Sehr hoch"
Allgemeine Definition (BSI-Standard 200-2)	Die Schadensauswirkungen sind **begrenzt und überschaubar**.	Die Schadensauswirkungen können **beträchtlich** sein.	Die Schadensauswirkungen können ein **existenziell bedrohliches, katastrophales** Ausmaß erreichen.
Definition für die Schadenskategorie: „Verstoß gegen Gesetze / Vorschriften / Verträge“	Verstöße gegen Vorschriften und Gesetze mit **geringfügigen Konsequenzen**.	Verstöße gegen Vorschriften und Gesetze mit **erheblichen Konsequenzen**.	**Fundamentaler** Verstoß gegen Vorschriften und Gesetze.
Definition für die Schadenskategorie „Beeinträchtigung der Aufgabenerfüllung“ (BSI-Standard 200-2)	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt **zwischen 24 und 72 Stunden**.	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt **zwischen einer und 24 Stunden**.	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit ist **kleiner als eine Stunde**.
Ergänzung der Definition für die Wasserwirtschaft (BSI-KritisV)	Es sind **weniger als 500 000 Personen** betroffen (fällt nicht unter KRITIS).	Es sind **mindestens 500 000 Personen** betroffen (fällt unter KRITIS).	

Für die Beeinträchtigung der Aufgabenerfüllung wird tolerierbare Dauer der Beeinträchtigung als Kriterium für die Einstufung in Schutzbedarfskategorien herangezogen. Der Übersicht halber sind auch die Schutzbedarfskategorien für die Schadenskategorie „Verstoß gegen Gesetze / Vorschriften / Verträge“ noch einmal aufgeführt. Dabei wird deutlich, dass die erreichte Schutzbedarfskategorie dabei in der Regel geringer ausfallen dürfte als für die Schadenskategorie „Beeinträchtigung der Aufgabenerfüllung“ [BSI17b].

Diese BSI-Definitionen können und sollen durch einzelne Institutionen ihren Bedürfnissen entsprechend angepasst werden. Für die Wasserwirtschaft wird als zweites wichtiges Kriterium für die Einstufung von Schutzbedarfen und Schadensausmaßen stets die Anzahl betroffener Personen herangezogen:

In der BSI-KritisV werden kritische Infrastrukturen in der Wasserwirtschaft als solche definiert, die mindestens 500 000 Personen versorgen (auch der Schwellenwert für Trinkwasseranlagen von 22 Mio. m³ Wasseraufkommen/Jahr basiert auf der Annahme von 500 000 versorgten Personen und einem Durchschnittsverbrauch von 44 m³ pro Person und Jahr) [KritisV16] .

Auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) schlägt für die Bestimmung von Schadensmaßen in der Trinkwasserversorgung eine Beurteilung anhand der Ausfalldauer und der Anzahl betroffener Personen vor: Das Schadensausmaß bei einer Ausfallzeit zwischen 24 und 72 Stunden ist demnach als „mäßig“ einzustufen, wenn weniger als 20 000 Personen betroffen sind; bei mehr als 20 000 Personen hingegen als „hoch“ [BBK16].

Die Anzahl der betroffenen Personen soll auch in dieser Arbeit als ein Kriterium für den Schutzbedarf herangezogen werden. Das BBK rät, die genauen Schwellenwerte betroffener Personen und möglicher Ausfallzeiten für den Einzelfall festzulegen. Das kann innerhalb dieser Arbeit, die ja eine Richtlinie für eine gesamte Branche liefern soll, nicht geleistet werden. Es wird deswegen den Einschätzungen der BSI-KritisV gefolgt, indem der Personen-Schwellenwert für die Schutzbedarfskategorie „hoch“ auf mindestens 500 000 betroffene Personen gesetzt wird. Bei einer Modifikation der BSI-KritisV sollten die Änderungen (z.B. dieser Schwellenwert) berücksichtigt werden.

Die Orientierung der Schutzbedarfskategorien an den Schwellenwerten der BSI-KritisV ist ein großer Vorteil für die Nutzerfreundlichkeit des IT-Grundschutz-Profils: Die Anwender können auf diese Weise einen Wert für die Schutzbedarfszuordnung ihrer eigenen Anlagen nutzen, den sie aufgrund des IT-SiG ohnehin erheben müssen.

Da eine Ausfallzeit unter einer Stunde im Wassersektor auch bei einer großen betroffenen Personenzahl kein wesentliches Schadensausmaß hervorruft (das BBK etwa berücksichtigt diese Zeitspanne nicht einmal, s. [BBK16]), werden die Schutzbedarfskategorien „hoch“ und „sehr hoch“ in dieser Arbeit zur Schutzbedarfskategorie „hoch“ zusammengefasst.

Tab. 3.3 liefert eine Übersicht über die in dieser Arbeit verwendeten Kategorien, Kriterien und Schwellenwerte. Die Kriterien für die Schutzbedarfskategorie „sehr hoch“ sind darin ausgegraut, da sie nicht verwendet werden.

Die Unterscheidung zwischen dem Schutzbedarf „normal“ und „hoch“ ist wichtig, da für Zielobjekte mit normalem Schutzbedarf die Standardanforderungen aus den IT-Grundschutz-Bausteinen als ausreichend erachtet werden, während für Zielobjekte mit mindestens hohem Schutzbedarf eine ergänzende Sicherheitsanalyse und gegebenenfalls zusätzliche Anforderungen notwendig sind [BSI17b].

Die verwendeten Schutzbedarfskategorien und ihre Definitionen sind kompatibel zu dem Vorgehen des Branchenspezifischen Sicherheitsstandards Wasser / Abwasser (B3S WA), da auch dort unterschiedliche Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe vorgesehen sind – und zwar ebenfalls abhängig davon, ob Anlagen unter die KRITIS-Definition (Schwellenwert: 500 000 betroffene Personen) fallen oder nicht [B3S17b; B3S17a].

3.4.2 Schutzbedarfsfeststellung

Die betrachteten Geschäftsprozesse sind, wie in Abschnitt 3.3.1 festgelegt,

- Für die Trinkwasserversorgung:
  - Gewinnung,
  - Aufbereitung,
  - Verteilung;
- Für die Abwasserbeseitigung:
  - Siedlungsentwässerung,
  - Abwasserbehandlung und Gewässereinleitung.

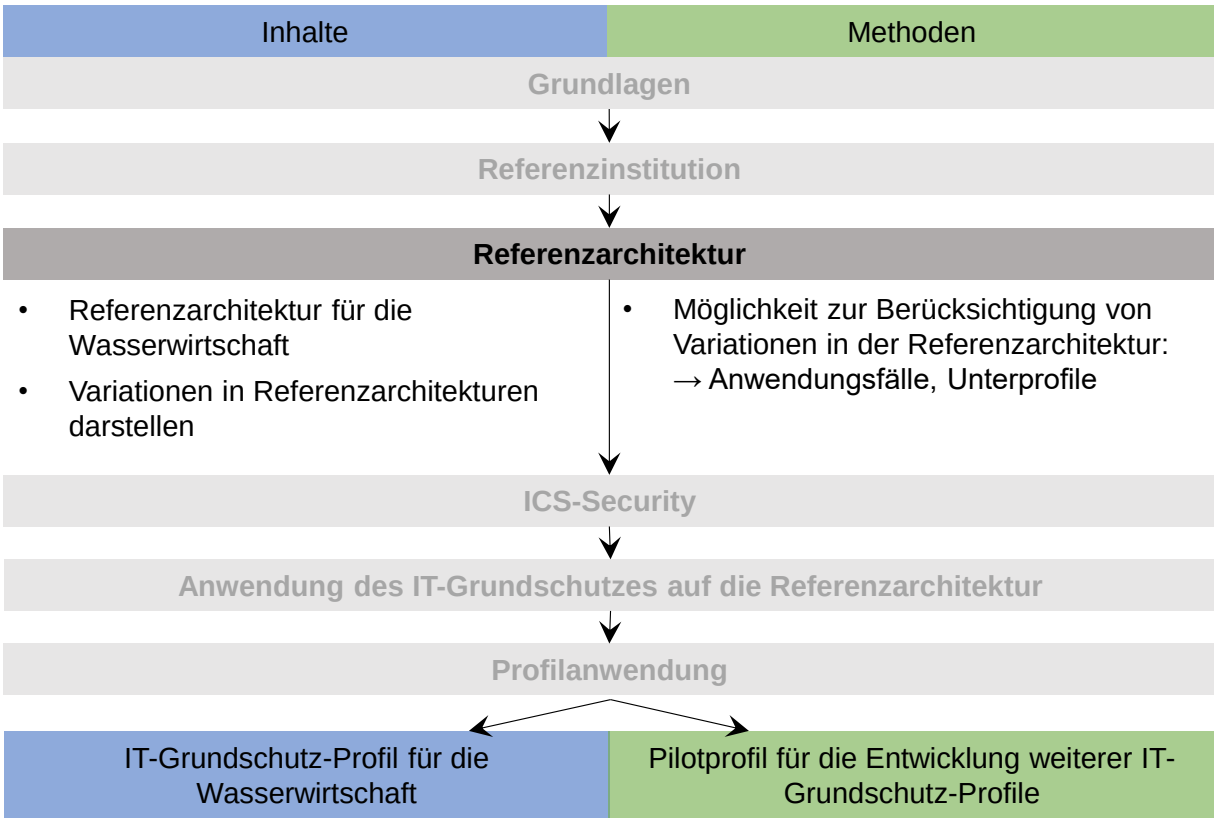
Da der Schutzbedarf wie in Abschnitt 3.4.1 definiert vor allem von der Anzahl Personen abhängt, die von einem Geschäftsprozess versorgt werden, kann an dieser Stelle keine pauschale Unterscheidung von Schutzbedarfen für verschiedene Geschäftsprozesse gemacht werden.

Dasselbe gilt für die Anlagen, die den Geschäftsprozessen zugeordnet werden. Diese sind nach Abschnitt 3.3.1

- Für die Trinkwasserversorgung:
  - Gewinnungsanlagen (Wasserwerke) mit Leitstand,
  - Aufbereitungsanlagen (Wasserwerke) mit Leitstand,
  - Wasserverteilungssysteme mit Leitstand;
- Für die Abwasserbeseitigung:
  - Kanalisation mit Leitstand,
  - Kläranlagen mit Leitstand.

Jedoch ist es für Anlagenbetreiber verhältnismäßig einfach, den Schutzbedarf ihrer Anlagen im Einzelfall festzustellen, da dieser sich mit der Zuordnung zu kritischen Infrastrukturen nach BSI-KritisV deckt (siehe Abschnitt 3.4.1).

4 Referenzarchitektur



Die Referenzarchitektur legt den Grundstein für ein IT-Grundschutz-Profil, da auf ihrer Basis die Schutzbedarfsfeststellung, Modellierung und Risikoanalyse erfolgt. Sie besteht aus

- einer **Zielobjektliste**,
- **Netzplänen** zur grafischen Darstellung der Zielobjektkonfigurationen und -verbindungen:
    - Physischer Netzplan zur Veranschaulichung der physischen Infrastruktur,
    - Logischer Netzplan zur Veranschaulichung des logischen Datenflusses.

Die IT-Infrastruktur in Abb. 3.3 bietet eine gute Grundlage für die Referenzarchitektur; jedoch bedürfen einige technische Gegebenheiten noch der Konkretisierung:

- Die Erläuterungen zur LAN-Technik für allgemeine ICS-Netze in Abschnitt 2.1.2 sollen in Abschnitt 4.1 speziell für die Wasserwirtschaft ergänzt werden.
- Die WAN-Technik ist bislang nur als allgemeiner Begriff behandelt worden und bedarf einer Konkretisierung. Dies geschieht in Abschnitt 4.2.
- Ein möglicher Fernzugriff bzw. der Einsatz mobiler Geräte wurde bislang nicht berücksichtigt. Diesbezüglich schafft Abschnitt 4.3 Abhilfe.
- Die notwendigen Software-Anwendungen für den ICS-Prozess werden in Abschnitt 4.4 erläutert.

In Abschnitt 4.5 wird zunächst eine **generische Referenzarchitektur** gegeben, die möglichst alle für die Wasserwirtschaft relevanten Zielobjekte sowie möglichst umfangreiche Netzpläne enthält.

Die Erstellung einer generischen Zielobjektliste stellt kein Problem dar – darin werden alle möglicherweise relevanten Zielobjekte aufgelistet. Bei der Anwendung auf eine konkrete Institution können nicht zutreffende Zielobjekte einfach herausgestrichen werden.

Schwieriger gestaltet sich die Erstellung eines generischen Netzplans, der die Konfiguration der Zielobjekte und die Verbindungen zwischen ihnen verdeutlichen soll. Hier gibt es keine „allgemeinste“ Form, da sich die Variationen oft gegenseitig ausschließen. Dies kommt beispielsweise bei der gemeinsamen LAN-Nutzung vor: ICS-Komponenten können sich das LAN *entweder* mit Office-Komponenten teilen, *oder* es gibt ein dediziertes ICS-LAN. Folglich muss in solchen Fällen in den generischen Netzplänen eine Entscheidung für eine Konfiguration getroffen werden. Die generischen Netzpläne sollen deswegen lediglich veranschaulichen, wie eine generische Konfiguration des gesamten ICS-Netzes aussehen könnte und an welchen Stellen Variationen möglich sind.

Die generische Referenzarchitektur hat folglich noch zu viele Freiheitsgrade, um ein für konkrete, reale Institutionen hilfreiches Profil daraus zu machen. Um konkretere Referenzarchitekturen für die Profilerstellung zu erhalten, werden in Abschnitt 4.6 Konfigurationsmöglichkeiten anhand von spezifischen **Anwendungsfälle**n dargestellt. Die resultierenden **spezifischen Referenzarchitekturen** haben gegenüber der generischen Referenzarchitektur eine eingeschränkte Liste von Zielobjekten sowie Netzpläne, in denen im Gegensatz zum generischen Netzplan nicht das *gesamte* ICS-Netz, sondern nur die für den Anwendungsfall relevanten Komponenten abgebildet sind. Diese spezifischen Netzpläne basieren auf den generischen Netzplänen, sind jedoch auf einen ausgewählten Aspekt reduziert und zeigen dessen Variationsmöglichkeiten.

Damit sind am Ende dieses Kapitels alle Voraussetzungen für eine Modellierung spezifischer Referenzarchitekturen mit IT-Grundschutz-Bausteinen erfüllt.

Wie auch schon in Kapitel 3 war die Autorin für Branchenkenntnisse der Wasserwirtschaft neben den Informationen aus Fachliteratur, Regelwerken und Normen auf Branchenexperten angewiesen. Die wenigen technischen und organisatorischen Informationen, die nicht anderweitig belegt werden konnten, stammen aus Gesprächen mit diesen Fachleuten der Wasserwirtschaft.

4.1 LAN-Technik

Der in Abschnitt 2.1.2.2 erwähnte Trend hin zu Verwendung ethernetbasierter Feldbussysteme in der Automatisierungstechnik betrifft auch die Local Area Networks (LANs) der Wasserwirtschaft. Als prozesstechnische Branche mit hohen Anforderungen an die Zuverlässigkeit der Anlagen und langen Anlagenlebenszyklen (siehe Abschnitt 3.2.1) werden Entscheidungen über den Einsatz neuer Technologien jedoch vergleichsweise konservativ getroffen [DWA11].

Aus diesem Grund sind in der Wasserwirtschaft auch analoge Einheitssignale noch im Einsatz. Es werden aber zunehmend proprietäre Feldbusse und auch Feldbussysteme auf Industrial-Ethernet-Basis sowie Funktechniken für die Echtzeitkommunikation verwendet. Auch gemischte Systeme aus klassischen und ethernetbasierten Feldbussen sind möglich; in diesem Fall repräsentieren Proxies die nicht vorhandene Ethernet-Schnittstelle der klassischen Feldbusgeräte [DWA11].

Ist die Datenübertragung nicht echtzeitkritisch, wird auf gewöhnliche Ethernet-LANs zurückgegriffen. Auch Funktechniken, etwa auf Basis des 2,4-GHz-ISM-Bands (darunter fällt auch WLAN), werden für die LAN-Kommunikation verwendet [DWA11].

Um ein LAN zu bilden, ist ein **Switch** notwendig, mit dem alle LAN-Teilnehmer verbunden werden. Für die rauen Einsatzbedingungen in Anlagen der Wasserwirtschaft sind die robusteren Industrial-Ethernet-Switches geeignet [DWA11].

Darüber hinaus bilden **Router** die Schnittstelle vom LAN zum WAN.

4.2 WAN-Technik

Sowohl für verteilte Steuereinheiten in Kanalnetzen als auch für die Kommunikation mehrerer Anlagen mit einem zentralen Leitstand ist die Nutzung eines Wide Area Networks (WAN) unvermeidlich. In der Wasserwirtschaft wird dafür auch häufig der Begriff *Fernwirktechnik* verwendet.

Im Allgemeinen sind für die WAN-Kommunikation keine Kabelverbindungen verfügbar, sodass auf die Dienste von Service Providern zurückgegriffen wird. Auch für Funkverbindungen lohnt sich der Betrieb eines von Service Providern unabhängigen Systems in der Regel nicht, da die eigene Sicherung von Übertragungssicherheit, Verfügbarkeit und Reichweite in der Regel teurer ist als die Inanspruchnahme eines Providers [DWA07].

Tab. 4.1 gibt einen Überblick über WAN-Kommunikationstechniken und ihre Eigenschaften.

Als Übertragungsmedium kann zwischen Kabel- und Funkübertragung unterschieden werden.

Kabelübertragung bedeutet bei der Nutzung eines Service Providers die Nutzung eines öffentlichen (Telefon-)Netzes, etwa Kupferleitungs- oder Glasfasernetze. Telefonverbindungen sind ursprünglich Wählverbindungen, es besteht also keine dauerhafte Verbindung zwischen den Kommunikationsteilnehmern. Wenn Daten anfallen, müssen sie deswegen zwischengespeichert werden, bis sie gesendet werden können. Dieses Problem kann man mit der Anmietung einer analogen oder digitalen (ISDN, VoIP) Standleitung umgehen [Bau09]. Auch das Vorhalten eigener Standleitungen ist möglich.

Bei der Funkübertragung gibt es grundsätzlich drei Möglichkeiten. Die erste Möglichkeit ist die Nutzung der öffentlichen, von Netzbetreibern betriebenen Mobilfunknetze (GSM / GPRS, UMTS, LTE). Durch die immer bessere Mobilfunkabdeckung wird sie zunehmend populär [Bau09].

Die zweite Möglichkeit ist die Beantragung von Funkfrequenzen bei der Bundesnetzagentur. Das ist für verschiedene Frequenzbereiche möglich, darunter fallen der Tetrafunk, Fernwirkfunk oder bestimmte Frequenzen des Richtfunks [BNetzA17b; BNetzA17c; Bau09]. Teilweise werden die zugeteilten Frequenzen mit der Zeitschlitztechnik auf mehrere Nutzer aufgeteilt, sodass jeder Nutzer pro Minute eine feste Sekundenzahl lang senden kann [Bau09].

Die dritte Möglichkeit ist die Nutzung lizenzfreier Funkfrequenzen, sogenannter Allgemeinzuteilungen. Darunter fallen die ISM-Frequenzbänder (ISM steht für Industrial, Scientific and Medical), bestimmte Richtfunkfrequenzen sowie die WLAN-Frequenzen 2.4 GHz und 5 GHz [BNetzA17a].

Die Datenübertragung mittels Mobilfunkdiensten, aber auch die über das Telefonnetz oder ähnliche Leitungsnetze, macht zunehmend Gebrauch vom Internet Protocol (IP). Das Protokoll hat sich durch den Erfolg des Internets als Quasi-Standard etabliert. Damit ersetzt es zunehmend die teilweise standardisierten Protokolle der Normenreihe IEC 60870-5 sowie eine Fülle von herstellspezifischen (proprietären) Protokollen, die zuvor für die Fernwirktechnik in der Wasserwirtschaft verwendet worden sind [DWA07].

Tab. 4.1: WAN-Kommunikationstechniken für die Fern-Datenübertragung in der Wasserwirtschaft

WAN-Technik zur Datenübertragung	
Übertragungsmedium	
Kabel (elektrisch/optisch)	Telefonnetz (analog, ISDN, DSL) Standleitung (gemietet oder eigen)
Funk (elektromagnetisch)	Netzbetreiber-Lizenz: Mobilfunk (GPRS, UMTS, LTE) Private Lizenz: Zeitschlitzfunk, Tetrafunk, Fernwirkfunk, Richtfunk Ohne Lizenz (Allgemeinzuteilung): ISM-Band, Richtfunk, WLAN-Frequenzen
WAN-Schnittstelle im LAN	
immer außer ISDN	Modem
für IP-Technik zusätzlich	Router, ggf. Webserver
Verfügbarkeit	
Wählverbindung	keine dauerhafte Verbindung, deswegen Vorverarbeitung und Zwischenspeicherung der Daten in den verteilten Standorten nötig
Standleitung / DSL / Mobilfunk	Verbindung immer verfügbar, Daten können direkt übertragen werden, wenn sie entstehen
Sicherheit	
Ohne Nutzung von Internetdiensten	Verbindungen sind nur durch physisches Eingreifen ins WAN-Übertragungsmedium vor Ort zugänglich
WAN-Datenübertragung über Internetdienste	Verbindung theoretisch von überall in der Welt zugänglich; Einsatz von Firewalls und VPN ratsam

Bei der Verwendung von IP über einen DSL-Anschluss oder Mobilfunk sind Standleitungen auf den ersten Blick nicht mehr notwendig: Der Internetanschluss besteht ohnehin dauerhaft; Daten werden in Pakete aufgeteilt und können jederzeit gesendet werden. Da mittlerweile viele Hersteller von Automatisierungstechnik ihre Geräte IP-fähig gemacht haben, vereinfacht sich auch die – bei proprietären Protokollen aufwendige – Integration von Geräten verschiedener Hersteller [DWA07]. Trotzdem kann eine Standleitung sinnvoll sein, wenn Betreiber nicht auf die höhere Verfügbarkeit einer exklusiv genutzten Standleitung verzichten können oder wollen.

Die Verwendung von IP hat jedoch auch einen Nachteil: In der Regel geht damit die Anbindung ans Internet einher. Während WAN-Technik ohne Internetanbindung zumindest eine räumliche Nähe zu einer WAN-Leitung erfordert, um sie abzuhören, ist das Internet von überall in der Welt zugänglich – physische Nähe ist nicht länger notwendig. Die Verwendung von IP macht damit zusätzliche Sicherheitsmaßnahmen wie Firewalls und verschlüsselte VPN (Virtual Private Network)-Verbindungen empfehlenswert [Bau09].

Welche WAN-Technik verwendet wird, hat einen direkten Einfluss auf die WAN-Schnittstelle, die im LAN eingesetzt wird.

Für jede Art von WAN-Technik (außer ISDN, da Daten hier digital über die Telefonleitungen übertragen werden), ist ein **Modem** nötig. Modems übersetzen die digitalen Signale eines Computers, Sensors oder einer PLC so, dass sie über die WAN-Übertragungsmedien Funk, elektrische Leiter oder Lichtleiter übertragen werden können.

Bei der Verwendung von IP kann zudem das Betreiben eines **Webservers** sinnvoll sein, wenn auf ein HMI zugegriffen werden soll – die Prozessdaten dorthin kopiert werden, sodass sie eingesehen werden können, aber keinen Zugriff auf den Prozess erlauben [DWA11]. In jedem Fall wird ein **Router** benötigt, der für die Verbindung des LAN zum WAN sorgt. Als Sicherheitskomponenten können eine **Firewall** und für das VPN ein **VPN-Router, VPN-Gateway oder VPN-Server** im Einsatz sein. Detailliertere Informationen zu den genannten Sicherheitskomponenten liefert Kapitel 5.

4.3 Fernzugriff und mobile Geräte

Der Zugriff auf das ICS-Netz ist nicht nur für interne Geräte möglich, die fest zum ICS-Netz gehören.

Zum einen kann die WAN-Verbindung nicht nur für die Verbindung des Leitstands mit den verteilten Komponenten genutzt werden – auch externe Geräte können über diese Verbindung mit ICS-Komponenten wie Sensoren, Aktoren, Steuergeräten oder Leitständen des ICS-Netzes kommunizieren. Dies kann zum Beispiel im Rahmen einer Fernwartung sinnvoll sein [DWA07].

Zum anderen kann der Zugriff auf ICS-Komponenten vor Ort mittels mobiler Geräte wie Laptops, Tablets oder Mobiltelefonen beziehungsweise Smartphones erfolgen. Mobile Geräte ermöglichen dem Betriebs- und Wartungspersonal den Zugriff auf ICS-Komponenten mit einem einzigen Gerät, das sie zu jeder verteilten Komponente mitnehmen können. Der Zugriff kann

sinnvoll sein, etwa um Gerätedaten auszulesen, Grafiken und Werte des Leitstands mobil verfügbar zu haben, und Störmeldungen zu erhalten [DWA07].

4.4 Anwendungen

Nicht nur die Geräte- und Kommunikationstechnik gehören zur Referenzarchitektur – auch Software zählt dazu. Hier soll der Fokus auf Anwendungen liegen, die in der Wasserwirtschaft in Zusammenhang mit der ICS-Infrastruktur genutzt werden. Sie lassen sich nach ihren Aufgaben gliedern:

Datenhaltung und Datenaustausch:

- Für die Datenhaltung ist der Historian zuständig. Hardwareseitig besteht er aus RAID-Systemen, externe Festplatten oder netzwerkgekoppelte Festplatten (NAS) [DWA11].
- Softwareseitig werden die Daten durch Datenbanken mit den zugehörigen Abfrage- und Suchfunktionen verwaltet, beispielsweise **SQL** (Structured Query Language). Als Programmierschnittstelle ist **ODBC** (Open Database Connectivity) verbreitet [DWA11].
- Als Dateiformat für den Export von Archivdaten oder Messdaten aus den Datenbanken, zum Beispiel für Managementsysteme im Office-Netz, empfiehlt das DWA-Merkblatt M 253 für die Wasserwirtschaft nicht die Nutzung von der weit verbreiteten Datenformate CSV oder ASCII, sondern das **XML** (Extensible Markup Language)-Format [DWA11].
- Wenn ein IP-basiertes Automatisierungsnetz (Industrial Ethernet) besteht, können **Webdienste** für die Datenübermittlung genutzt werden [AWWA14]. Dafür hat sich das Protokoll **SOAP** (Simple Object Access Protocol) etabliert, das auf übliche Web-Anwendungsprotokolle wie **HTTP** (Hypertext Transfer Protocol), **SMTP** (Simple Mail Transfer Protocol) oder **FTP** (File Transfer Protocol) aufsetzt [EM07].
- Gerade für das automatische Versenden von Nachrichten, beispielsweise Alarmen, können auch **SMS** verwendet werden [AWWA14].
- Für die Datenübermittlung zwischen Geräten unterschiedlicher Hersteller mit unterschiedlichen Protokollen hat sich der Standard **OPC** (Open Platform Communications) durchgesetzt [DWA07]. Für Kommunikation innerhalb des industriellen Netzes (zwischen dezentralen Stationen und Leitstand) empfiehlt das DWA-Merkblatt M 253 für die Wasserwirtschaft das windowsbasierte OPC HDA, für den Datenaustausch mit Managementsystemen das plattformunabhängige OPC UA [DWA11]. OPC UA kann auch in Verbindung mit SOAP-Webdiensten verwendet werden [EM07].
- Für die Nutzung von OPC ist ein OPC-Server an jeder Datenquelle sowie ein OPC-Client an jeder Datensenke nötig. OPC-Server sind Anwendungen, die meist von Herstellern von Geräten, zum Beispiel von SPSen, angeboten werden [Mat09]. OPC-Clients sind Bestandteile eines Anwenderprogramms, das die Daten des Quellgeräts benötigt – zum Beispiel ein Office-Programm oder eine HMI-Software [WZ11].

Datenvisualisierung und Bedienung:

- Für die Visualisierung und Bedienung gibt es unterschiedliche **HMI-Softwarelösungen**. Es existieren sowohl geräteunabhängige als auch herstellergebundene Applikationen. Ein bekanntes Beispiel ist die WinCC-Software der Firma Siemens.
- Die Visualisierungs- und Bedienoberfläche kann in IP-basierten Netzen ein sogenannter Thin Client sein, der Daten nur darstellt, während die eigentliche Software auf einem Server läuft [DWA11].
- Besonders für die Funktionen Visualisierung und ggf. Bedienung nimmt auch die Verbreitung von **Webdienste**n zu. Dabei sind unterschiedliche Ausprägungsgrade denkbar [DWA11]:
    - Nur Visualisierung: Prozessdaten werden im Browser dargestellt. Dafür wird ein Webserver betrieben, auf den Daten nur kopiert werden – es wird also nicht mit den Original-Prozessdaten gearbeitet. Nutzer des Web-Dienstes (in der Regel außerhalb des Leitstands) können deswegen die Daten nur anzeigen, nicht aber verändern.
    - Visualisierung und Bedienung: Der Browser wird auch für Bedienung genutzt. Dafür werden Original-Prozessdaten verwendet. Um die Bedienung umsetzen zu können, ist der Browser mit einer Laufzeitumgebung (beispielsweise Java oder Silverlight), Browser-Werkzeugen und / oder Software-Schnittstellen ausgestattet.
- Komponenten mit Visualisierungssoftware werden als HMI bezeichnet. Häufig ist solche Software zusätzlich auf mobilen Geräten oder Office-IT-Komponenten installiert. Operator-Station ist der Begriff für Komponenten, auf denen eine Bediensoftware, also HMI-Software mit Schreibrechten, installiert ist.

SPS-Programmierung (Engineering):

- Als Software für die SPS-Programmierung können Entwicklungsumgebungen wie **Codesys** verwendet werden, die mit vielen Geräten unterschiedlicher Hersteller kompatibel sind. Es gibt aber auch **herstellerspezifische Engineering-Software**, zum Beispiel die Siemens-Software Step 7 [WZ11].
- Der Standard **DIN IEC 61131-3** vereinheitlicht die Programmiersprachen für SPSen [WZ11]. Die meisten Engineering-Softwares sind mit der Norm kompatibel. Für die Wasserwirtschaft wird im DWA-Merkblatt M 253 die Programmierung mittels Funktionsbausteinen, Ablaufsprache (SFC) oder Continuous Function Chart (CFC) empfohlen [DWA11].
- Damit die SPSen mit Sensoren und Aktoren unterschiedlicher Hersteller kommunizieren werden können, gibt es mehrere Möglichkeiten. Einerseits haben sich zur Vereinheitlichung Datenblattformate gebildet. Beispiele sind **GSD** (Gerätestammdatendatei)**,**

CF (Capability File, Common File Format) oder **(E)DD** ((Electronic) Device Description). Spezielle Interpreter können solche Datenblätter auslesen. Alternativ kann die Integration mittels Software-Stellvertretern (Proxies) erfolgen, die die gesamte Gerätefunktionalität erfüllen. Um die Software-Stellvertreter ausführen zu können müssen spezielle Interfaces implementiert sein. Diese Idee setzt die **FDT/DTM** (Field Device Tool / Device Type Manager)-Technologie um [EM07].

- Die Engineering-Software und die Interpreter bzw. Interfaces zur Feldgeräte-Integration sind auf der Engineering-Workstation installiert. Die Datenblätter oder Proxies für die Sensoren und Aktoren stellen die Hersteller [EM07]. Nach der Programmerstellung auf der Engineering-Workstation werden die SPS-Programme kompiliert und auf die SPSen geladen [KWS].

Netzmanagement, Softwaremanagement:

- Netze werden mit Hilfe von Protokollen wie **SNMP** (Simple Network Management Protocol) oder dem **syslog**-Standard überwacht und konfiguriert. Die Konfiguration der Netze kann an zum Netz gehörenden Geräten selbst oder von einer zentralisierten Stelle aus, etwa dem Leitstand, erfolgen [AWWA14]. Nicht nur aktive Netzwerkgeräte wie Router und Switches können SNMP- oder syslog-Daten versenden, auch alle anderen Komponenten im Netz (Drucker, Server, Rechner) sind dazu potenziell in der Lage [MS05].
- **Software-Updates** (Beispiele sind Patches für Betriebssysteme, Signaturen für Antivirenprogramme oder aktuelle Software-Lizenzen) werden bei Nicht-ICS meist automatisiert von der jeweiligen Software veranlasst und aus dem Internet heruntergeladen. Bei ICS werden solche Updates in der Regel erst durch die ICS-Hersteller getestet und freigegeben und anschließend manuell installiert [AWWA14].

4.5 Generische Referenzarchitektur

4.5.1 Generische Zielobjektliste

Eine Auflistung der generischen Zielobjekte, die für das in dieser Arbeit erstellte IT-Grundschutz-Profil für die Wasserwirtschaft berücksichtigt werden, ist in Tab. 4.2 gegeben. Die Zielobjekte sind in sechs Kategorien unterteilt:

- **Organisation (O)**: Für die Informationssicherheit relevante Managementprozesse
- **IT-Systeme (IT)**: ICS-Hardware
- **Anwendungen (A)**: Software für die Erbringung der ICS-Prozesse
- **Netzkomponenten (N)**: Hard- und Software für die Vernetzung und Kommunikation der IT-Systeme und Anwendungen

- **Infrastruktur (IN)**: Physische Orte, an denen Hardwarekomponenten sich befinden können
- **Sicherheit (S)**: Komponenten, die nicht in erster Linie der Erbringung der ICS-Prozesse, sondern der Informationssicherheit der übrigen Komponenten dienen

Auf die Komponenten der Kategorie S wird in Kapitel 5 noch genauer eingegangen.

Außer einer Nummer, die die einzelnen Zielobjekte ihrer Kategorie zuordnet und eindeutig benennt, enthält die Tabelle auch eine kurze Beschreibung der Zielobjekte. Ausführlichere Beschreibungen finden sich für die Geräte in Abschnitt 2.1.2.1, für die Kommunikationstechnik in den Abschnitten 2.1.2.2, 4.1 und 4.2, für die Anwendungen in Abschnitt 4.4 und für die Sicherheitskomponenten in Abschnitt 5.3.

Tab. 4.2: Generische Zielobjektliste

Nr.	Zielobjekt	Beschreibung
Organisation		
O1	Sicherheits-management	Teil des Managements, das sich mit der Informationssicherheit befasst.
O2	Notfallmanagement	Stellt die Kontinuität des Betriebs in Notfällen sicher.
IT-Systeme		
IT1	Feldgerät	Sensor oder Aktor. Beispiele für Sensoren sind Druck- oder Durchflussmesser, Beispiele für Aktoren Pumpen oder Ventile.
IT2	SPS	Speicherprogrammierbare Steuerung. Spezialisierter Computer für die automatisierte Prozesssteuerung. Auch bekannt unter dem englischen Begriff PLC (Programmable Logic Controller).
IT3	HMI	Bedien- und Benutzeroberfläche für die Prozesssteuerung, insbesondere auch für die Koordination aller SPSen. Hier kann der gesamte Prozess überwacht werden. Auch Eingriffe, beispielsweise Sollwertsetzungen, sind möglich.
IT4	Historian	Rechner bzw. Server, auf dem (vergangene) Prozessdaten archiviert werden.
IT5	Engineering-Workstation	Rechner, auf dem die Programme für die SPSen geschrieben werden. Dedizierte Rechner für diesen Zweck werden auch als Programmiergerät (PG) bezeichnet.
IT6	Control Server	Zentraler Speicherort für alle Daten und Programme, die eine Prozesssteuerung ermöglichen. Dient oft der Erfüllung von SCADA / PLS / DCS-Aufgaben.
IT7	Webserver	Stellt ICS-Funktionen, etwa des HMI oder Historian, über das Internet (im Browser) zur Verfügung.
IT8	Mobilgerät	Laptop, Tablet oder Smartphone, das in verschiedenen Bereichen des ICS-Netzes für verschiedene Funktionen zum Einsatz kommen kann. Beispiele sind Engineering- oder HMI-Funktionen und das Empfangen von Alarmen.
IT9	Externe Komponente	Ein Laptop oder Desktop-PC, der nicht zum ICS-Netz gehört. Entweder eine Office-Komponente oder ein PC eines ICS-Herstellers, der beispielsweise für Fernwartung genutzt werden kann.
IT 10	Office-IT-Komponente	Ein Desktop-PC, Laptop, Drucker oder eine sonstige Komponente zur Erfüllung von nicht-ICS-relevanten Aufgaben.

Anwendungen		
A1	Engineering-Software	Softwareumgebung, mit der Programme für SPSen geschrieben und kompiliert werden können. Da die SPS-Programmiersprachen im Standard DIN IEC 61131-3 vereinheitlicht werden, sind die meisten Programme mit der Norm kompatibel.
A2	SPS-Programm	Kompiliertes Programm, das zur Ausführung auf die SPS geladen wird.
A3	HMI-Software	Anwendung, die eine (meist grafische) Darstellung der aktuellen Prozessdaten bietet. Auch Bedienfunktionen, etwa für das Setzen von Sollwerten und das Bedienen von Aktoren, sind enthalten.
A4	Datenbank	Anwendung zum Archivieren vergangener Prozessdaten.
A5	Webdienst	Anwendung, die ein IP-basiertes Netz nutzt, um Dienste auf Basis von HTTP, SMTP oder FTP anzubieten. Das wichtigste Protokoll für Webdienste ist SOAP. Eine Anwendung, die häufig als Webdienst bereitgestellt wird, ist die HMI-Software.
A6	Netzmanagement-Software	Anwendung, die für die Überwachung und Konfiguration der Netze und Netzwerkgeräte verwendet wird. Beispiele sind das Protokoll SNMP oder der syslog-Standard.
A7	OPC	Standard für die Kommunikation zwischen Geräten unterscheidlicher Hersteller. OPC-Server sind Anwendungen, die von ICS-Herstellern angeboten werden, um ihr Gerät OPC-fähig zu machen. OPC-Clients sind Anwendungen, die den Zugriff auf einen OPC-Server ermöglichen.
A8	Mail, SMS, Instant Messaging	Eine Anwendung für kurze, automatisierte Nachrichten, die von den Steuergeräten gesendete Alarme überträgt.
A9	Betriebssystem	Windows, Unix-System oder Mac OS für PCs oder Laptops bzw. Firmware für eingebettete Systeme wie SPSen.
Netzkomponenten		
N1	Switch	Netzwerkgerät, das LAN-Teilnehmer zu einem LAN verbindet.
N2	Router	Netzwerkgerät, das für die Verbindung eines LANs zu einem anderen oder zu einem WAN zuständig ist.
N3	Modem	Netzwerkgerät, digitale Signale für ein analoges WAN-Übertragungsmedium umformt.
N4	IT-Verkabelung	Kabel zum Verbinden der einzelnen Geräte eines Netzes, beispielsweise Ethernet-Kabel.
N5	Feldbus	Steht hier stellvertretend für alle Echtzeit-Kommunikationstechniken: Einheitssignale, klassische Feldbustechnik, Funk und Industrial Ethernet.
N6	Fernwartung	WAN-Verbindung zum System eines ICS-Herstellers zum Zweck der Fernwartung.
Infrastruktur		
IN1	Leitstand	Räumlichkeit, von der aus die Prozesssteuerung erfolgt. Darin befindet sich in jedem Fall das HMI und möglicherweise Engineering-Workstations, Historian und / oder ein Server.
IN2	Büro	Räumlichkeit für Office-IT-Komponenten.
IN3	Serverraum	Räumlichkeit mit speziellen klimatischen und / oder zugangstechnischen Bedingungen, in der Server und Großrechner ohne Bedienschnittstelle untergebracht sind.

IN4	Schutzschrank	Schaltschrank, in dem SPSen untergebracht und verschaltet werden.
IN5	Mobiler Arbeitsplatz	Arbeitsplatz eines Mobilgeräts.
IN6	Feld	Steht für die Räumlichkeiten (oder den Ort ohne spezielle Räumlichkeiten), in der die zu steuernden Maschinen, Feldgeräte und ggf. SPSen untergebracht sind. In der Automatisierungstechnik auch als Feld bekannt.
Sicherheit		
S1	Firewall	Hard- oder Software, die Datenverkehr im Netz oder auf einem Host nach bestimmten Regeln filtert. Dazu gehören unter anderem Layer-3-Firewalls (Paketfilter) und Layer-7-Firewalls (Application Layer Gateways).
S2	VPN	Umfasst die Soft- und Hardware für den Aufbau einer VPN-Verbindung, zum Beispiel VPN-Router, VPN-Gateways oder VPN-Server.
S3	IDS / IPS	Intrusion Detection System / Intrusion Prevention System.
S4	Antiviren-Software	Software, die anhand von Signaturen bekannte Malware erkennt.

4.5.2 Generische Netzpläne

Zur Veranschaulichung der Verknüpfungen zwischen den bislang nur aufgelisteten Zielobjekten werden in den folgenden Abschnitten generische Netzpläne der Referenzarchitektur gegeben. Dabei wird zwischen einem physischen und einem logischen Netzplan unterschieden, während die spezifischen Netzpläne – je nach Anwendungsfall – sowohl logische als auch physische Komponenten vereinen. Die Grundlage für alle Netzpläne bildet die gemischte ICS-Netzstruktur aus Abb. 3.3 mit der verteilten Netzstruktur auf der linken und der konzentrierten Netzstruktur auf der rechten Seite. Wie in der Einleitung dieses Kapitels 4 bereits erwähnt, musste in den generischen Netzplänen oft eine Konfigurationsmöglichkeit aus vielen ausgewählt werden. Für Netzpläne zu spezifischen Anwendungsfällen, die verschiedene Konfigurationsmöglichkeiten abbilden, sei auf Abschnitt 4.6 verwiesen.

In Abb. 4.1 ist die Legende zu den folgenden Netzplänen gegeben.

- Rechteckige Kästen zeigen **Komponenten** an, Linien ihre **Verbindungen**. Sowohl Komponenten (z.B. eine SPS) als auch Verbindungen (z.B. der Feldbus) können Zielobjekte repräsentieren.
- Soweit sich die Komponenten in die **Automatisierungspyramide** (siehe Abschnitt 2.1.1) einordnen lassen, ist dies farblich dargestellt. Dabei werden die oberen beiden Ebenen zur Unternehmensebene zusammengefasst und umfassen alle Office-IT-Komponenten (gelb), die Prozessleitebene umfasst alle in dieser Arbeit als Prozessleitkomponenten zusammengefassten Komponenten (grün), die Steuerungsebene die SPSen (türkis) und die Feldebene Feldgeräte (blau).

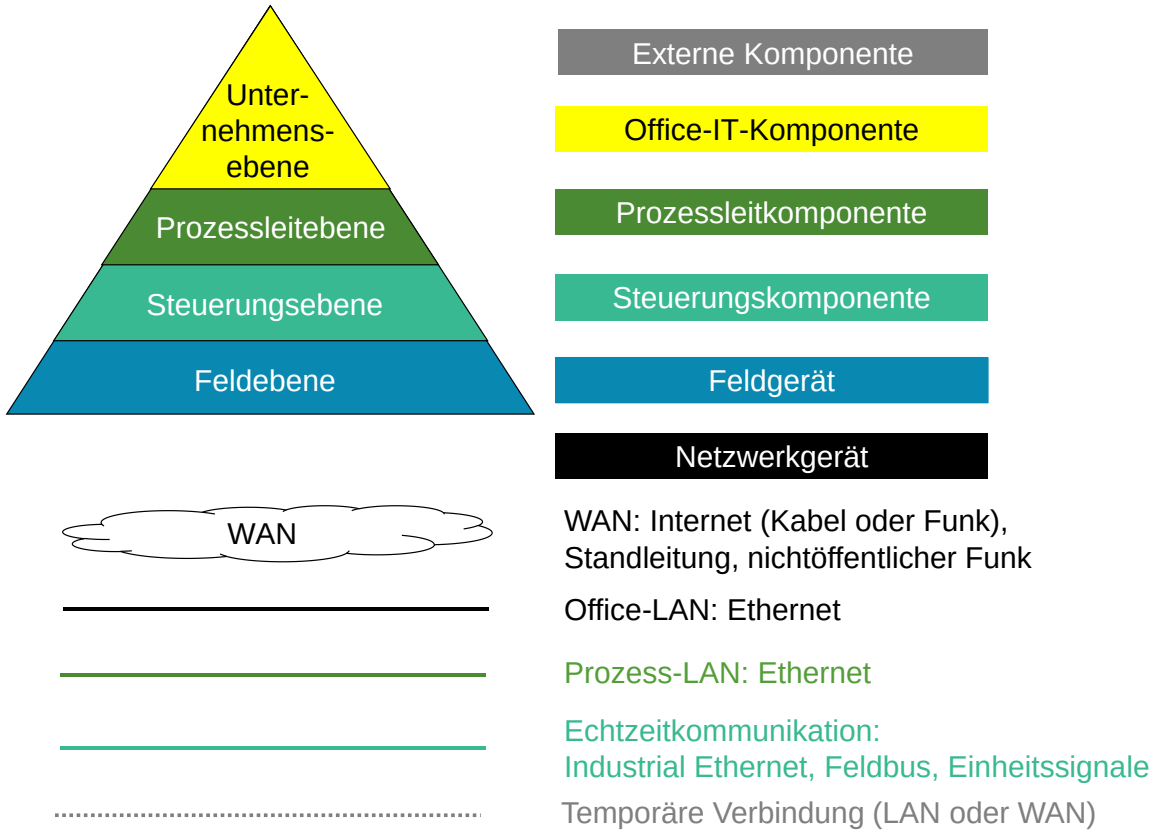


Abb. 4.1: Legende zu den Netzplänen: Komponenten, Einordnung in die Automatisierungspyramide und Verbindungen der Komponenten

- **Externe Komponenten** (grau) stellen in den Netzplänen alle Komponenten dar, die nicht fest zum ICS-Netz einer Institution gehören. Dies können Office-Komponenten, Komponenten anderer Institutionen (etwa für die Fernwartung) oder mobile Komponenten (Tablets oder Laptops) sein.
- **Netzkomponenten** sind schwarz dargestellt und nur im physischen Netzplan eingezeichnet.
- **WAN-Verbindungen** werden durch eine Wolke dargestellt. Dabei steht WAN in aller Regel für eine Internetverbindung über öffentliche Telefonleitungen oder Mobilfunk; ist aber generisch gehalten, um auch Standleitungen und nichtöffentliche Funkverbindungen abzudecken (siehe Abschnitt 4.2).
- **LAN-Verbindungen** sind durch Linien dargestellt. Schwarze und grüne Linien stehen für Ethernet-Verbindungen. Schwarze Verbindungen stehen für reine Office-Netze, grüne Linien verbinden ICS-Komponenten. Türkise Verbindungen stehen für alle Formen von Echtzeitkommunikation: Industrial Ethernet, klassische Feldbusse oder Einheitssignale (siehe Abschnitt 2.1.2.2).
- Ist die Verbindungslinie grau und gepunktet, kennzeichnet sie eine **temporäre Verbindung**, zum Beispiel ein Fernwartungszugang zu einem externen PC oder eine LAN-

Verbindung eines Mobilgeräts. Mehrere temporäre Verbindungen bestehen in der Regel nicht gleichzeitig, zum Beispiel kann ein mobiles Gerät nicht mit zwei (verteilten) SPSen gleichzeitig direkt verbunden sein.

4.5.2.1 Physischer Netzplan

Ein physischer Netzplan der generischen Referenzarchitektur ist in Abb. 4.2 zu sehen. Außer den Komponenten und Verbindungen zeigt der physische Netzplan die Räumlichkeiten, in denen Komponenten verortet sind. Auch Netzkomponenten werden aufgeführt. Anwendungen werden im physischen Netzplan nicht abgebildet.

- Für die ICS-Komponenten des zentralen Leitstands (links) ist dabei angenommen, dass alle Komponenten mit schreibendem Zugriff auf die Steuergeräte, also mindestens HMI und Engineering-WS, sich in einem abschließbaren Raum, **Leitstand** genannt, befinden.
- Historian und Server, die keine oder zumindest keine dauerhaft genutzte Bedienschnittstelle haben, sind im Netzplan nicht im Leitstand, sondern in einem separaten **Serverraum** verortet.
- Office-Komponenten für die Verwaltung auf zentraler Leitstands-Ebene haben nicht nur ein **separates LAN** (eigener Switch), sondern auch eigene Räumlichkeiten – sie sind im Netzplan als **Büro** gelb gekennzeichnet.
- Für den lokalen Leitstand (rechts) ist ein **gemeinsames LAN** für ICS- und Office-Komponenten angenommen. Auch haben Leitstands- und Office-Komponenten **gemeinsame Räumlichkeiten** (Büro = Leitstand).
- Steuer- und Feldgeräte, die echtzeitfähig miteinander kommunizieren, werden räumlich der **Anlage** zugeordnet, zu der sie gehören. Dabei können mehrere SPSen, Sensoren und Aktoren zu ein- und derselben Anlage gehören; bei den verteilten Steuergeräten können aber auch räumliche Trennungen zwischen ihnen liegen.
- **Externe Komponenten** können über das WAN auf die ICS- oder Office-Netze zugreifen. Dasselbe gilt für **Mobilgeräte**, die jedoch auch direkte Schnittstellen zu einzelnen Geräten, beispielsweise SPSen, besitzen können. Verbindungen zu externen und mobilen Geräten sind in der Regel temporär.

In Abb. 4.2 sind bezüglich zweier Aspekte Annahmen getroffen worden: Bezüglich der räumlichen Verordnung der Zielobjekte und bezüglich der gemeinsamen Nutzung der Netze durch Office- und ICS-Komponenten. Variationen dieser Aspekte werden in den Anwendungsfallgruppen in Abschnitt 4.6 behandelt:

- Die Anwendungsfallgruppe **Architektur (AR)** enthält Anwendungsfälle, die sich mit der gemeinsamen Nutzung von Local Area Networks (LAN) und Wide Area Networks (WAN) durch Office-IT-Komponenten und ICS-Komponenten befassen.
- Die Anwendungsfallgruppe **Benutzerzugang (UA)** enthält Anwendungsfälle, die den physischen Zugang von Benutzern zur ICS-Anlage betrachten.

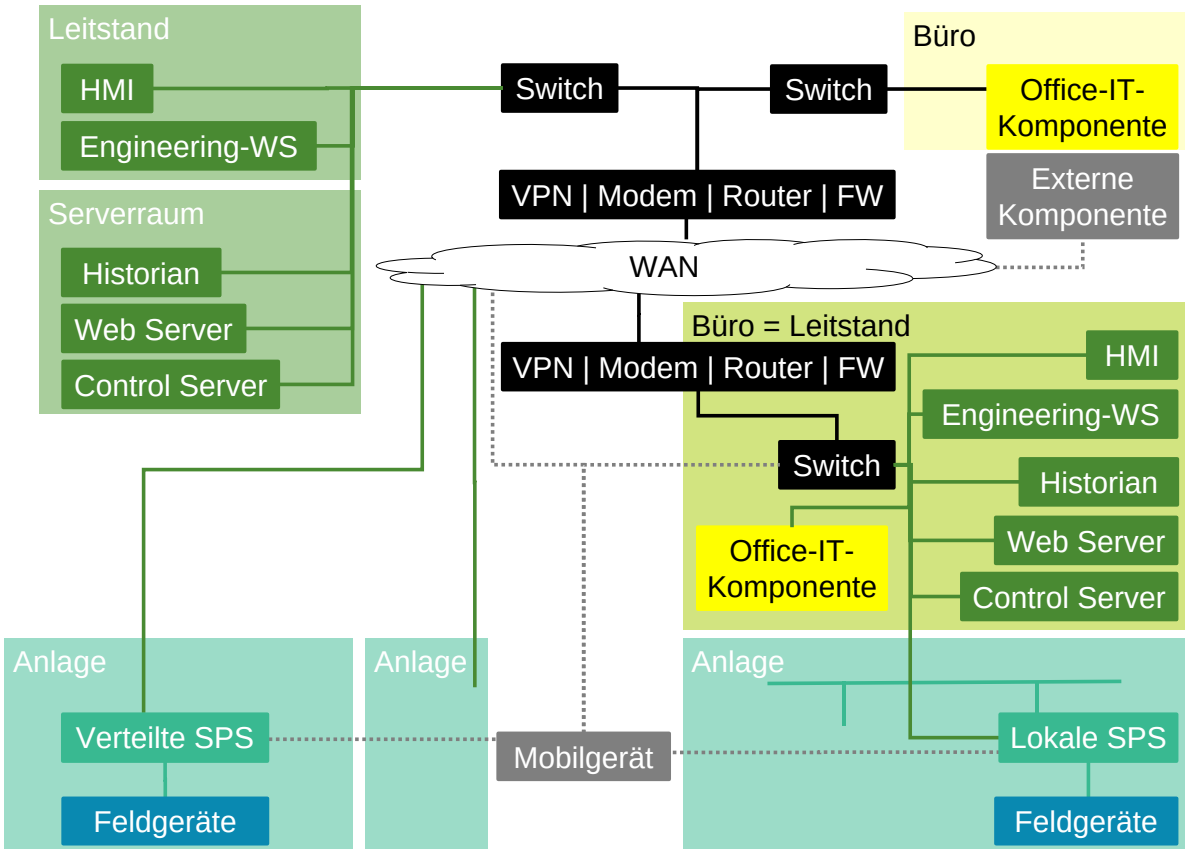


Abb. 4.2: Physischer Netzplan der generischen Referenzarchitektur

4.5.2.2 Logischer Netzplan

Der logische Netzplan in Abb. 4.3 soll den logischen Datenfluss zwischen den Anwendungen abbilden. Die Netzwerkgeräte und der physische Ort der Komponenten werden nicht abgebildet.

Die Komponenten sind – bis auf die nicht dargestellten Netzwerkgeräte – dieselben wie im physischen Netzplan. Zusätzlich sind jedoch, entsprechend der Zielobjektliste, ICS-relevante Anwendungen abgebildet, die auf den jeweiligen Komponenten installiert sind. Eine nähere Beschreibung der Anwendungen findet sich in der generischen Zielobjektliste (Abschnitt 4.5.1) und in Abschnitt 4.4.

- In der Regel sind diese **Anwendungen auf dedizierten Komponenten** installiert.
- Office-Komponenten sind nicht dargestellt, da **Office-Anwendungen** nicht zum Geltungsbereich dieses Profils gehören. Wenn ICS-Anwendungen auf Office-Komponenten installiert sind, werden diese Office-Komponenten im logischen Netzplan als externe Komponente betrachtet.
- Wie auch auf dem **Mobilgerät** können auf **externen Komponenten** eine Vielfalt von möglichen Anwendungen installiert sein, darunter HMI-Software, Engineering-Software oder Netzmanagementsoftware. Dabei ist es sowohl beim externen PC als auch beim Mobilgerät möglich, dass eine, mehrere oder keine der genannten Anwendungen tatsächlich installiert sind.

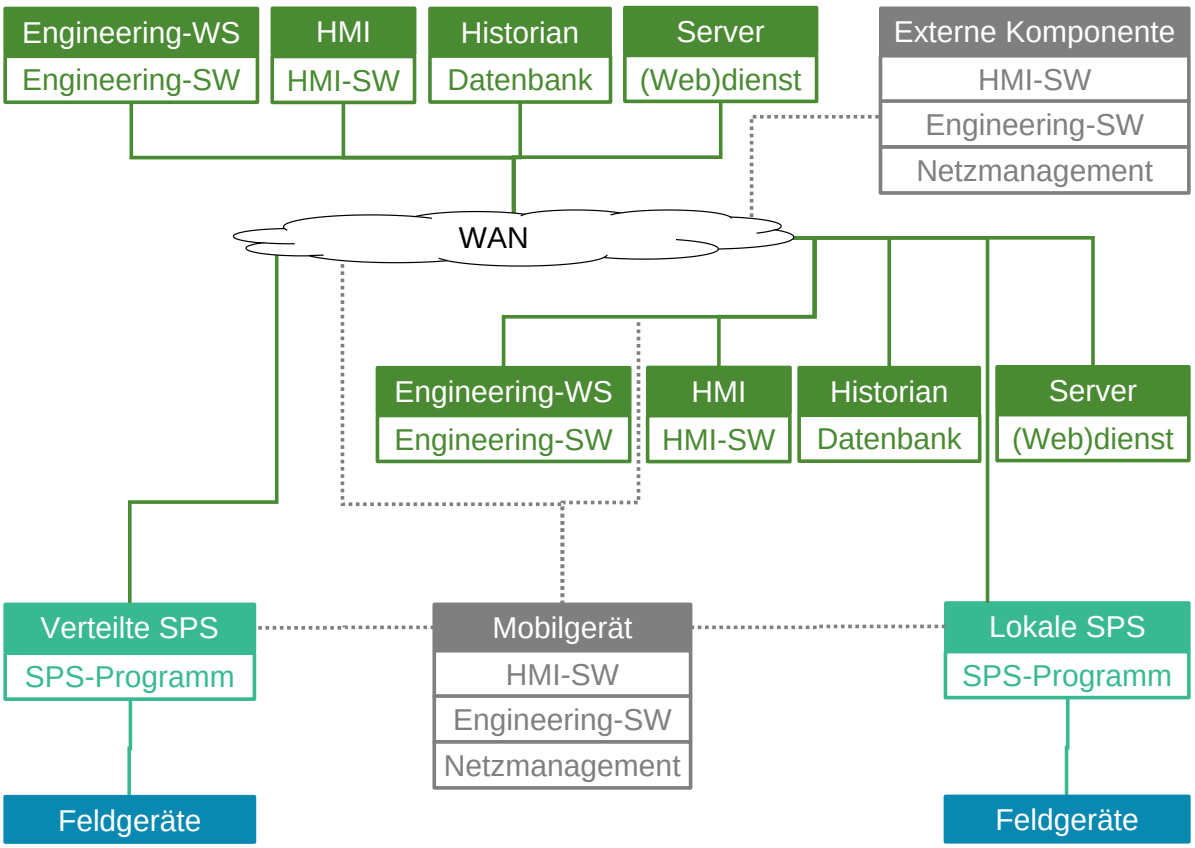


Abb. 4.3: Logischer Netzplan der generischen Referenzarchitektur

Der Datenfluss zwischen den Anwendungen ist sehr vielfältig und zudem stark vom Anwendungsfall abhängig, weshalb er nicht im generischen logischen Netzplan, sondern nur für spezielle Anwendungsfälle in den spezifischen Netzplänen in Abschnitt 4.6 dargestellt wird:

- Die Anwendungsfallgruppe **Benutzerzugang (UA)** enthält Anwendungsfälle, die den Zugriff auf das HMI und die HMI-Software (HMI-SW) betrachten.
- Die Anwendungsfallgruppe **SPS-Programmierung und -Wartung (PLC)** enthält Anwendungsfälle, die die Programmierung und den Zugriff auf SPSen und ihre Programme betrachten, besonders mittels Engineering-Workstations (Engineering WS) und entsprechender Engineering-Software (Engineering-SW).
- Die Anwendungsfallgruppe **Netzmanagement (NM)** enthält Anwendungsfälle, die den Betrieb und die Konfiguration der einzelnen Zielobjekte, vor allem der Netzkomponenten, und der darauf installierten Software betrachten.
- Die Anwendungsfallgruppe **Programmzugriff (PA)** enthält Anwendungsfälle, die die automatisierte oder interaktive Kommunikation zwischen verschiedenen Anwendungen betrachten.

4.6 Anwendungsfälle

Wenn es an die Ist-Analyse des eigenen Systems zur Ermittlung der Referenzarchitektur geht, liegt Anlagenbetreibern das Denken in Anwendungsfällen näher als das Denken in Referenzarchitekturen. Welche Anwendungsfälle sein System erfüllt, kann jeder Betreiber eines ICS beantworten; wie der Netzplan des Systems aussieht, nicht unbedingt. Häufig sind die Netzstrukturen „historisch gewachsen“ und nicht dokumentiert.

Aus diesem Grund wird in dem in dieser Arbeit erstellten IT-Grundschutz-Profil die Anpassung der Referenzarchitektur an die ICS-Anlagen der Profilanwender vorgenommen, indem die Anwender für ihre Anlagen passende Anwendungsfälle auswählen.

4.6.1 Hauptprofil und Unterprofile

Die Anwendungsfälle werden in fünf Gruppen gegliedert. Jede Anwendungsfallgruppe behandelt einen Aspekt der Referenzarchitektur. Ein Unterprofil umfasst jeweils eine solche Anwendungsfallgruppe – es sind im Rahmen des Profils für die Wasserwirtschaft also fünf Unterprofile vorgesehen.

Wie die in Abschnitt 2.2.3 (Tab. 2.3) eingeführte Struktur des IT-Grundschutz-Profils sich auf das Hauptprofil und die Unterprofile aufteilt, veranschaulicht Tab. 4.3. Die Unterabschnitte der Profilabschnitte 1 bis 3 sowie 8 und 9 sind für die Unterprofile nicht direkt relevant und sind deswegen der Übersichtlichkeit halber ausgeblendet.

Die **Unterprofile (UP)** sind Teilprofile, die auf einen Aspekt des Hauptprofils spezialisiert sind. Innerhalb eines Unterprofils werden in Form von Anwendungsfällen Variationen dieses Aspekts vorgestellt. Die maßgeblichen Abschnitte der Unterprofile sind die Abschnitte UP6 und UP7: Der Anwender des Profils sucht in Abschnitt UP6 (Referenzarchitektur) die für ihn zutreffenden Anwendungsfälle aus (in der Regel mindestens einen pro Unterprofil) und erhält eine dazu passende **spezifische** Referenzarchitektur, bestehend aus einer spezifischen Zielobjektliste und einem spezifischen Netzplan. Im selben Abschnitt erfolgt – auf Basis der spezifischen Referenzarchitektur – die Schutzbedarfsfeststellung der einzelnen Zielobjekte. Abschnitt UP7 (Anforderungen und Maßnahmen) enthält die Modellierung der spezifischen Referenzarchitekturen mit IT-Grundschutz-Bausteinen und eine Liste der für den Anwendungsfall relevanten Anforderungen.

Das übergeordnete **Hauptprofil (HP)** enthält alle Inhalte, die für jeden Profilanwender relevant sind. Es bereitet den Anwender auf die Anpassung des Profils an seine Anlagen vor und hilft ihm bei der anschließenden Überführung aller in den Unterprofilen ausgewählten Anwendungsfälle in ein vollständiges Sicherheitskonzept. Das Hauptprofil enthält dazu die Abschnitte 1 (Formale Aspekte), 2 (Management Summary), 3 (Anwendung des Profils), 4 (Geltungsbereich), 5 (Abgrenzung des Informationsverbunds) und 8 (Risikobehandlung). Außerdem wird im Abschnitt 6 (Referenzarchitektur) eine **generische** Referenzarchitektur, bestehend aus einer generischen Zielobjektliste und einem generischen Netzplan, gegeben, die die Grundlage für die Anwendungsfallauswahl darstellt.

Sicherheitsmaßnahmen, die Organisation und Management betreffen, werden im Hauptprofil behandelt, weil sie **anwendungsfallunabhängig** und architekturunabhängig sind und somit keine spezifischen Referenzarchitekturen erfordern. Konkret bedeutet dies, dass die Modellierung und die Auswahl geeigneter Maßnahmen für die Zielobjekte der Kategorie *Organisation* im Hauptprofil erfolgt, und zwar im Abschnitt 7 (Anforderungen und Maßnahmen).

Tab. 4.3: Struktur des IT-Grundschutz-Profils, aufgeteilt auf Hauptprofil und Unterprofile

Hauptprofil	Unterprofile
1 Formale Aspekte	**UP1 Formale Aspekte**
2 Management Summary	**UP2 Management Summary**
3 Anwendung des Profils	
4 Geltungsbereich	
5 Abgrenzung des Informationsverbunds 5.1 Organisationsstruktur 5.2 Geschäftsprozesse und Anlagen 5.3 Schutzbedarf der Anlagen 5.4 ICS-Netzstruktur	
6 Generische Referenzarchitektur 6.1 Generische Zielobjektliste 6.2 Generische Netzpläne 6.3 Schutzbedarf der anwendungsfallunabhängigen Zielobjekte	**UP6 Spezifische Referenzarchitektur** UP6.1 Spezifische Zielobjektlisten UP6.2 Spezifische Netzpläne UP6.3 Schutzbedarf der spezifischen Zielobjekte
7 Anforderungen und Maßnahmen 7.1 Modellierung der anwendungsfallunabhängigen Zielobjekte 7.2 Auswahl der Anforderungen 7.3 ggf. Umsetzungsvorgaben	**UP7 Anforderungen und Maßnahmen** UP7.1 Modellierung der spezifischen Zielobjekte UP7.2 Auswahl der Anforderungen UP7.3 ggf. Umsetzungsvorgaben
8 Risikobehandlung 8.1 Integration und Realitätsabgleich der Gesamt-Referenzarchitektur 8.2 Vorgehensweise bei Abweichungen 8.3 Hilfestellungen zur ergänzenden Risikoanalyse	
9 Anhang	**UP9 Anhang**

4.6.2 Anwendungsfallgruppen der AWWA

Die Anwendungsfallgruppen, die in dieser Arbeit für die Wasserwirtschaft verwendet werden, basieren auf Anwendungsfällen der American Water Works Association (AWWA). Die AWWA ist ein internationaler, gemeinnütziger Verband, der Standards und Informationsmaterial rund um die Themen Wasserversorgung und -aufbereitung veröffentlicht [AWWA17a].

Die AWWA-Handreichung *Process System Security Guidance* basierte auf ursprünglich 20 Anwendungsfällen in fünf Gruppen [AWWA14]. In einer 2017 veröffentlichten, aktualisierten Version ist die Anzahl der Anwendungsfälle auf 40 verdoppelt worden, die fünf Kategorien wurden jedoch beibehalten [AWWA17c]. Die deutschen Branchenverbände DWA und DVGW orientieren sich bei der Erarbeitung ihres branchenspezifischen Sicherheitsstandards Wasser / Abwasser (B3S WA) an den 20 AWWA-Anwendungsfällen der ersten Version [WT16; Ter16].

Die AWWA gliedert ihre Anwendungsfälle in die fünf Gruppen

- **Architektur** (Architecture, **AR**),
- **Netzmanagement** (Network Management, **NM**),
- **Benutzerzugang** (User Access, **UA**),
- **Programmzugriff** (Program Access, **PA**) und
- **SPS-Programmierung und -Wartung** (PLC Programming and Maintenance, **PLC**).

Die fünf Anwendungsfallgruppen sollen in diesem Abschnitt vorgestellt und zu jedem Anwendungsfall der Gruppe – also zu jeder Variationsmöglichkeit – eine Referenzarchitektur gegeben werden. Dabei wird in Anlehnung an den B3S WA die Liste von 2014 verwendet.

In den folgenden Abschnitten wird für jede Anwendungsfallgruppe eine spezifische Zielobjektliste und für jeden Anwendungsfall eine spezifische Referenzarchitektur gegeben. Die spezifische Zielobjektliste wird dabei auf die unmittelbar für den Anwendungsfall relevanten Objekte begrenzt und enthält der Übersichtlichkeit halber nur noch die Nummer und Bezeichnung der Zielobjekte – die ausführliche Beschreibung ist identisch zur generischen Zielobjektliste und kann dort nachgelesen werden.

In der Referenzarchitektur können mehr Objekte als in der spezifischen Zielobjektliste auftauchen, wenn sie zur Veranschaulichung notwendig sind. Beispielsweise sind die Feldgeräte, Steuergeräte und grundlegenden LAN- und WAN-Verbindungen in jeder Referenzarchitektur eingezeichnet, um die grundlegende Darstellung der konzentrierten und verteilten Anlagenstruktur aus Abschnitt 3 (Abb. 3.3) beizubehalten. Die spezifischen Zielobjektlisten aller Anwendungsfallgruppen decken zusammengenommen die gesamte generische Zielobjektliste ab.

Abb. 4.4 enthält eine weiterführende Legende zu den Referenzarchitekturen der Anwendungsfälle. Die Komponenten und Verbindungen der Komponenten sind analog zum generischen Netzplan in Abschnitt 4.5.2 dargestellt (siehe Legende in Abb. 4.1), jedoch wurden nur die für den jeweiligen Anwendungsfall relevanten Komponenten und Verbindungen berücksichtigt.

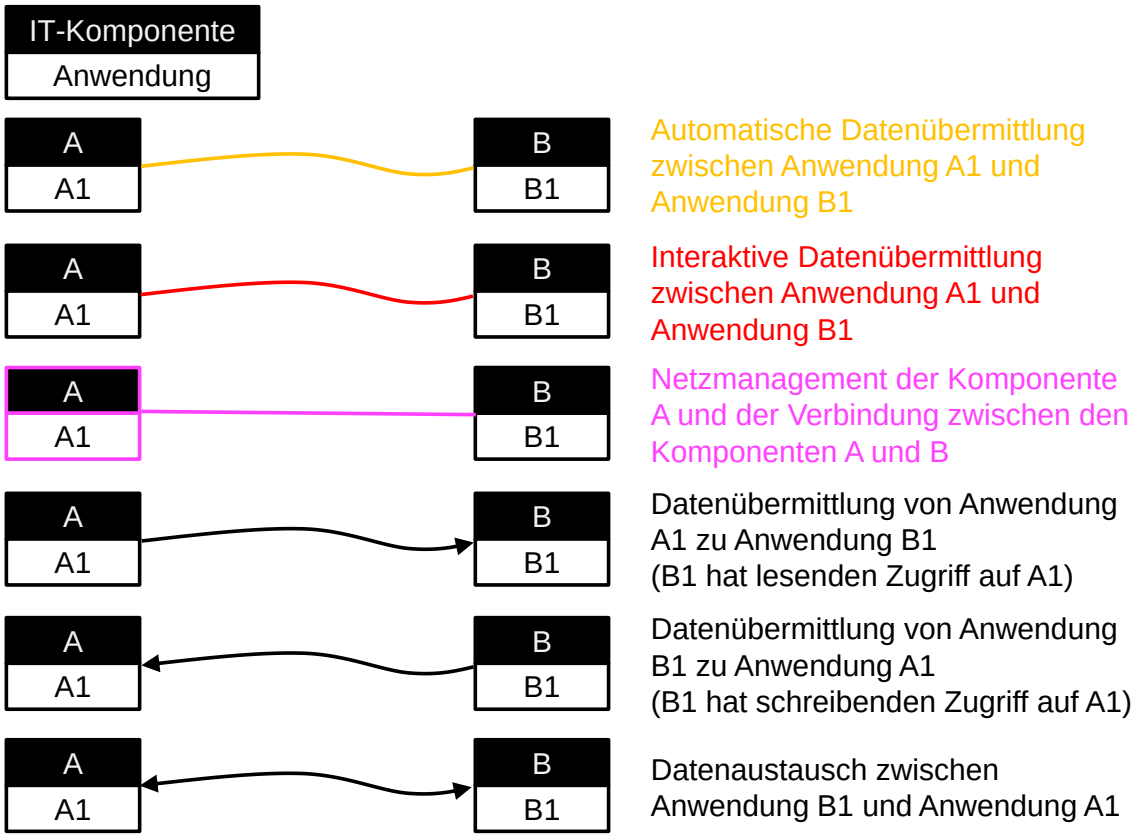


Abb. 4.4: Legende zu den Netzplänen: Datenübermittlung

- Für den betreffenden Anwendungsfall relevante **Anwendungen** sind in einem weißen Feld unterhalb der Komponente dargestellt.
- Linien in Rottönen stellen die **Datenübermittlung** dar: Orangefarbene Linien stehen für automatisierte Datenübermittlung, rote für interaktive Datenübermittlung. Ist eine Komponente oder Verbindung pinkfarben gekennzeichnet, steht dies für den Zugriff auf die Netzmanagementdaten einer Komponente bzw. auf die Konfiguration einer (Netz)verbindung.
- Pfeile verdeutlichen die **vorherrschende Richtung der Datenübermittlung**: Ein Pfeil von einer Komponente A zu einer Komponente B bedeutet, dass Daten von einer Anwendung der Komponente A zur einer Anwendung der Komponente B übermittelt werden; B hat in diesem Fall also nur lesenden Zugriff auf A. Ein Pfeil von B nach A bedeutet dementsprechend eine Datenübermittlung von B nach A bzw. schreibenden Zugriff der Komponente B auf die Komponente A. Ein Pfeil in beide Richtungen kennzeichnet einen Datenaustausch zwischen beiden Komponenten.

Da die Erstellung aller fünf Unterprofile für alle Anwendungsfälle den Rahmen dieser Masterarbeit sprengen würde, wird beispielhaft das Unterprofil für die Anwendungsfallgruppe *Architektur* erstellt. Die in den folgenden Abschnitten ebenfalls gegebenen Referenzarchitekturen für die anderen Anwendungsfallgruppen legen jedoch bereits den Grundstein für die Erstellung analoger Unterprofile für die übrigen Gruppen.

4.6.3 Architektur (Architecture, AR)

Die Anwendungsfallgruppe AR beschäftigt sich mit der Netzstruktur der ICS- und der Office-IT-Komponenten. Da es in dieser Anwendungsfallgruppe um die Netzarchitektur geht, stehen die Netzkomponenten mitsamt zugehöriger Sicherheitskomponenten im Vordergrund.

ICS-Komponenten werden in der spezifischen Zielobjektliste in Tab. 4.4 mit aufgeführt; sie sind aber für die spätere Anforderungsauswahl nur unter dem Aspekt ihrer Platzierung im Netz relevant. Externe Komponenten sind bezüglich ihrer Stellung in der Architektur wie Office-IT-Komponenten zu behandeln und deswegen nicht explizit erwähnt. Mobilgeräte sind in der Architektur nicht fest verankert; ihre Einbindung hängt von der Art ihrer Verwendung ab – deswegen werden auch sie in der Anwendungsfallgruppe AR nicht betrachtet.

Tab. 4.4: Spezifische Zielobjektliste für die Anwendungsfallgruppe AR

Nr.	Zielobjekt
IT-Systeme	
IT1	Feldgerät
IT2	SPS
IT3	HMI
IT4	Historian
IT5	Engineering-Workstation
IT6	Control Server
IT7	Webserver
IT10	Office-IT-Komponente
Netzkomponenten	
N1	Switch
N2	Router
N3	Modem
N4	IT-Verkabelung
N5	Feldbus
N6	Fernwartung
Sicherheit	
S1	Firewall
S2	VPN
S3	IDS / IPS

Der Anwendungsfall **AR1: Dediziertes ICS-Netz** (siehe Abb. 4.5) beschreibt eine Architektur, in der Office-IT und ICS-Komponenten vollständig getrennt sind. In diesem Fall haben die Office-Komponenten keinerlei Auswirkungen auf das ICS-Netz und sind deswegen nicht Teil der Referenzarchitektur. Dies gilt sowohl für die verteilte ICS-Netzstruktur (linke Hälfte der Abb. 4.5) mit einem zentralen Leitstand (bestehend aus HMI und ggf. Engineering-WS), der über ein WAN mit dem Feld verbunden ist, als auch für die konzentrierte ICS-Netzstruktur (rechte Hälfte der Abb. 4.5) mit lokalem Leitstand im selben LAN wie die Feldgeräte.

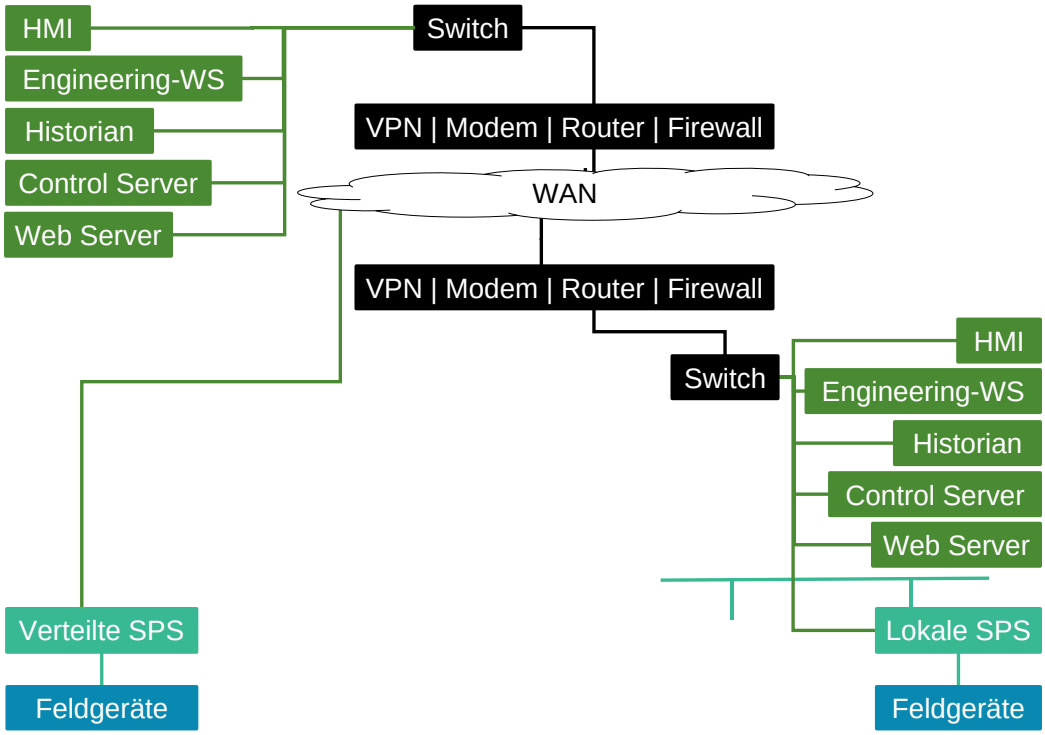


Abb. 4.5: Netzplan des Anwendungsfalls AR1: Dediziertes ICS-Netz

Der Anwendungsfall **AR2: Gemeinsames WAN** (Abb. 4.6) zeigt eine Architektur, bei der das WAN, das die Kommunikation zwischen dem zentralen Leitstand und den verteilten SPSen sowohl zwischen dem zentralen und den lokalen Leitständen ermöglicht, von Office-IT-Komponenten und ICS-Komponenten gemeinsam genutzt wird. Wie beim Fall AR1 gilt dies für Office-IT-Komponenten sowohl auf Ebene des zentralen als auch der lokalen Leitstände. Die LANs sind jedoch weiterhin getrennt: Separate Switches bilden das ICS- und das Office-LAN.

Der dritte Anwendungsfall, **AR3: Gemeinsames LAN** (Abb. 4.7), stellt noch eine Steigerung der gemeinsamen Netznutzung dar. Nun wird nicht nur das WAN, sondern auch die lokalen Netze auf zentraler und lokaler Ebene gemeinsam von ICS- und Office-IT-Komponenten genutzt. Das bedeutet, dass die Komponenten an ein- und demselben Switch und somit in derselben Kollisionsdomäne hängen.

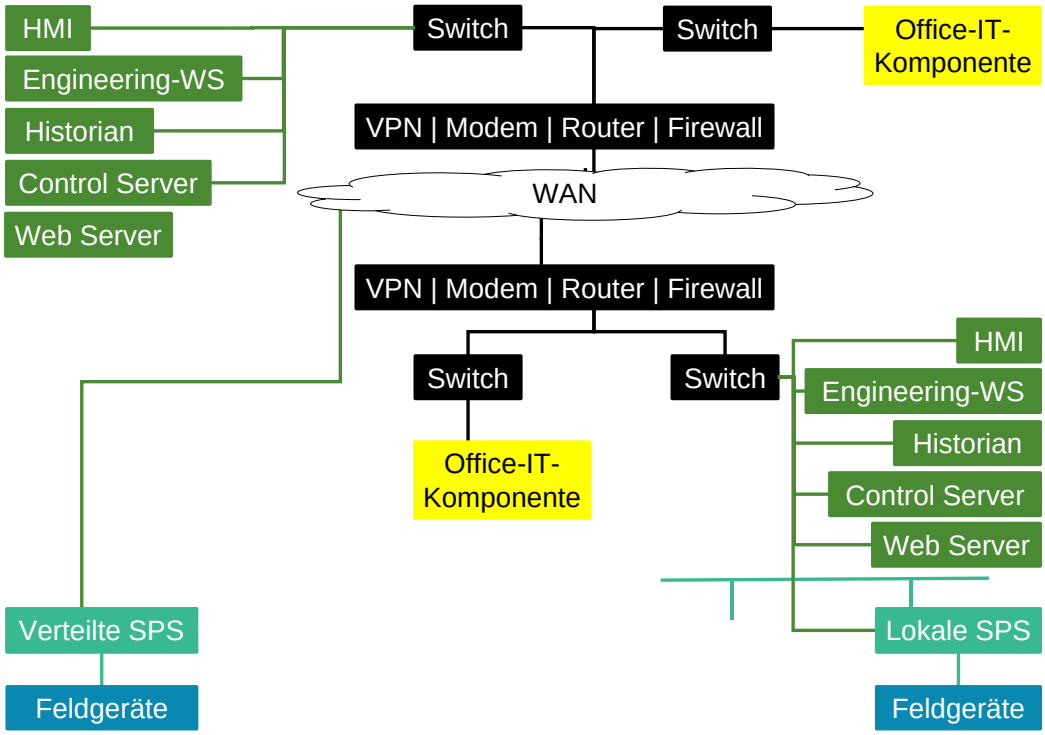


Abb. 4.6: Netzplan des Anwendungsfalls AR2: Gemeinsames WAN

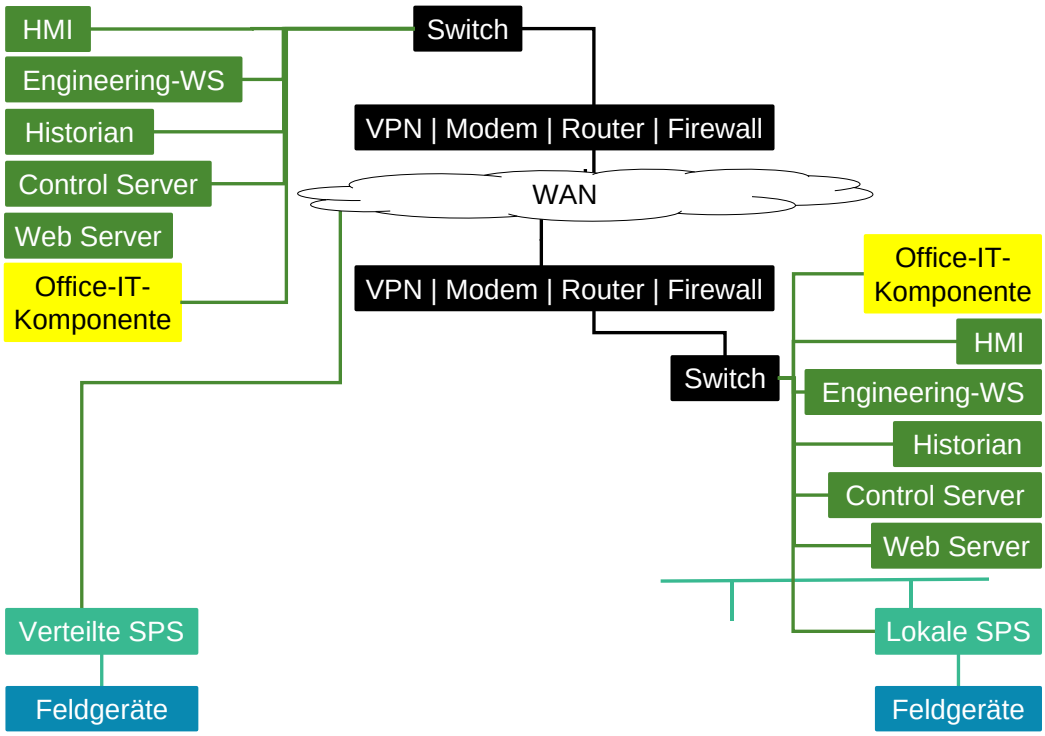


Abb. 4.7: Netzplan des Anwendungsfalls AR3: Gemeinsames LAN

4.6.4 Netzmanagement (Network Management & System Support, NM)

Die Anwendungsfallgruppe NM beschäftigt sich mit dem Management und der Konfiguration von Netzwerkgeräten und Netzverbindungen.

Dafür sind also Zielobjekte besonders die Netzwerkgeräte von Bedeutung und zusätzlich alle Netzverbindungen in den LANs. Welche Komponenten sie im Einzelnen verbinden, ist dabei nicht relevant. Deswegen werden HMI, Engineering-Workstation, Historian und ggf. Server in den Referenzarchitekturen zu dieser Anwendungsfallgruppe wieder verallgemeinert als Prozessleitkomponenten dargestellt. Auch SPSen und Feldgeräte werden einbezogen, da auch ihre Verbindungen konfiguriert werden müssen. Des Weiteren wird ein PC oder Mobilgerät (nicht unbedingt eine ICS-Komponente) betrachtet, auf dem Software für das Netzmanagement installiert ist. OPC kann wiederum die Kommunikation zwischen Geräten und Anwendungen unterschiedlicher Hersteller ermöglichen (siehe Abschnitt 4.4). Eine Übersicht der relevanten Zielobjekte findet sich in Tab. 4.5.

Tab. 4.5: Spezifische Zielobjektliste für die Anwendungsfallgruppe NM

Nr.	Zielobjekt
IT-Systeme	
IT1	Feldgerät
IT2	SPS
IT 3-6	Prozessleitkomponente
IT7	Mobilgerät
IT8	Externe Komponente
Anwendungen	
A6	Netzmanagement-Software
A7	OPC
Netzkomponenten	
N1	Switch
N2	Router
N3	Modem
N4	IT-Verkabelung
N5	Feldbus

Der Anwendungsfall **NM1: Lokales, individuelles Netzmanagement** (Abb. 4.8) sieht vor, dass das Netzmanagement auf jeder Komponente einzeln und jeweils nur für diese Komponente und ihre eigenen Netzverbindungen erfolgt. Je nach Art der Komponente kann die erforderliche Software auf der Komponente selbst installiert sein oder auf einem direkt mit der Komponente verbundenen Mobilgerät oder PC. Verbindungen für das Netzmanagement werden pinkfarben dargestellt (siehe Legende in Abb. 4.4)

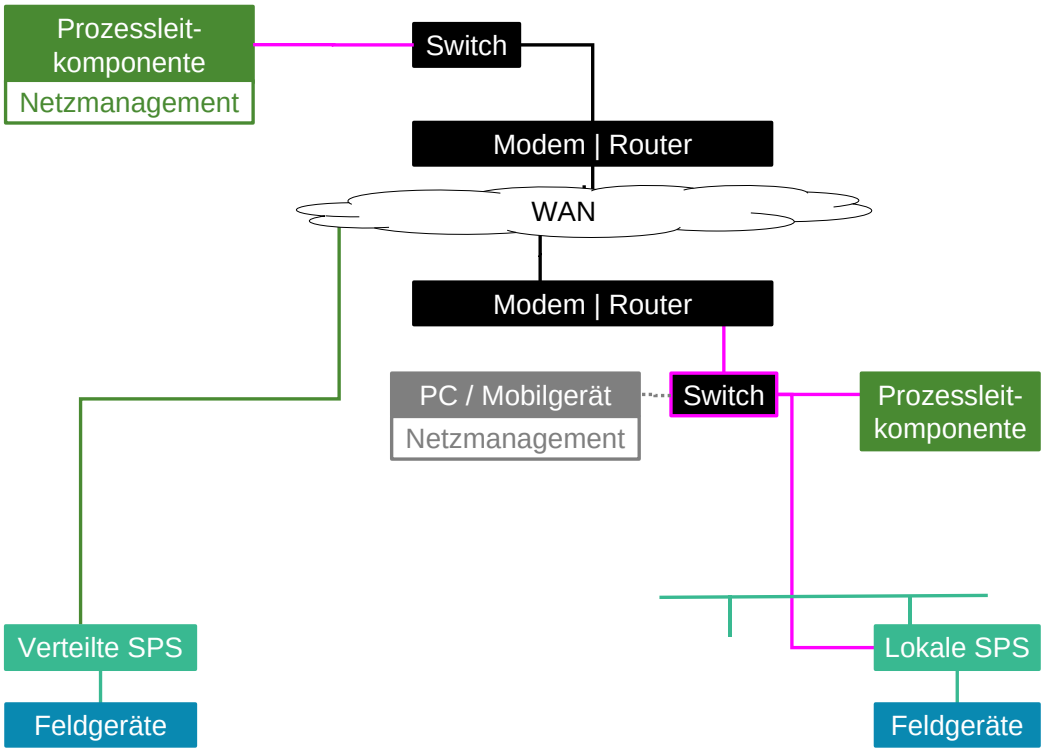


Abb. 4.8: Netzplan des Anwendungsfalls NM1: Lokales, individuelles Netzmanagement

Beim Anwendungsfall **NM2: Lokales, zentralisiertes Netzmanagement** (Abb. 4.9) erfolgt das Netzmanagement von einer Komponente aus für ein ganzes LAN mitsamt aller Netzwerkgeräte und Netzverbindungen.

Der Anwendungsfall **NM3: Fern-Netzmanagement** (Abb. 4.10) zu guter Letzt deckt den Fall ab, dass das Netzmanagement von einer zentralen Komponente aus über ein WAN hinweg für alle ICS-Netze gemeinsam erfolgt.

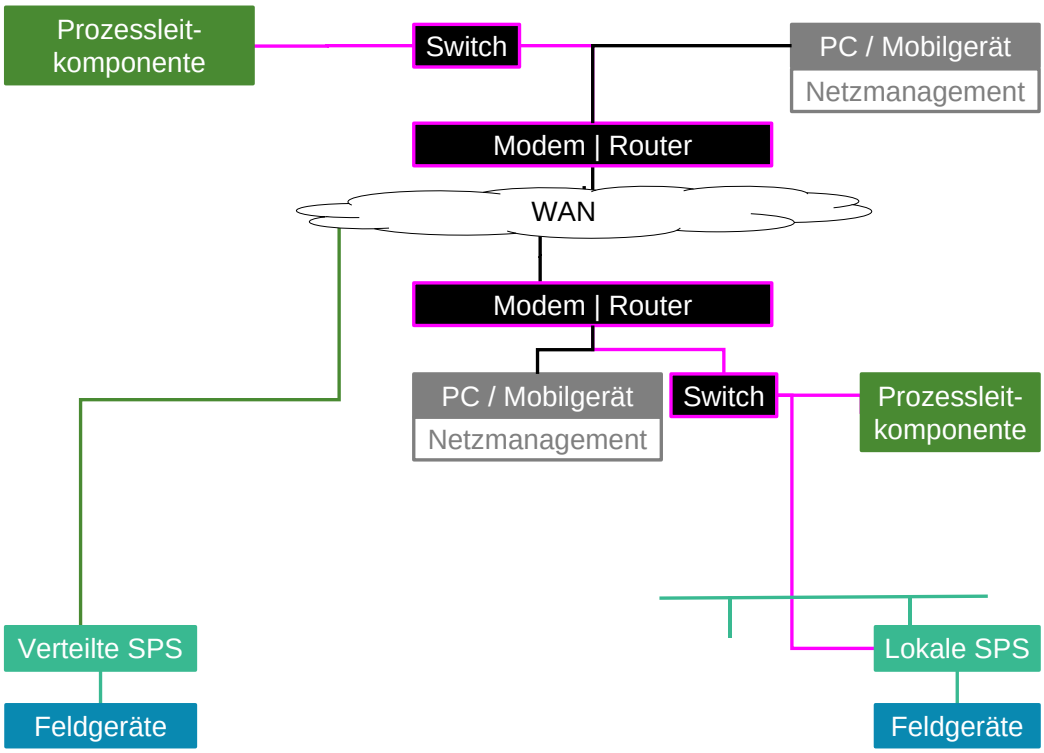


Abb. 4.9: Netzplan des Anwendungsfalls NM2: Lokales, zentralisiertes Netzmanagement

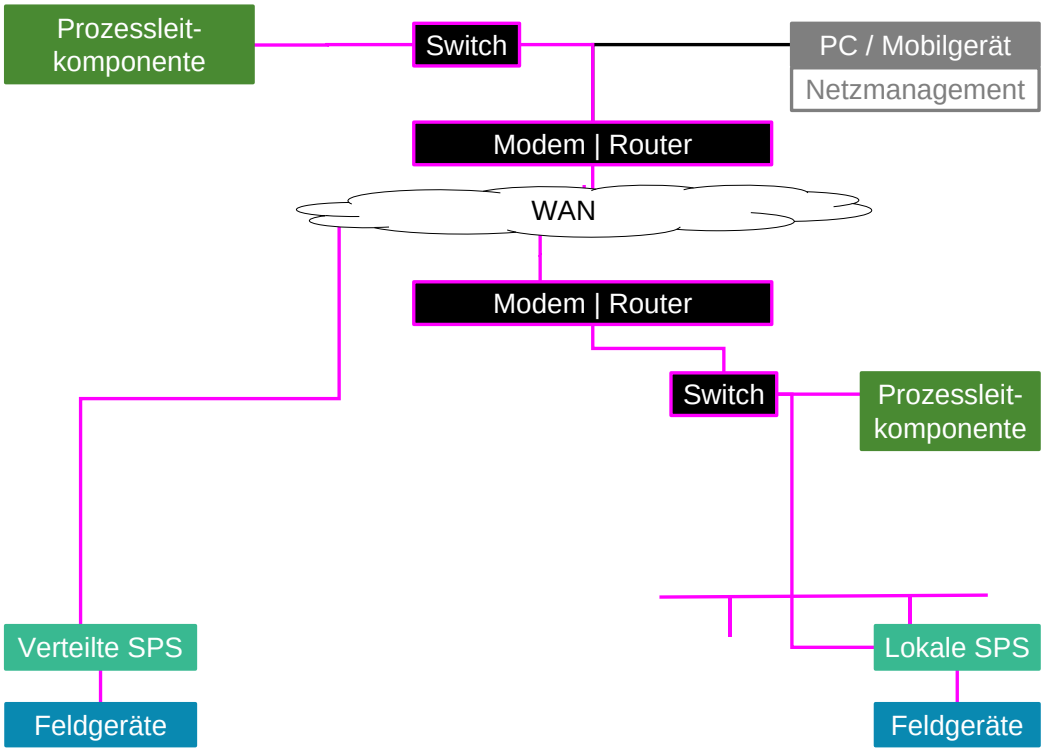


Abb. 4.10: Netzplan des Anwendungsfalls NM3: Fern-Netzmanagement

4.6.5 Benutzerzugang (User Access, UA)

Die Anwendungsfallgruppe UA befasst sich mit den Möglichkeiten, wie ein Nutzer auf das Leitsystem zugreifen kann. Unter „Zugriff auf das Leitsystem“ wird hier der Zugang zum HMI verstanden, denn von hier können aktuelle Systemzustände eingesehen und beeinflusst werden. Für die Programmierung der SPS ist eine eigene Anwendungsfallgruppe vorgesehen, siehe Abschnitt 4.6.7.

Relevante Komponenten für diese Anwendungsfallgruppe sind deswegen Steuerungen mit den darauf laufenden SPS-Programmen (denn darauf wird zugegriffen) und alle Komponenten mit HMI-Software (denn diese können zugreifen). In den ersten beiden Anwendungsfällen ist HMI-Software nur auf dem HMI selbst installiert, in den beiden darauffolgenden wird auch HMI-Software auf externen Komponenten betrachtet und im letzten Anwendungsfall erfüllt ein Webserver mit einem Webdienst im Browser die HMI-Funktionen. OPC kann bei der Kommunikation zwischen Komponenten verschiedener Hersteller unterstützen (siehe Abschnitt 4.4). Für die Betrachtung des Benutzerzugangs ist außerdem die physische Infrastruktur, also die Verortung der Komponenten in Räumlichkeiten, sehr wichtig.

Als Sicherheitskomponenten sind für die Absicherung des Nutzerzugriffs vor allem Firewalls und bei Kommunikation über ein WAN auch VPN-Verbindungen relevant.

Die spezifische Zielobjektliste findet sich in Tab. 4.6.

Tab. 4.6: Spezifische Zielobjektliste der Anwendungsfallgruppe UA

Nr.	Zielobjekt
IT-Systeme	
IT2	SPS
IT3	HMI
IT6	Server
IT8	Externe Komponente
Anwendungen	
A2	SPS-Programm
A3	HMI-Software
A5	Webdienst
A7	OPC
Infrastruktur	
IN1	Leitstand
IN2	Büro
IN3	Serverraum
IN4	Schutzschrank
IN5	Mobiler Arbeitsplatz
IN6	Feld
Sicherheit	
S1	Firewall
S2	VPN

Im Anwendungsfall **UA1: Systemzugriff vom Leitstand aus** (Abb. 4.11) wird angenommen, dass das HMI in einer Räumlichkeit steht, die zur Institution gehört, nur Leitstandsfunktionalitäten enthält und physisch abgesichert ist (zum Beispiel abgeschlossen und / oder mit Zugangskontrolle). In der Referenzarchitektur wird diese Räumlichkeit als grün hinterlegter „Leitstand mit Zugangskontrolle“ gekennzeichnet. Der Bereich der SPSen, Feldgeräte (und zu steuernden Maschinen) wird türkis hinterlegt und als „Feld“ bezeichnet.

Der Datenaustausch erfolgt in beide Richtungen und teils automatisiert, teils interaktiv: Die SPSen und Feldgeräte senden automatisch aktuelle Systemzustände, vom HMI aus können Benutzer interaktiv ins System eingreifen (zum Beispiel neue Sollwerte setzen oder Aktoren direkt ansteuern).

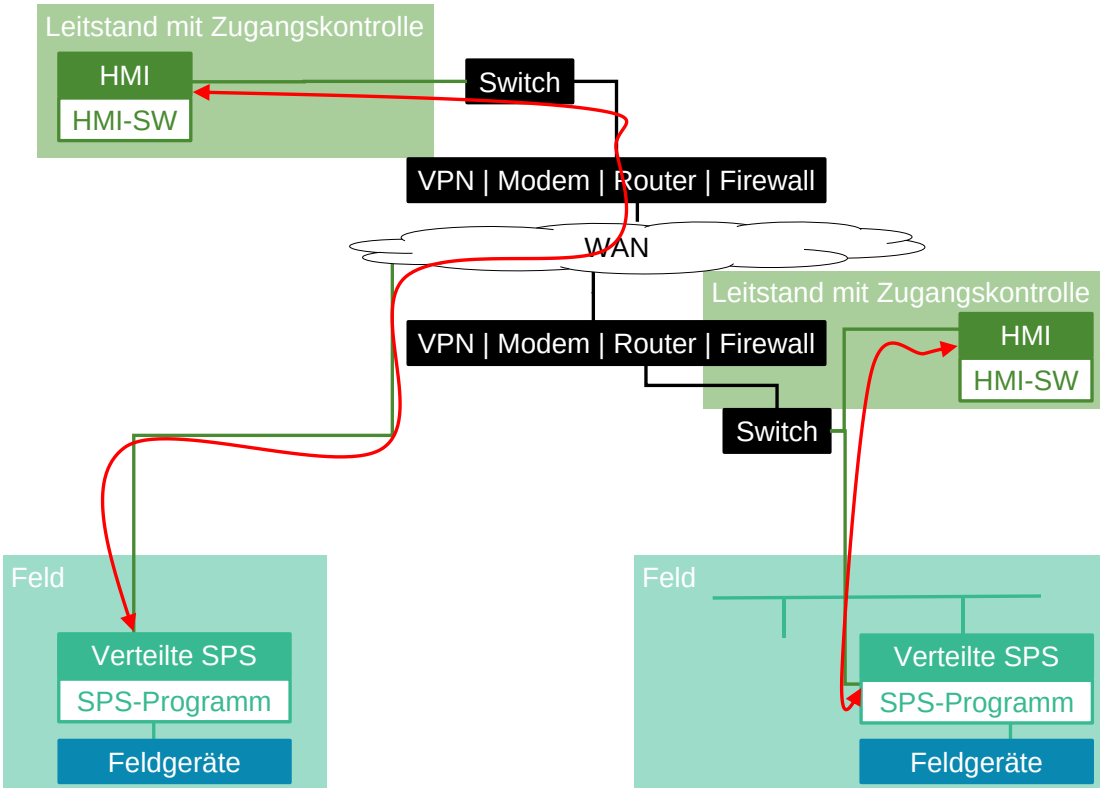


Abb. 4.11: Netzplan des Anwendungsfalls UA1: Systemzugriff vom Leitstand aus

Beim Anwendungsfall **UA2: Systemzugriff von der Anlage aus** wird ebenfalls ein Systemzugriff von dedizierten, in der eigenen Institution verorteten HMIs, angenommen. Allerdings stehen diese HMIs nicht in Leitständen mit Zugangskontrolle, sondern irgendwo auf dem Gebiet der verteilten oder lokalen Anlagen. Als „Anlage“ werden hier alle Räumlichkeiten des ICS-Betreibers zusammengefasst, egal ob Feld oder Büroräume, und blau hinterlegt. In der Referenzarchitektur ist angenommen, dass das HMI des zentralen Leistands in normalen Büros ohne besondere Zugangskontrolle (hellgrün) steht, das HMI des lokalen Leitstands ebenfalls ohne besondere Zugangskontrolle irgendwo in der Anlage (beispielsweise im Feld).

Der Datenaustausch erfolgt wie in UA1 in beide Richtungen.

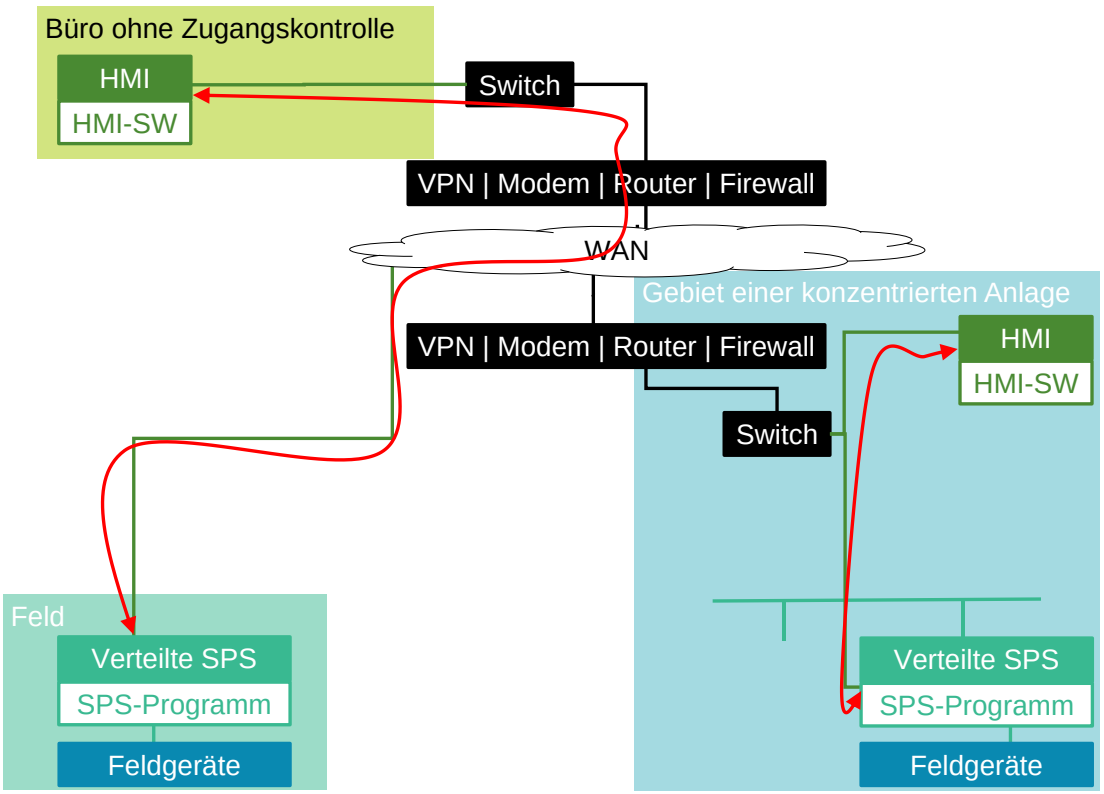


Abb. 4.12: Netzplan des Anwendungsfalls UA2: Systemzugriff von der Anlage aus

Für den Anwendungsfall **UA3: Fernzugriff** (Abb. 4.13) wird angenommen, dass die HMI-Software (auch) auf einer externen Komponente installiert ist, die sich nicht im Besitz und nicht auf dem Anlagengebiet des ICS-Betreibers befindet, sondern in einem in Abb. 4.13 als grau hinterlegten „externen Gebiet“. Die externe Komponente kann über ein WAN direkt auf die interne HMI-Funktionalität zugreifen. Ihr Nutzer hat dieselben Möglichkeiten wie ein Nutzer des internen HMIs: Er kann Systemzustände auslesen und interaktiv in das System eingreifen. Dafür kann das externe System entweder die zur Anlage gehörigen HMI-Funktionalitäten nutzen, die die Befehle dann automatisch an die Steuerungen weiterleiten (in Abb. 4.13 dargestellt) oder direkt auf das Steuerungssystem zugreifen.

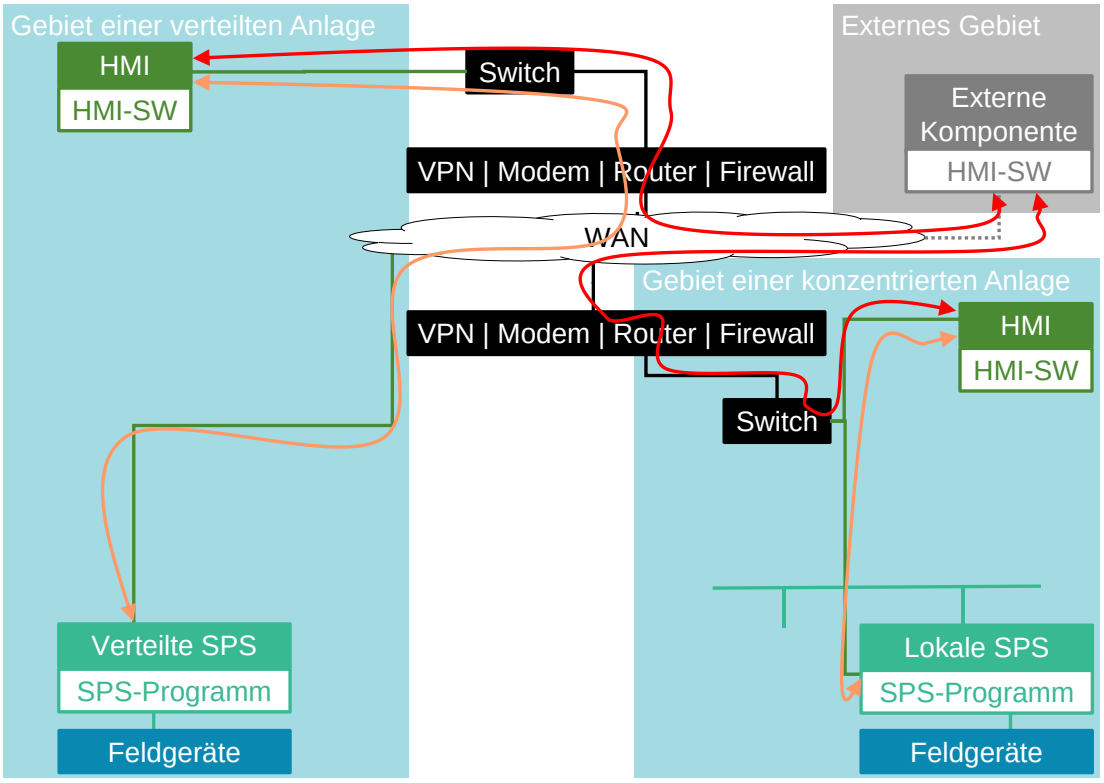


Abb. 4.13: Netzplan des Anwendungsfalls UA3: Fernzugriff

Der Anwendungsfall **UA4: Rein lesender Fernzugriff** (Abb. 4.14) entspricht dem Anwendungsfall UA3; jedoch erhält das externe HMI hier nur aktuelle Informationen über Systemzustände und kann selbst nicht ins System eingreifen.

Der Anwendungsfall **UA5: Rein lesender Fernzugriff im Webbrowser** (Abb. 4.15) wiederum entspricht dem Anwendungsfall UA4 mit dem Unterschied, dass ein Webdienst bereitgestellt wird, sodass die Systemzustände prinzipiell von jedem Rechner aus in einem Webbrowser angesehen werden können. Eine Installation der HMI-Software auf dem Zielrechner ist dann nicht mehr nötig. Dafür wird, wie in Abb. 4.15 dargestellt, ein Webserver eingerichtet, der Kopien der Systemzustände aus dem HMI erhält, auf die der Webdienst dann zugreifen kann.

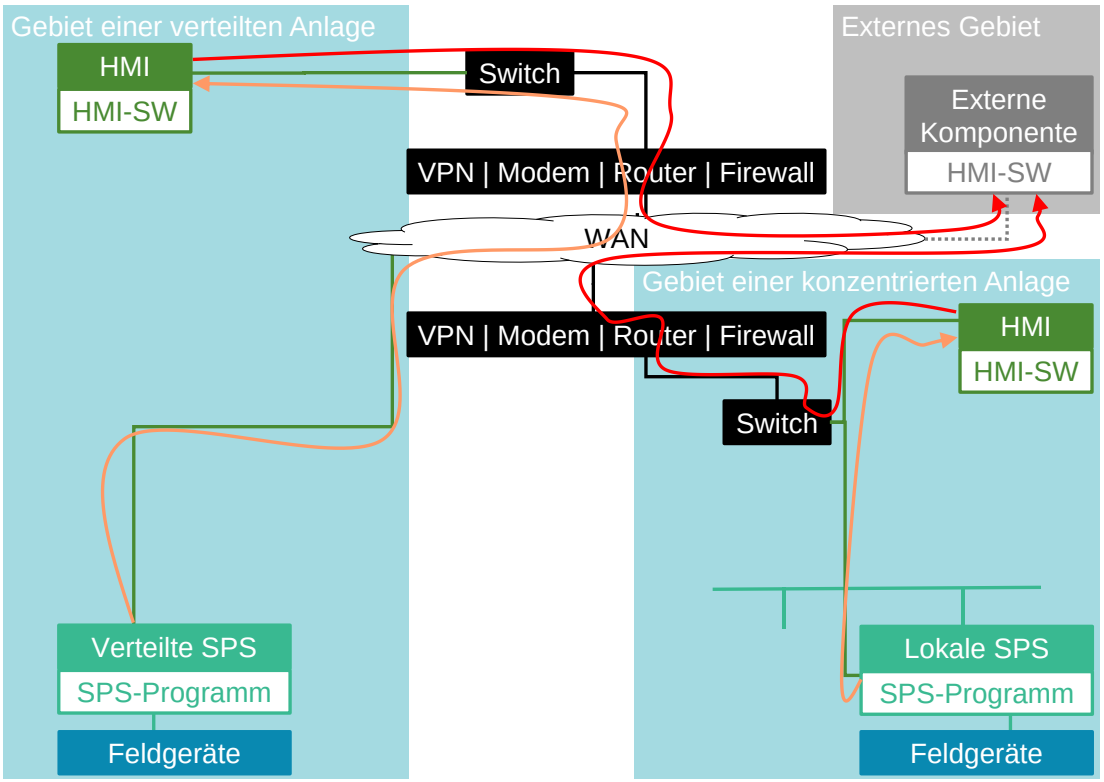


Abb. 4.14: Netzplan des Anwendungsfalls UA4: Rein lesender Fernzugriff

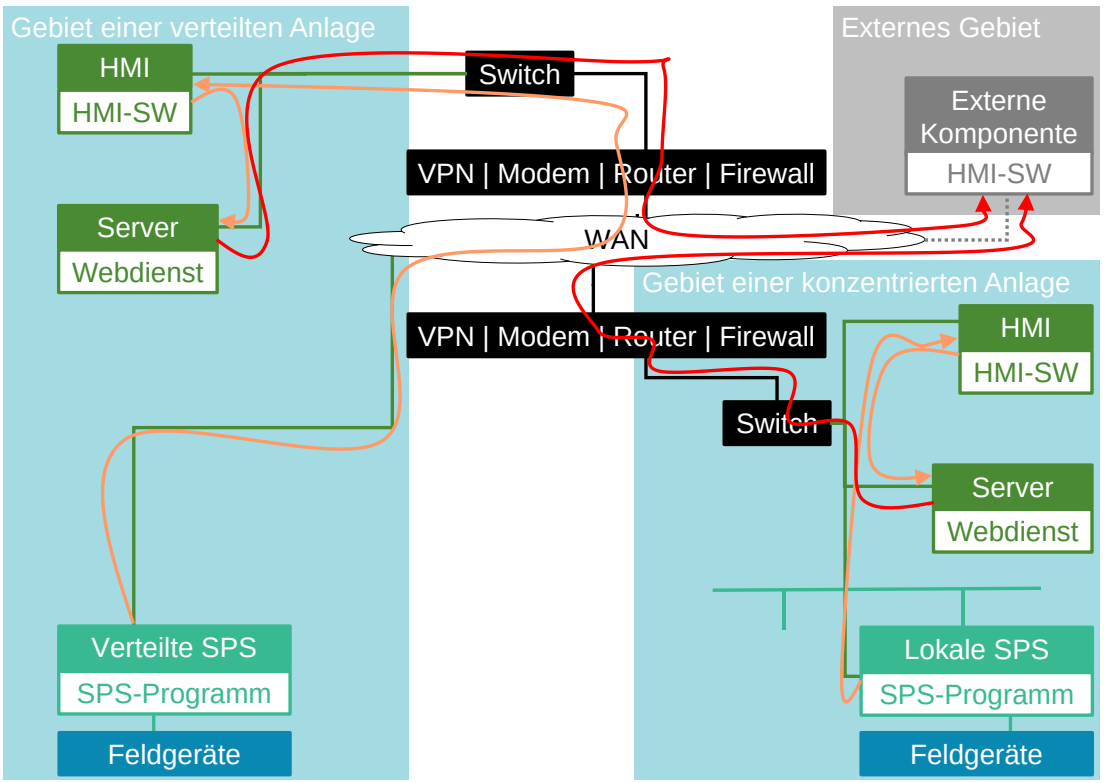


Abb. 4.15: Netzplan des Anwendungsfalls UA5: Rein lesender Fernzugriff im Webbrowser

4.6.6 Programmzugriff (Program Access, PA)

Die Anwendungsfallgruppe PA beschäftigt sich mit damit, welche Anwendungen (automatisiert oder interaktiv) auf welche Daten zugreifen können.

Dafür zählen – je nach Anwendungsfall – verschiedenste Anwendungen und Komponenten mitsamt Daten zu den Zielobjekten (eine Übersicht findet sich in Tab. 4.7).

Dazu zählen das HMI mitsamt Betriebssystem, Antivirenprogramm, Softwarelizenzen und HMI-Software, die Engineering-Workstation mit Betriebssystem (Operating System, OS), Antivirenprogramm (AV), Softwarelizenzen und Engineering-Software, der Historian mit Betriebssystem, Antivirenprogramm, Softwarelizenzen und einer Datenbanksoftware, externe Komponenten mit Mailprogrammen, SMS oder (Update-)Dateien, Mobilgeräte (Laptops, Tablets oder Smartphones von Mitarbeitern des ICS-Betreibers) mit Mailprogrammen oder SMS, SPSen mit Firmware, Alarmfunktionalitäten per Mail oder SMS, sowie Netzmanagementprotokolle wie SNMP und Syslog auf allen Komponenten. OPC unterstützt gegebenenfalls bei der Kommunikation zwischen Geräten unterschiedlicher Hersteller (siehe Abschnitt 4.4). Eine Firewall kann unerwünschte Programmen und Diensten den Zugriff verweigern.

Tab. 4.7: Spezifische Zielobjektliste für die Anwendungsfallgruppe PA

Nr.	Zielobjekt
IT-Systeme	
IT2	SPS
IT3	HMI
IT4	Historian
IT5	Engineering-Workstation
IT8	Externe Komponente
Anwendungen	
A1	Engineering-Software
A2	SPS-Programm
A3	HMI-Software
A4	Datenbank
A5	Webdienst
A6	Netzmanagement-Software
A7	OPC
A8	Mail, SMS, Instant Messaging
A9	Betriebssystem
Netzkomponenten	
N1	Switch
N2	Router
N3	Modem
Sicherheit	
S1	Firewall
S4	Antiviren-Software

Der erste Anwendungsfall **PA1: Automatisiertes Senden von Nachrichten** (Abb. 4.16) befasst sich mit Nachrichten per E-Mail oder SMS, die die Steuergeräte automatisiert versenden. Ein häufiges Einsatzszenario sind Alarme bei nicht gewollten Betriebszuständen, etwa das Überhitzen eines Motors oder das Volllaufen eines Behälters. Die Nachrichten können an interne HMIs im lokalen oder zentralen Leitstand und Mobilgeräte des ICS-Betreibers, aber auch an externe Komponenten gerichtet sein.

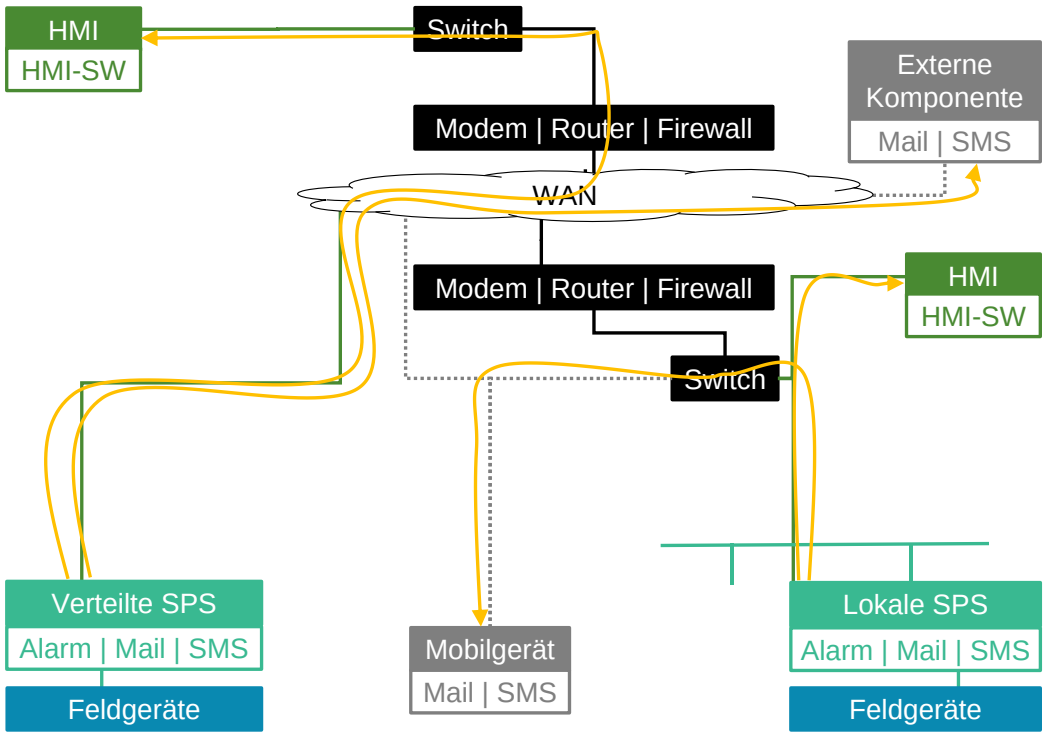


Abb. 4.16: Netzplan des Anwendungsfalls PA1: Automatisiertes Senden von Nachrichten

Der Anwendungsfall **PA2: Interaktives Senden von Dateien** (Abb. 4.17) behandelt das Szenario, dass Mitarbeiter interaktiv über das WAN Dateien an eine externe Komponente versenden. Dabei findet das Versenden aus dem ICS-Netz heraus, also von einer ICS-Komponente aus statt. Beispiele sind das Versenden von Archivdaten, Engineering-Daten oder HMI-Daten vom Historian, einer Engineering-WS oder dem HMI aus.

Der Anwendungsfall **PA3: Interaktives Empfangen von Dateien** (Abb. 4.18) entspricht dem Anwendungsfall PA2 mit dem Unterschied, dass in diesem Fall ein Nutzer der externen Komponente eine Datei über das WAN an eine Komponente im ICS-Netz versendet.

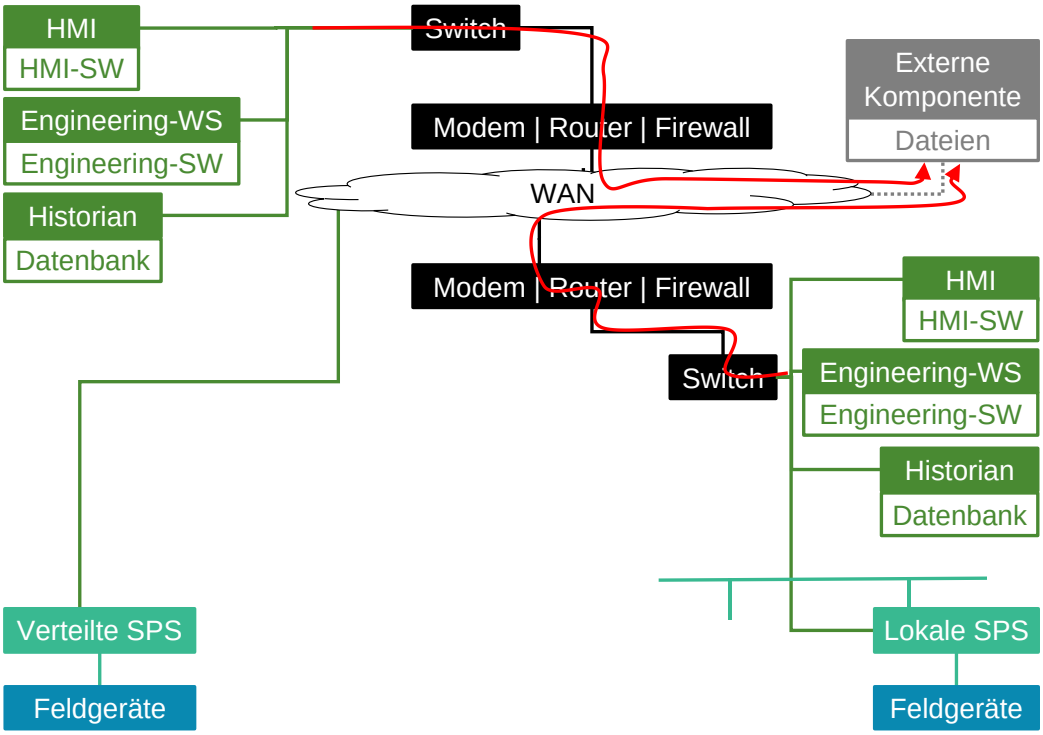


Abb. 4.17: Netzplans des Anwendungsfalls PA2: Interaktives Senden von Dateien

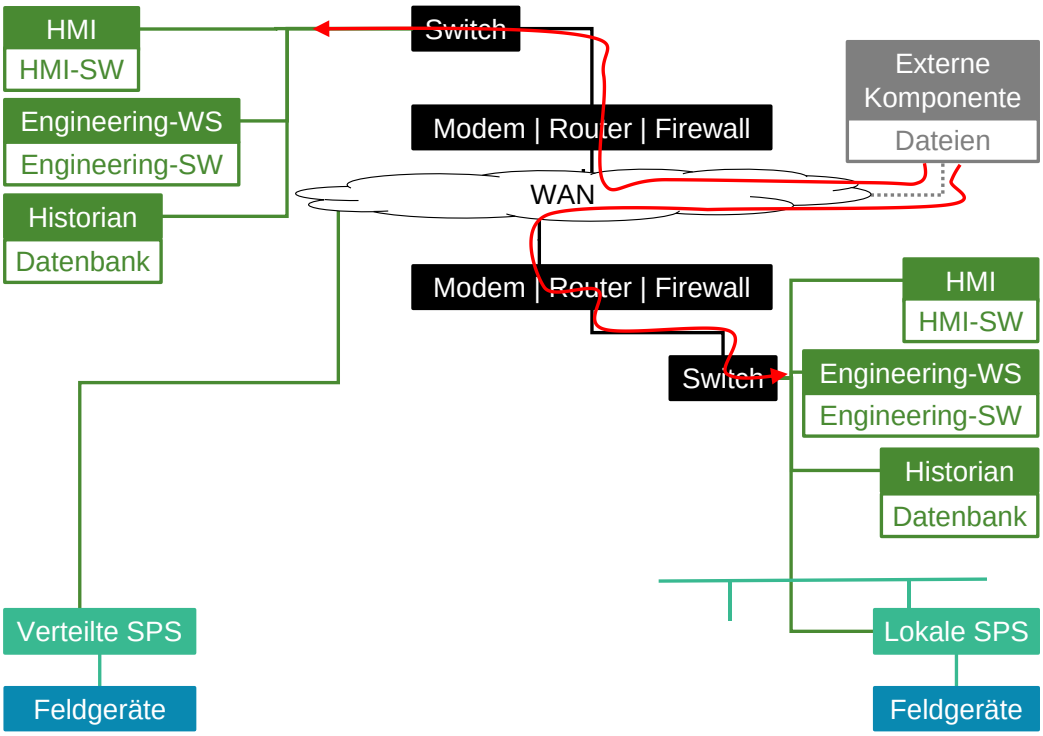


Abb. 4.18: Netzplan des Anwendungsfalls PA3: Interaktives Empfangen von Dateien

Der Anwendungsfall **PA4: Automatisierte Software-Updates** (Abb. 4.19) beschäftigt sich mit Patches und Updates für Betriebssysteme (Operating Systems, OS) oder SPS-Firmware, Signaturen für Antivirenprogramme (AV) oder aktuellen Softwarelizenzen, die die ICS-Komponenten automatisiert von einer externen Quelle über ein WAN herunterladen. Hier können potenziell alle ICS-Komponenten betroffen sein. Die Besonderheit dieses Anwendungsfalles im Vergleich zu den anderen Anwendungsfällen der Gruppe PA ist, dass nicht nur Daten, sondern potenziell ausführbare Dateien (die sich auch selbst installieren) übermittelt werden.

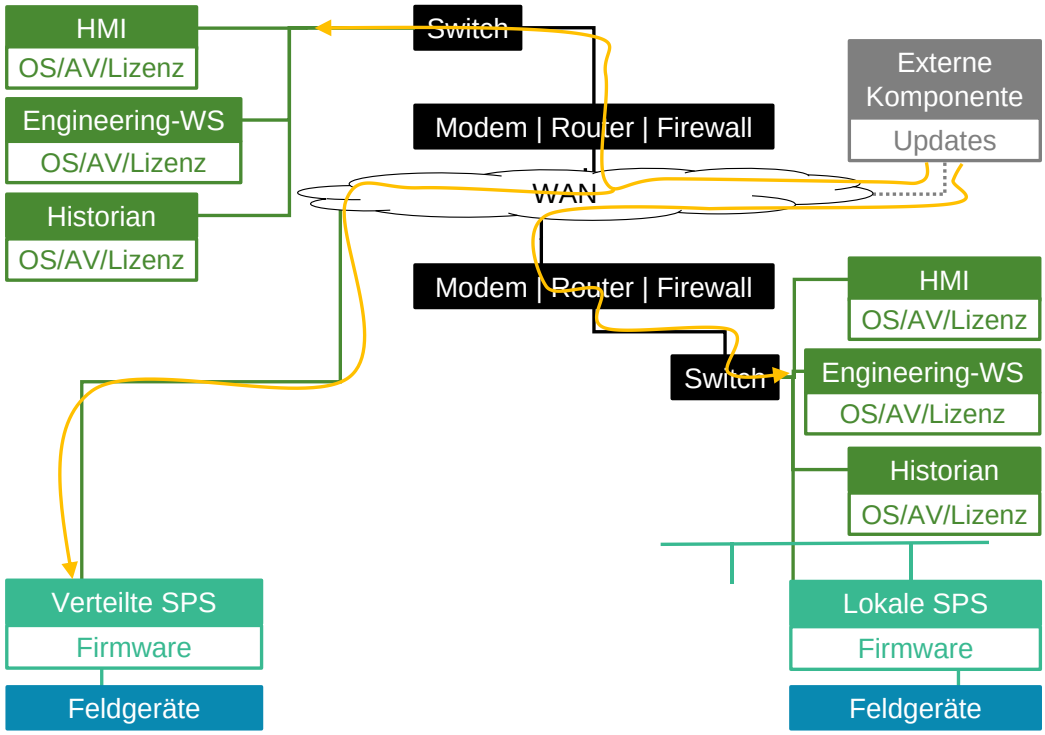


Abb. 4.19: Netzplan des Anwendungsfalls PA4: Automatisierte Software-Updates

Dies grenzt ihn auch vom Anwendungsfall **PA5: Automatisierter Datenaustausch** (Abb. 4.20) ab. Auch in diesem Fall werden automatisiert Daten ausgetauscht; jedoch nur Daten und keine ausführbaren Programme. Dafür betrachtet dieser Anwendungsfall einen Daten*austausch* (also in beide Richtungen) übers WAN zwischen einer externen Komponente und den ICS-LANs.

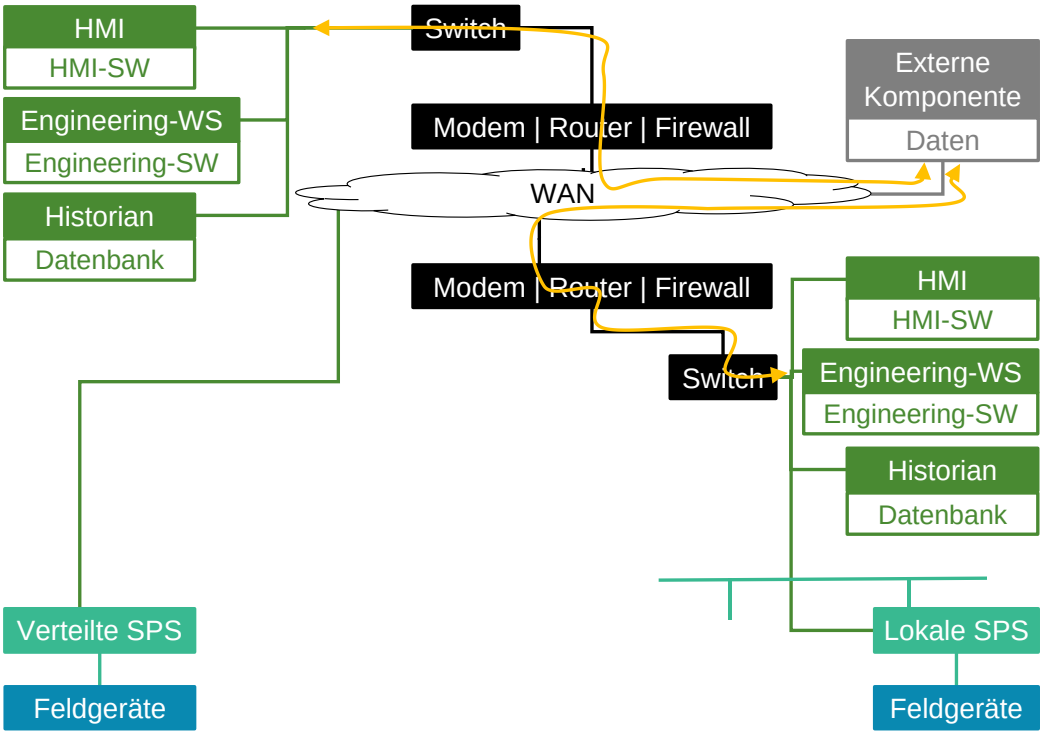


Abb. 4.20: Netzplan des Anwendungsfalls PA5: Automatisierter Datenaustausch

Der letzte Anwendungsfall der Gruppe PA ist der Fall **PA6: Automatisierter Datenaustausch für das Netzmanagement** (Abb. 4.21). Er beschäftigt sich mit dem automatisierten Datenaustausch von Netzmanagement-Dateien, etwa in Form von Logdateien (z.B. Syslog) oder Daten des Netzmanagementprotokolls SNMP, zwischen ICS-Komponenten oder Netzwerkgeräten und einer externen Komponente. Dieser Anwendungsfall legt dabei den Fokus nur auf den Datenaustausch. Das gesamte Netzmanagement behandelt die Anwendungsfallgruppe NM.

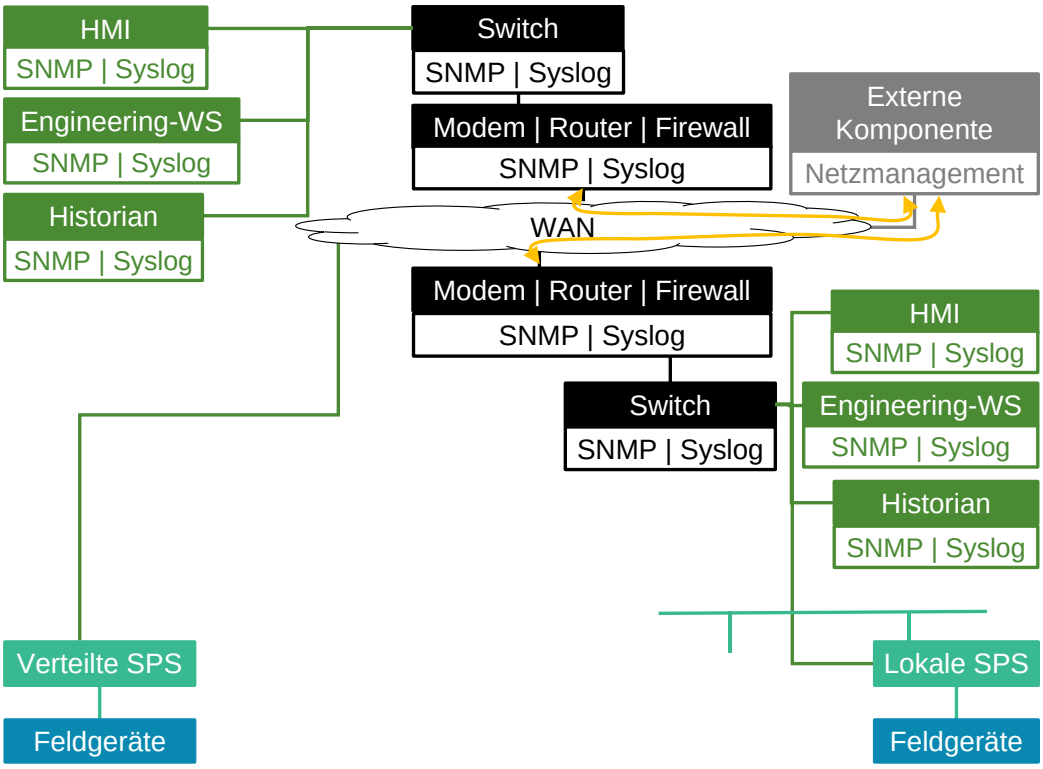


Abb. 4.21: Netzplan des Anwendungsfalls PA6: Automatisierter Datenaustausch für das Netzmanagement

4.6.7 SPS-Programmierung und -Wartung (PLC Programming and Maintenance, PLC)

Die Anwendungsfallgruppe PLC umfasst verschiedene Anwendungsfälle des schreibenden Zugriffs auf SPS-Programme. Das bedeutet, dass eine Komponente mit installierter Engineering-Software Zugriff auf die SPSen hat, um sie mit neuen Programmdateien zu bespielen. Da die SPS-Programme für die gesamte automatisierte Anlagensteuerung zuständig sind, haben diese Programme große Auswirkungen auf die von ihnen gesteuerten Prozesse.

Relevante Zielkomponenten für diese Anwendungsfallgruppe sind neben den SPSen mit ihren SPS-Programmen vor allem Engineering-Workstations und andere (externe oder mobile) Komponenten, auf denen Engineering-Software installiert ist. Externe Komponenten können auch für die Fernwartung verwendet werden. OPC kann für die Kommunikation zwischen Geräten und Anwendungen unterschiedlicher Hersteller sorgen (siehe Abschnitt 4.4). Als Sicherheitskomponenten sind VPN und Antiviren-Software berücksichtigt. Da eine Installation von Antiviren-Software auf SPSen nicht immer möglich ist (für genauere Informationen siehe Kapitel 5), ist diese in den Netzplänen bei SPSen mit einem Fragezeichen gekennzeichnet. Für die spezifische Zielobjektliste siehe Tab. 4.8.

Tab. 4.8: Spezifische Zielobjektliste für die Anwendungsfallgruppe PLC

Nr.	Zielobjekt
IT-Systeme	
IT2	SPS
IT5	Engineering-Workstation
IT7	Mobilgerät
IT8	Externe Komponente
Anwendungen	
A1	Engineering-Software
A2	SPS-Programm
A7	OPC
Netzkomponenten	
N6	Fernwartung
Anwendungen	
A1	Engineering-Software
A2	SPS-Programm
A7	OPC
Sicherheit	
S2	VPN
S4	Antiviren-Software

Der Datenfluss erfolgt dabei in der Regel interaktiv und von der Engineering-Workstation zur SPS: Das fertig kompilierte Programm wird auf die SPS überspielt.

Dem Anwendungsfall **PLC1: Lokale, individuelle SPS-Programmierung** (Abb. 4.22) liegt die Annahme zugrunde, dass SPSen nur lokal programmiert werden können, indem ein (mobiles) Gerät vor Ort mit der jeweiligen SPS verbunden wird.

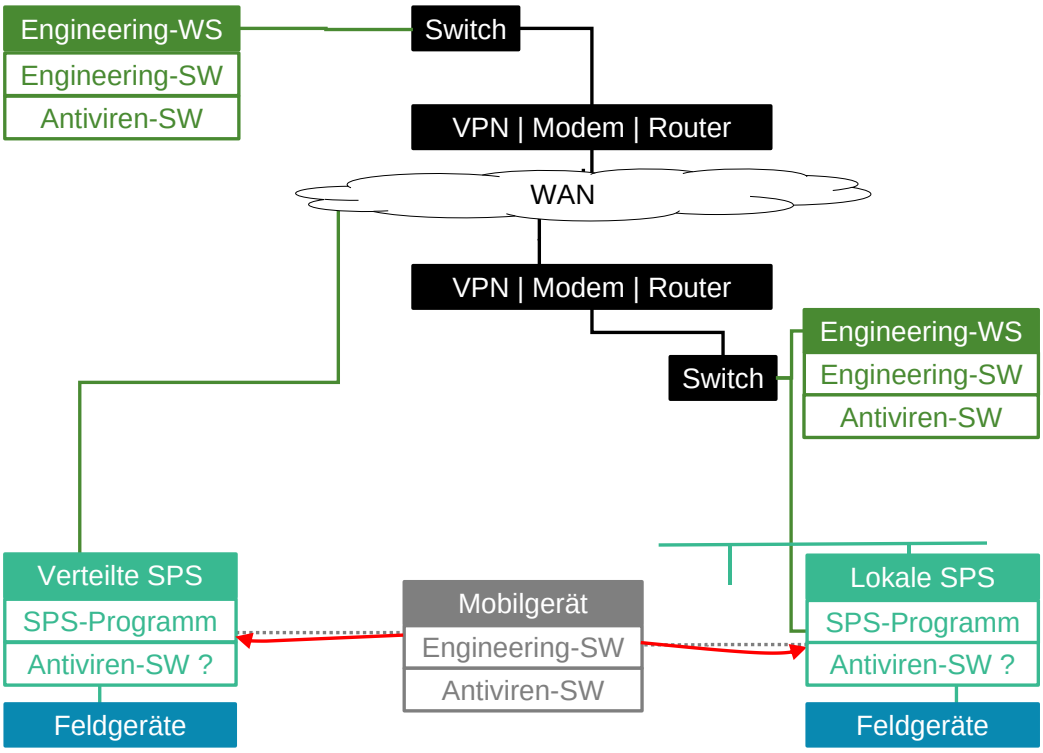


Abb. 4.22: Netzplan des Anwendungsfalls PLC1: Lokale, individuelle SPS-Programmierung und -Wartung

Auch beim Anwendungsfall **PLC2: Lokale, zentralisierte SPS-Programmierung** (Abb. 4.23) können SPSen nur lokal programmiert werden, jedoch von einer zentralen Engineering-Workstation aus, die die SPSen der gesamten lokalen Anlage programmiert.

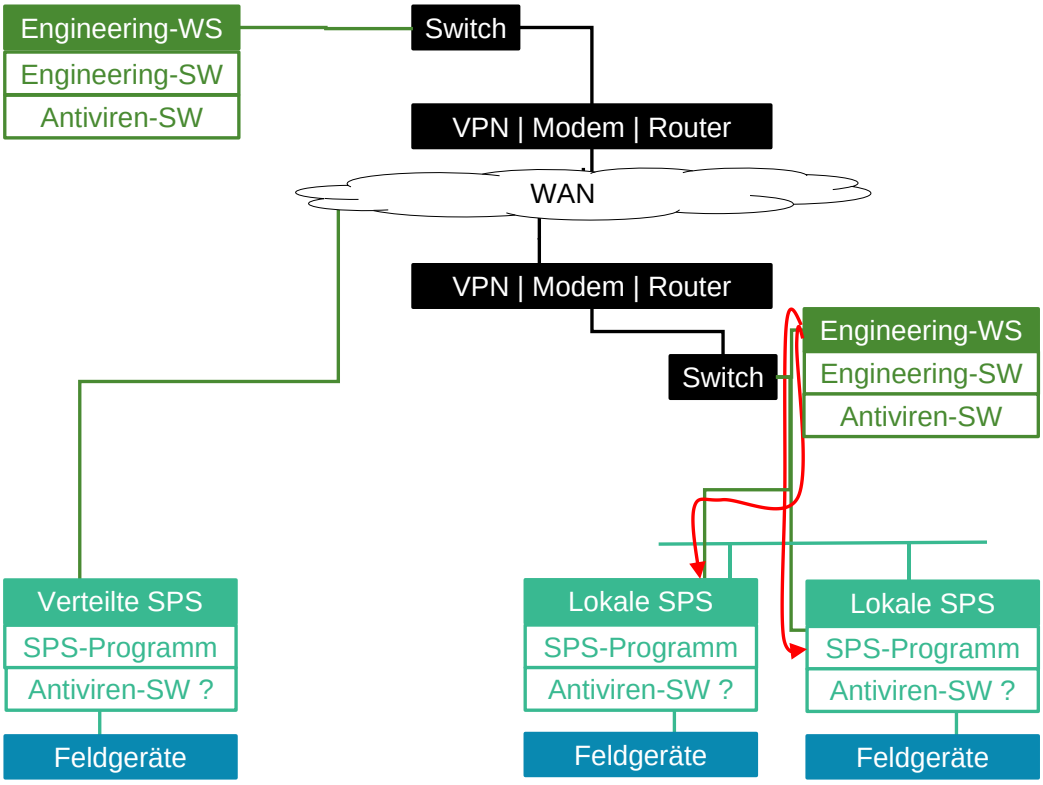


Abb. 4.23: Netzplan des Anwendungsfalls PLC2: Lokale, zentralisierte SPS-Programmierung und -Wartung

Der dritte Anwendungsfall **PLC3: SPS-Fernprogrammierung und -Fernwartung** (Abb. 4.24) schließlich deckt alle Fälle ab, in denen SPSen über ein WAN programmiert werden. Dies kann die Programmierung von einer Engineering-Workstation in der zentralen Leitwarte ebenso sein wie die Programmierung durch eine externe, durch ein WAN mit dem ICS-Netz verbundene Komponente.

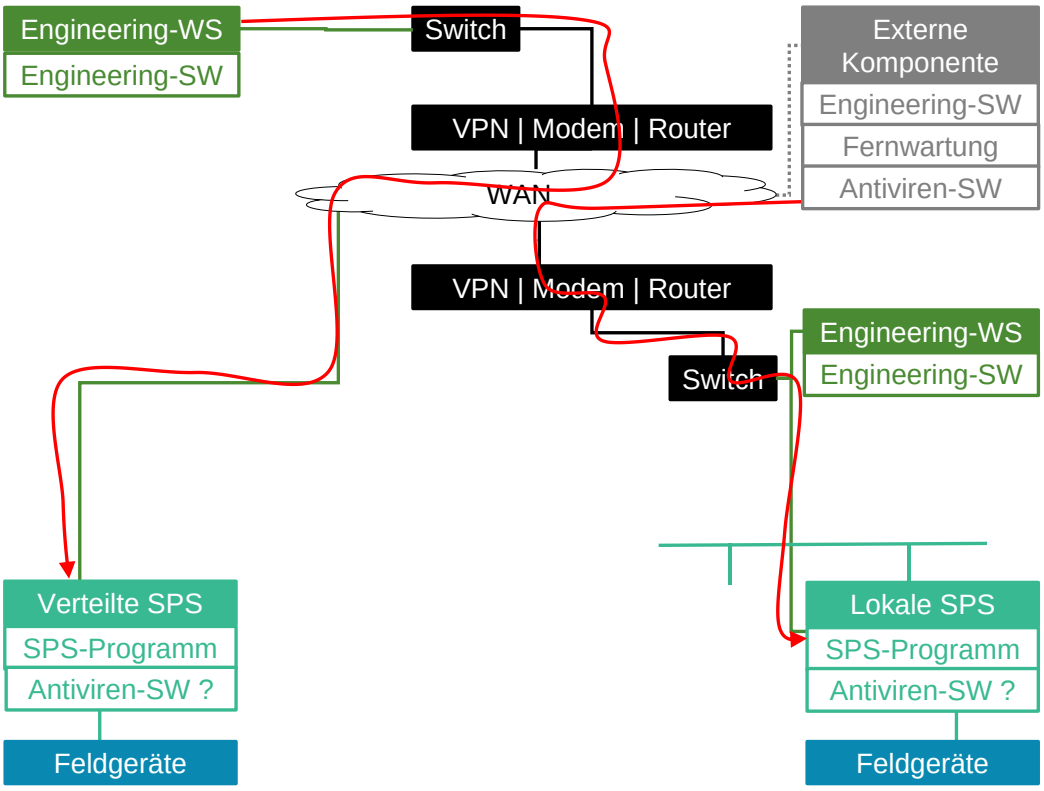


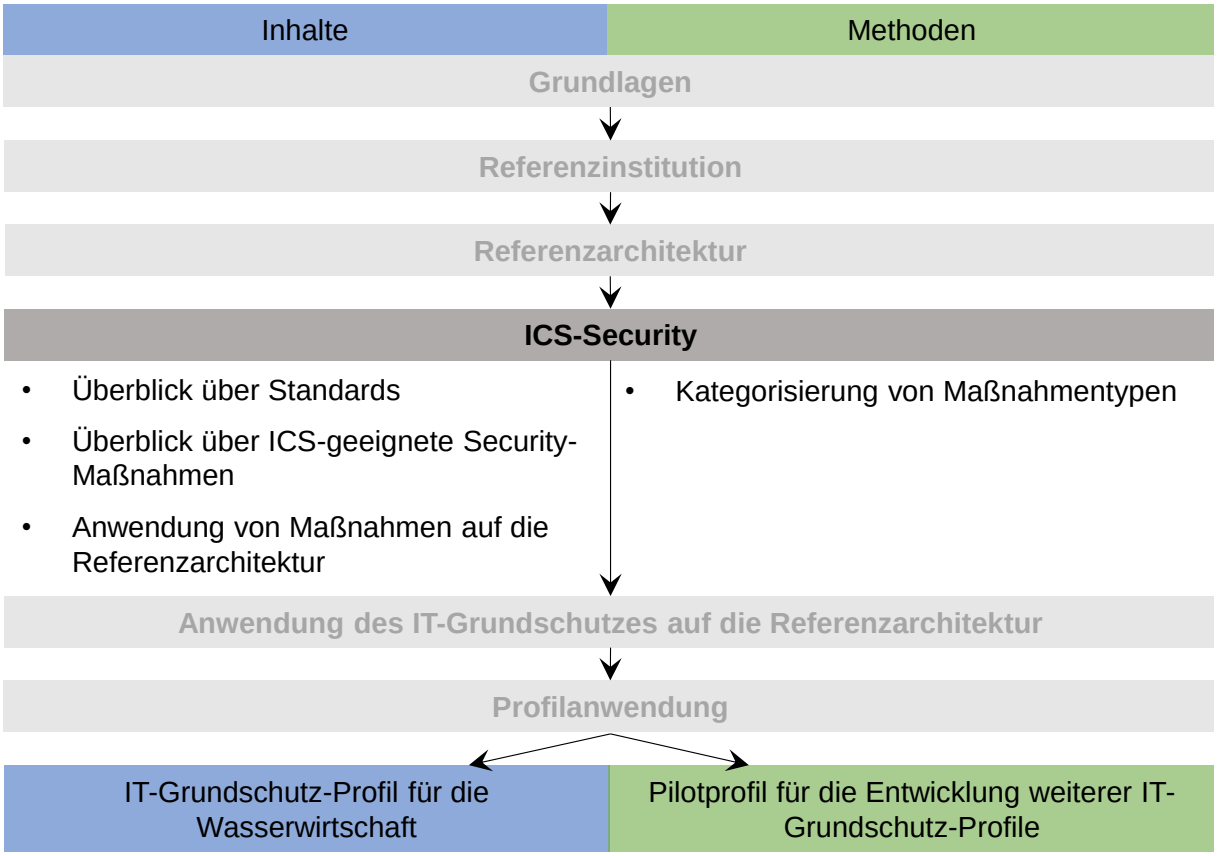
Abb. 4.24: Netzplan des Anwendungsfalls PLC3: SPS-Fernprogrammierung und -Fernwartung

Nachdem nun alle Anwendungsfälle im Einzelnen vorgestellt wurden, gibt Tab. 4.9 abschließend einen Überblick über alle Anwendungsfälle, in ihre Gruppen gegliedert. Angegeben sind neben den Kürzeln sowohl die englischsprachigen Gruppenbezeichnungen der AWWA als auch die deutsche Bezeichnung, die für die Unterprofile des in dieser Arbeit erstellten Profils verwendet wird.

Tab. 4.9: Übersicht über alle Anwendungsfälle, gruppiert nach Unterprofilen (Anwendungsfallgruppen)

Kürzel	Unterprofil-Bezeichnung	AWWA-Bezeichnung
AR	**Architektur**	**Architecture**
AR1	Dediziertes ICS-Netz	
AR2	Gemeinsames WAN	
AR3	Gemeinsames LAN	
NM	**Netzmanagement**	**Network Management & System Support**
NM1	Lokales, individuelles Netzmanagement	
NM2	Lokales, zentralisiertes Netzmanagement	
NM3	Fern-Netzmanagement	
UA	**Benutzerzugang**	**User Access**
UA1	Systemzugriff vom Leitstand aus	
UA2	Systemzugriff von der Anlage aus	
UA3	Fernzugriff	
UA4	Rein lesender Fernzugriff	
UA5	Rein lesender Fernzugriff im Webbrowser	
PA	**Programmzugriff**	**Programm Access**
PA1	Automatisiertes Senden von Nachrichten	
PA2	Interaktives Senden von Dateien	
PA3	Interaktives Empfangen von Dateien	
PA4	Automatisierte Software-Updates	
PA5	Automatisierter Datenaustausch	
PA6	Automatisierter Datenaustausch für das Netzmanagement	
PLC	**SPS-Programmierung und -Wartung**	**PLC Programming and Maintenance**
PLC1	Lokale, individuelle SPS-Programmierung und -Wartung	
PLC2	Lokale, zentralisierte SPS-Programmierung und -Wartung	
PLC3	SPS-Fernprogrammierung und -Fernwartung	

5 ICS-Security



Dieses Kapitel soll sinnvolle ICS-Security-Maßnahmen und die dahinterstehenden Grundprinzipien erläutern. Eine vollständige Beschreibung sinnvoller Maßnahmen und Prinzipien füllt ganze Bücher und Regelwerke und kann nicht Ziel dieses Kapitels sein. Stattdessen soll es einen strukturierten Überblick über ICS-Security geben, um die Referenzarchitektur aus Kapitel 4 mit Sicherheitskomponenten zu vervollständigen und zu verstehen, welche Maßnahmentypen in welchen Unterprofilen des in dieser Arbeit erstellten IT-Grundschutz-Profils relevant sind.

Zum Einstieg werden die wichtigsten Standards, Normen und Richtlinien für die ICS-Security zusammengefasst (Abschnitt 5.1).

Danach geht es tiefer ins Inhaltliche: Abschnitt 5.2 erklärt die Unterschiede zwischen IT-Security und ICS-Security, bevor in Abschnitt 5.3 grundlegende Prinzipien für ICS-Security und typische Maßnahmen dargestellt werden. Grundsätzlich bedient sich die ICS-Security ähnlicher Maßnahmen wie die IT-Security, jedoch liegen die Prioritäten bei der Anwendung anders. Deswegen wird stets die besondere Eignung (oder Nicht-Eignung) der vorgestellten Prinzipien und Maßnahmentypen für ICS-Security herausgestellt und begründet.

Der Fokus liegt auf Maßnahmen, die die übergreifende Architektur von ICS-Netzen betreffen, da in dieser Arbeit beispielhaft das Unterprofil für die Anwendungsfallgruppe Architektur (AR)

erstellt wird. In Abschnitt 5.4 werden die Architektur betreffende Maßnehmen konkret auf die AR-Referenzarchitekturen aus Kapitel 4 angewendet.

Jedes Unterprofil deckt einen bestimmten Aspekt der ICS-Sicherheit ab. Aus diesem Grund ist in jedem Unterprofil nur ein Ausschnitt der hier erwähnten sinnvollen Maßnahmentypen relevant. Eine Zuordnung der Maßnahmentypen zu den verschiedenen Unterprofilen erfolgt in Kapitel 6 in Abschnitt 6.2.

5.1 Standards, Normen und Richtlinien

In diesem Abschnitt wird ein Überblick über die wichtigsten Standards mit Bezug zur ICS-Security gegeben. Dabei soll insbesondere verdeutlicht werden, wie sich der IT-Grundschutz, zu dessen Modernisierung diese Arbeit beiträgt, in die nationale und internationale Normenlandschaft einfügt. Grundsätzlich gilt, dass bei der Erstellung des IT-Grundschutzes die internationalen Standards und Best Practices einbezogen werden. Die vorgestellten Standards sind also keineswegs als gänzlich voneinander unabhängige „Insellösungen“ zu betrachten.

Standards zur IT-Security sind zahlreich. In verschiedenen Ländern, verschiedenen Branchen, von verschiedenen Organisationen gibt es verschiedene Richtlinien; manche mit verpflichtendem, viele nur mit empfehlendem Charakter. An dieser Stelle muss deshalb eine Auswahl getroffen werden.

Dieser Abschnitt beschränkt sich auf die Standards, die

- konkrete Vorgehensweisen und Maßnahmen empfehlen und / oder
- sich explizit mit der Sicherheit von ICS beschäftigen und / oder
- grundlegend für andere Standards sind, die sich explizit mit ICS beschäftigen und /oder
- häufig angewendet oder von anderen Standards oder Dokumenten referenziert werden.

Der Fokus bei der Auswahl liegt dabei entsprechend des Schwerpunkts dieser Arbeit auf Standards, die sich an kritische Infrastrukturen und / oder die Wasserwirtschaft richten. Deutsche und insbesondere BSI-Dokumente werden detaillierter berücksichtigt, da sie für diese Arbeit von besonderer Relevanz sind. Internationale und US-amerikanische Standards dienen häufig als Vorbilder beziehungsweise Grundlagen für ihre deutschen Pendants.

5.1.1 International

5.1.1.1 ISO / IEC

Die International Organization for Standardization (ISO) legt internationale Normen in allen Bereichen fest. Die International Electrotechnical Commission (IEC) ist ihr Pendant für den Bereich Elektrotechnik und Elektronik. Beide Organisationen haben ihre Sitze in der Schweiz [ISO17; IEC17]. ISO-Standards sind kostenpflichtig.

Die **Normenreihe ISO / IEC 27000** ist für die Informationssicherheit reserviert. In der ISO / IEC 27001 werden allgemeine Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) formuliert. Der IT-Grundschutz stellt eine Umsetzung dieser Anforderungen dar (siehe auch Abschnitt 2.2.1.1). Die ISO / IEC 27002 enthält Basisanforderungen für die Umsetzung eines ISMS und wird von vielen anderen internationalen Standards referenziert. Sie verweist auch selbst auf andere internationale Standards. Die Norm enthält über 100 potenzielle Sicherheitsmaßnahmen; darunter technische genauso wie organisatorische Maßnahmen [KL15].

Die 27000-Reihe ist keine ICS-spezifische Normenreihe, sondern kann auf alle Institutionen angewendet werden. Es existieren branchenspezifische Richtlinien für die Energieversorgung (ISO / IEC 27019), die Telekommunikation (ISO / IEC 27011) und den Gesundheitssektor (ISO / IEC 27709) [BSI13].

Die Besonderheit von ISO27001 ist, dass nach dieser Norm zertifiziert werden kann (auch die Zertifizierung mittels IT-Grundschutz basiert auf dem ISO-27001-Zertifikat). Sie ist international populär und ermöglicht multinationalen Unternehmen Sicherheitszertifikate, die in mehreren Ländern akzeptiert werden [Fra10].

Die Vorgehensweise der ISO 27000-Reihe unterscheidet sich grundlegend von der des IT-Grundschutzes. Während die Anwendung des IT-Grundschutzes sich an der IT-Struktur der Anwender orientiert (siehe Abschnitt 2.2), müssen Anwender bei der Anwendung der ISO zunächst eine Risikoanalyse durchführen, wobei das Schutzniveau eigenständig festgelegt werden kann. Nur für vorhandene Risiken müssen dann Maßnahmen implementiert werden [Kre15]. Der IT-Grundschutz hingegen legt einen normalen Schutzbedarf fest und nimmt dem durchschnittlichen Anwender damit die Risikoanalyse ab (siehe Abschnitt 2.2).

Gegenüber IT-Grundschutz ist die ISO 27000-Reihe außerdem kompakter: ISO 27001 (allgemeine Anforderungen an ein ISMS) und ISO 27002 (konkretere Best Practices) kommen gemeinsam auf etwa 150 Seiten, die bisherigen IT-Grundschutz-Kataloge auf etwa 5000. Die „Controls“ der ISO-Norm sind weniger konkret formuliert als die Maßnahmen des IT-Grundschutzes [Fra10].

Beide Systeme, sowohl das des ISO-Standards als auch das des IT-Grundschutzes, haben Vor- und Nachteile: Die ISO 27000-Reihe lässt Anwendern mehr Freiheiten bei der Implementierung, während der IT-Grundschutz eine detailliertere Anleitung bietet [Fra10].

5.1.1.2 ISA

Die International Society of Automation (ISA) ist eine gemeinnützige Organisation, die Standards für die Automatisierungstechnik entwickelt [ISA17].

Die ISA hat eine Reihe von Standards speziell für ICS-Security herausgegeben, die ursprünglich unter dem Namen **ISA 99** bekannt war. Mit der Adaption der Standards durch die IEC wurden sie umbenannt in **ISA / IEC 62443** und wird seit 2009 von beiden Organisationen gemeinsam weiterentwickelt [BSI13].

Die IEC 62443 ist in vier Dokumentgruppen gegliedert und enthält sowohl technische als auch organisatorische Maßnahmen speziell für ICS-Betreiber und -Hersteller [KL15]. Damit ist sie, im Gegensatz zum IT-Grundschutz, spezifisch auf ICS zugeschnitten.

Die erste Gruppe, „General“, enthält allgemeine Konzepte und Begriffsdefinitionen. Die zweite Gruppe mit dem Titel „Policies and Procedures“ beschreibt die Einführung und Aufrechterhaltung eines ISMS für ICS, ähnlich wie die ISO 27001 für allgemeine IT-Systeme. Eine überarbeitete Version, die besser zur ISO 27001 kompatibel ist, ist in Arbeit. Die dritte Gruppe, „System“, definiert Anforderungen für ICS-Integratoren und die vierte Gruppe, „Component“, leistet das Gleiche für Hersteller [ISA10]. Der Standard formuliert hier jedoch nur funktionelle Anforderungen und gibt keine Hinweise zur konkreten technischen Implementierung [ENISA14].

ISA 62443-3-3 und ISA 62443-4-2 sollen, ähnlich wie die ISO 27001 für allgemeine IT-Systeme, die Grundlage für die Zertifizierung von ICS bieten [ENISA14]

5.1.2 USA

5.1.2.1 NERC

Die North American Electric Reliability Corporation (NERC) ist eine gemeinnützige Organisation, die für die Zuverlässigkeit des Stromerzeugungs- und -übertragungssystems in Kontinental-USA, Canada und dem nördlichen Mexiko zuständig ist [NERC16].

NERC gibt zu diesem Zweck eine Reihe von Standards heraus; darunter einen aus neun Dokumenten bestehenden Standard zum Schutz kritischer Infrastrukturen (Critical Infrastructure Protection, CIP), der unter dem Namen **NERC CIP** bekannt ist. Auch wenn die Standards ursprünglich für das Stromnetz im nordamerikanischen Raum gedacht sind (für dessen Betreiber sind sie auch verpflichtend) [BSI13], umfassen sie viele Empfehlungen, die auf ICS im Allgemeinen anwendbar sind – denn viele ICS-Geräte und -Protokolle aus der Energiebranche werden auch in anderen Branchen genutzt [KL15].

5.1.2.2 NIST

Das National Institute of Standards and Technology (NIST) ist eine dem US-Handelsministerium unterstellte Bundesbehörde der USA, die für Standardisierung zuständig ist [NIST16; BSI13]. Die NIST-Dokumente sind kostenfrei erhältlich.

Die Special Publication **SP 800-53** [NIST13] ist nicht ICS-spezifisch. Ähnlich wie der IT-Grundschutz für deutsche Behörden ist dies der Standard, nach dem sich US-amerikanische Behörden richten müssen. Der grundlegende Ansatz ist etwas starrer als der der ISO 27000-Reihe, jedoch etwas flexibler (und weniger detailliert) als der des IT-Grundschutzes: Je nach Schutzbedarf des betreffenden IT-Systems wird eine grundlegende Liste von Maßnahmen empfohlen („baseline security controls“), die jedoch hinterher individuell angepasst werden kann. [NIST13].

Mit der Special Publication **SP 800-82** [NIST15a], die erstmalig 2006 erschienen ist, widmet sich NIST explizit den ICS und stellt Begriffsdefinitionen und Empfehlungen für Sicherheitsmaßnahmen zur Verfügung. Das Ziel des Dokumentes ist es, die Anpassung der allgemeinen SP 800-53 an ICS-Bedürfnisse zu ermöglichen [NIST15b]. Die Maßnahmen – sowohl technische als auch organisatorische – sind streckenweise technisch sehr konkret [BSI13].

Speziell für kritische Infrastrukturen hat das NIST im Jahr 2014 außerdem das **Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)** herausgegeben. Seine Anwendung ist jedoch – anders als für die SP 800-53 – freiwillig. Es ist ein sehr schlankes Dokument (etwa 40 Seiten im Vergleich zu über 400 Seiten der SP 800-53). Der Grund dafür ist die eher abstrakte Natur des Frameworks: Es soll helfen, sinnvolle Sicherheitsanforderungen zu kategorisieren und Prioritäten zu setzen, indem es fünf Funktionen eines Sicherheitskonzeptes beschreibt: „Identify“, „Protect“, „Detect“, „Respond“ und „Recover“. Für konkrete Maßnahmen referenziert es bestehende Standards wie NIST SP 800-53, der ISO / IEC 27000-Reihe und ISA / IEC 62443 [NIST14].

5.1.2.3 DHS

Das US-Department of Homeland Security (DHS) ist das Ministerium für Innere Sicherheit der USA. Es ist unter anderem für die IT-Sicherheit der Vereinigten Staaten zuständig [DHS16].

Zum DHS gehört auch das Industrial Control Systems Cyber Emergency Response Team (**ICS-CERT**), das in Kooperation mit der Industrie die Sicherheit der ICS-Anlagen in den USA verbessern soll [ICS-CERT17a]. Das ICS-CERT gibt eine Reihe von Empfehlungen zur Absicherung von ICS heraus [ICS-CERT17b]. Diese sind jedoch eher ausführliche Erläuterungen einzelner Grundprinzipien wie Defense in Depth, Incident Response, Forensik oder Patch Management als ein komplettes Modell für die Einführung eines Sicherheitskonzeptes. Dies unterscheidet die Empfehlungen von Standards wie ISO 27001, IT-Grundschutz, IEC 62443 oder NIST 800-53.

Auch der Schutz chemischer Anlagen vor Terrorangriffen fällt unter den Aufgabenbereich des DHS. Zu diesem Zweck gibt es die Chemical Facilities Anti-Terrorism Standards (**CFATS**) heraus, die auch eine große Anzahl von IT-Security-Maßnahmen für ICS enthalten [KL15].

5.1.2.4 AWWA

Die American Water Works Association (AWWA) ist ein internationaler, gemeinnütziger Verband, der Standards und Informationsmaterial rund um die Themen Wasserversorgung und -aufbereitung veröffentlicht [AWWA17a].

Die AWWA gibt einen **Cybersecurity Guide** und ein dazugehöriges **Tool** heraus. Damit adaptiert der Verband das NIST Cybersecurity Framework für die Wasserwirtschaft [AWWA17b].

Anhand von Anwendungsfällen empfiehlt das Cybersecurity Tool IT-Security-Maßnahmen, die für die Bedürfnisse der Wasserwirtschaft angemessen sind. Dabei nutzt es die Referenzen auf

bestehende Standards, die das NIST Cybersecurity Framework vorschlägt. Bei Anwendung des Tools wird eine Priorisierung der empfohlenen Maßnahmen vorgenommen [AWWA17c]:

- Priorität 1: Die Maßnahmen stellen die Minimalanforderungen an die Informationssicherheit sicher und sollten sofort umgesetzt werden.
- Priorität 2: Die Maßnahmen bewirken eine signifikante, sofortige Verbesserung der Informationssicherheit.
- Priorität 3: Die Maßnahmen bewirken eine zusätzliche Sicherheit gegen Angriffe auf das Prozessleitsystem und sollten umgesetzt werden, sobald das Budget es zulässt.
- Priorität 4: Die Maßnahmen bewirken eine Sicherheit gegen seltenere, besonders ausgefeilte Angriffe.

Der AWWA Cybersecurity Guide und das Tool werden regelmäßig überarbeitet, zuletzt am 22. Februar 2017 [AWWA17c].

Die Anwendungsfälle, die im Rahmen des Tools zur Identifikation sinnvoller Maßnahmen verwendet werden, liegen den Anwendungsfällen für das in dieser Arbeit erstellte IT-Grundschutz-Profil zugrunde (siehe auch Abschnitt 4.6.2).

5.1.3 Deutschland

5.1.3.1 BSI

Der **IT-Grundschutz** des BSI ist das ISO-27000-ISMS des BSI und wurde schon ausführlich in Abschnitt 2.2 beschrieben. Der IT-Grundschutz richtet sich nicht speziell an ICS, sondern an allgemeine Institutionen. Jedoch werden im Rahmen der Modernisierung ICS explizit mit einbezogen, indem eigene **IT-Grundschutz-Bausteine für ICS** erarbeitet werden. Auch diese Arbeit trägt mit der Entwicklung eines IT-Grundschutz-Pilotprofils anhand des Beispiels von ICS-Netzen in der Wasserwirtschaft zur Erweiterung des IT-Grundschutzes auf ICS bei.

Für deutsche Behörden ist die Zertifizierung auf Basis von IT-Grundschutz vorgeschrieben [Fra10].

Mit dem **ICS-Security-Kompendium** hat das BSI bereits 2013 eine Handreichung für ICS-Betreiber vorgelegt, die auch konkrete technische und organisatorische Maßnahmen für die Informationssicherheit enthält. Zu den empfohlenen Maßnahmen werden die entsprechenden Maßnahmen aus den Standards ISA / IEC 62443, VDI / VDE 2182, NERC CIP und den Best Practices des DHS / ICS-CERT referenziert [BSI13].

Separat gibt es ein ICS-Security-Kompendium für Hersteller von ICS-Komponenten [BSI14a].

Mit dem **LARS ICS** (Light and Right Security ICS) bietet das BSI zudem ein rechnergestütztes Tool für die industrielle Informationssicherheit an [BSI14b].

5.1.3.2 VDI / VDE

Der Verein Deutscher Ingenieure (VDI) ist eine Vereinigung von Ingenieuren und Akademikern angrenzender Disziplinen in Deutschland, der sich auch in der Normung betätigt [VDI17]. Der Verband der Elektrotechnik, Elektronik und Informationstechnik ist sein elektrotechnisches Pendant [VDE17].

Gemeinsam haben die beiden Verbände die Richtlinie **VDI / VDE 2182** zur Informationssicherheit in der industriellen Automatisierung entwickelt – also einen Standard explizit für die Sicherheit von ICS.

Im Standard werden ICS-Betreiber, -Hersteller und -Integratoren gleichermaßen berücksichtigt, und auch die Abhängigkeiten zwischen diesen drei Gruppen. Dies ist eine Besonderheit gegenüber anderen ICS-Security-Standards, die Hersteller, Betreiber und Integratoren oft getrennt behandeln: Der VDI / VDE-Standard möchte das Sicherheitskonzept prozessorientiert über den gesamten Lebenszyklus eines ICS betrachten. Ein weiteres Ziel des VDI / VDE–Standards ist die Verschlankung der Maßnahmenkataloge aus ISO 27000 bzw. IT-Grundschutz [BSI13]. Enthalten sind lediglich beispielhafte Maßnahmenempfehlungen für bestimmte Anwendungsbeispiele [VDI2182-1; VDI2182-2.1].

5.1.3.3 DWA / DVGW

Die Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) und der Deutsche Verein des Gas- und Wasserfaches (DVGW) sind als Branchenverbände der Wasserwirtschaft bereits in Abschnitt 3.1.2.2 vorgestellt worden. Dasselbe gilt für den von den beiden Verbänden erarbeitete **Branchenspezifischen Sicherheitsstandard Wasser / Abwasser (B3S WA)**.

Fachleute aus beiden Verbänden haben aus den Maßnahmen und Best Practices des IT-Grundschutzes und ICS-Security-Kompendiums diejenigen Maßnahmen ausgewählt, die für die Wasserwirtschaft sinnvoll sind [B3S17b; B3S17c]. Die Maßnahmenauswahl für das in dieser Arbeit erstellte IT-Grundschutz-Profil basiert auf der Auswahl des B3S WA (siehe Abschnitte 6.3 und 6.4).

5.2 Unterschiede zwischen IT-Security und ICS-Security

Ein großes Problem der ICS-Security ist, dass man bewährte IT-Security-Maßnahmen nicht einfach auf ICS übertragen kann. Der Grund dafür sind prinzipielle Unterschiede zwischen IT- und ICS-Netzen. Dieser Abschnitt gibt einen Überblick über diese Unterschiede und ihre Auswirkungen auf die Security.

5.2.1 Lebensdauer

ICS sind für sehr viel längere Lebensdauern ausgelegt als Office-IT-Systeme. Während Office-IT nach etwa drei bis fünf Jahren ausgetauscht wird, werden die Lebensdauern von ICS eher in Dekaden berechnet: 15 bis 30 Jahre sind keine Seltenheit [MS12; KL15].

Die langen Lebensdauern haben Konsequenzen für die ICS-Sicherheit. Die erste ist banal, aber weitreichend: Die Systeme sind oft schlichtweg alt. Mit moderner Security-Hardware oder -Software sind sie oft nicht kompatibel oder ihre Ressourcen reichen nicht aus [MS12].

Zudem wurden ICS, die jetzt im Einsatz sind, oft zu einer Zeit entwickelt, zu der Netztechnik und -protokolle in IT- und ICS-Netzen noch grundverschieden waren. Folglich waren ICS aus Office-Netzen und aus dem Internet nicht erreichbar – es gab eine „Air Gap“ zwischen ICS-Netzen und anderen Netzen. Security spielte deswegen zur Entwicklungszeit dieser ICS keine große Rolle [MS12].

Die Zyklen des technischen Fortschritts sind jedoch deutlich kürzer als die Lebenszyklen von ICS. Das Internet mitsamt seiner Netztechnik und seinen Protokollen (allen voran IP) hat mittlerweile auch in ICS-Netzen Einzug gehalten. Deshalb – aber auch durch die zunehmende Verbreitung von Drahtlosnetzen und mobilen Datenträgern und Geräten, die eine Air Gap überbrücken können – gehören ICS-Netze, die völlig von anderen Netzen abgeschottet sind, der Vergangenheit an. Die logische Folge: Schadprogramme für klassische IT-Systeme können nun auch auf ICS gelangen, und die sind dagegen nicht gewappnet [KL15].

Dass während der Lebensdauer eines IT-Systems Sicherheitslücken auftreten, ist auch in der Office-IT normal. Das Problem wird mit Patches gelöst, nachträglichen Security-Updates, die Sicherheitslücken schließen, wenn sie entdeckt werden. Patches werden von den Herstellern angeboten.

Da ICS jedoch so lange Lebensdauern haben, werden die verwendeten Systeme möglicherweise nach einiger Zeit von den Herstellern nicht mehr gepflegt, also keine Patches mehr bereitgestellt. Wird ein System in der Office-IT vom Hersteller nicht mehr gepflegt, kann es ausgetauscht werden. In ICS-Netzen ist ein Austauschen von einzelnen Komponenten mit größeren Komplikationen verbunden, was auch mit ihrem Auslegungszweck zu tun hat [KL15].

5.2.2 Auslegungszweck

Office-IT ist für die Verarbeitung von Daten ausgelegt; IT-Security in der Office-IT muss vertrauliche Daten schützen. Oft werden die Ziele der Informationssicherheit unter dem Kürzel

CIA zusammengefasst: Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit) – in dieser Rangfolge. Wichtig ist, unberechtigtem Zugriff auf die Daten (C) und ihrer Manipulation (I) entgegenzuwirken und sicherzustellen, dass ein berechtigter Zugriff stets möglich ist (A) [MS12].

ICS hingegen sind dafür ausgelegt, einen Prozess in der physischen Welt zu führen. Daten sind nur insofern wichtig, als dass sie Nachrichten an Aktoren und von Sensoren in der physischen Welt darstellen. Die oberste Priorität ist nicht der Schutz der Daten, sondern die zuverlässige Ausführung des physischen Prozesses (und der Schutz der Menschen, die sich in der Nähe aufhalten). Dafür müssen die Daten rechtzeitig – in Echtzeit – und ohne Veränderungen übermittelt werden und die ICS müssen zuverlässig funktionieren, oft monatelang ohne Unterbrechung. Die oberste Priorität haben die Verfügbarkeit (A) der ICS und ihre ordnungsgemäßen Funktion, für die die Integrität (I) der Daten und Algorithmen unverzichtbar ist [MS12; NIST15a].

Hinzu kommt, dass ICS oft nicht in temperierten und staubgeschützten Serverräumen stehen, sondern in für IT-Systeme schwierigen Bedingungen: Staub, Hitze, Vibrationen, Kälte, Feuchtigkeit oder explosionsgefährdete Bereiche fordern besonders robuste Systeme [MS12].

Sowohl die Priorisierung der Verfügbarkeit als auch die schwierigen Bedingungen führen dazu, dass ICS häufig nur die notwendigsten Ressourcen und Funktionen haben. Für zusätzliche Programme, die der Sicherheit dienen, sind sie nicht ausgelegt. Jede zusätzliche Anwendung – etwa Antivirenprogramme, die Dateien vor der Ausführung prüfen – bedrohen potenziell die Echtzeitfähigkeit. Da ICS oft für die Führung sensibler oder kritischer Prozesse verantwortlich sind, müssen ICS-Hersteller die Zuverlässigkeit ihrer Geräte garantieren. Oft erlischt diese Garantie, wenn zusätzliche Programme oder Patches installiert werden [MS12].

Für Änderungen am System, die Installation von Updates oder die Installation neuer Komponenten müssen ICS oft neu gestartet werden. Was bei IT-Systemen Routine ist, wird bei ICS, die monatelang laufen und oft Prozesse führen, die sich nicht ohne weiteres anhalten lassen, zum Problem. Betreiber sind deswegen konservativ bei der Einführung von Neuerungen und regelmäßige Updates sind oft schlichtweg unmöglich [MS12].

Dass für Office-IT relative harmlose Operationen wie ein Neustart für ICS so kritisch sind, hat auch Auswirkungen auf die Gefährdungen, die ICS-Security berücksichtigen muss.

5.2.3 Intention der Gefährdungen

Das Wichtigste in einem Office-IT-System sind in der Regel die Daten, die es verarbeitet. Sie müssen deswegen in der Regel gegen Angreifer verteidigt werden, die unerlaubt auf diese Daten zugreifen wollen. Auch Angriffe auf die Verfügbarkeit der Daten sind verbreitet, etwa Denial-of-Service-Attacken. Allen Szenarien gemeinsam ist aber, dass in ihrem Mittelpunkt ein Angreifer steht, der dem System bewusst schaden will [KL15].

Für ICS-Security trifft diese Angriff-und-Verteidigungs-Rhetorik den Kern nicht. Bei der Mehrheit der ICS-Sicherheitsvorfälle gibt es gar keinen Angreifer, sondern ihre Ursache sind Soft-

oder Hardwarefehler oder Bedienfehler [KL15; MS12]. Selbst eine völlig normale Variation des Systemzustands wie eine verlangsamte Datenrate oder ein zusätzlich beanspruchter Prozessor kann in ungünstiger Konstellation einen Sicherheitsvorfall zur Folge haben [Lan12]. ICS können auf diese Weise auch, sozusagen als Kollateralschaden, von Schadsoftware beeinflusst werden, die eigentlich Office-IT zum Ziel hatte [MS12].

Es gibt auch Angreifer, deren Schadprogramme speziell auf ICS zugeschnitten sind. Ihr Ziel sind jedoch in der Regel nicht die Daten, die ICS-Geräte verarbeiten, sondern die Maschinen, die sie kontrollieren. Bei den bekannten Vorfällen von IT-Angriffen auf ICS – allen voran der Computerwurm Stuxnet, der Zentrifugen des iranischen Urananreicherungsprogramms sabotieren sollte – war eine Manipulation oder Sabotage der geführten Maschinen oder Prozesse das Ziel [Zet14].

Zusammenfassend sind für ICS grundlegend andere Sicherheitsmaßnahmen notwendig als für Office-IT, weil

- die Systeme selbst anders sind: Auf ICS können, weil sie längere Lebensdauern haben und primär auf Zuverlässigkeit ausgelegt sind, viele bewährte IT-Security-Maßnahmen, die auf der Installation zusätzliche Software basieren, nicht umgesetzt werden;
- die Gefährdungen andere sind: ICS können – leichter als Office-IT – ohne böswillige Absicht ernsthaft gefährdet werden, und gezielte Angreifer haben andere Ziele als bei Angriffen auf Office-IT.

Die folgenden Abschnitte geben einen Überblick über Grundprinzipien für ICS-Security und sinnvolle Maßnahmentypen für ICS.

5.3 Grundprinzipien und Maßnahmentypen für ICS-Security

Weil es zwischen Office-IT und ICS die im vorherigen Abschnitt aufgeführten Unterschiede gibt, eignen sich einige IT-Security-Maßnahmen nicht gut für ICS. Dafür gibt es eine Reihe von Maßnahmen, die sich aufgrund der speziellen Eigenschaften von ICS besonders gut eignen. Und natürlich gibt es eine ganze Reihe von Maßnahmen, die für Office-IT und ICS gleichermaßen wichtig sind.

An dieser Stelle kann und soll kein vollständiger Überblick über Maßnahmen gegeben werden; dafür gibt es eine große Anzahl Lehrbücher, vor allem aber auch eine große Anzahl von Normen und Standards, von denen die wichtigsten für ICS in Abschnitt 5.1 vorgestellt wurden. Stattdessen werden in diesem Abschnitt drei wiederkehrende Grundprinzipien vorgestellt, denen ICS-Security-Maßnahmen folgen:

- Komplexitätsreduktion (Abschnitt 5.3.1),
- Zugriffsschutz (Abschnitt 5.3.2) und
- Systemkenntnis (Abschnitt 5.3.3).

Für jedes Prinzip werden typische Maßnahmenbeispiele angegeben.

In Abschnitt 5.4 werden die für das in dieser Arbeit erstellte Unterprofil AR (Architektur) relevanten Maßnahmen genauer betrachtet und auf die AR-Referenzarchitektur angewendet.

5.3.1 Komplexitätsreduktion

Die lange Lebensdauer von ICS-Komponenten und -Netzen und ihre Trägheit gegenüber Veränderungen kann für die Security als großer Vorteil genutzt werden: ICS-Netze sind zwar viel empfindlicher gegenüber unvorhergesehenen Veränderungen als Office-Netze; dafür ist es aber auch einfacher, die Variation unvorhergesehener Veränderungen einzuschränken.

Das Prinzip der Komplexitätsreduktion umfasst zwei Kernpunkte:

- Strukturierung bzw. Gruppierung von Komponenten und
- Vermeidung unnötiger Variationsmöglichkeiten.

Der Zweck von Komplexitätsreduktion besteht in der Minimierung der Angriffsfläche beziehungsweise der möglichen Fehlerquellen im System. Außerdem erleichtert Komplexitätsreduktion die Identifikation und Implementierung weiterer Schutzmaßnahmen. Die folgenden Maßnahmen können deswegen gewissermaßen als Basis für weitere Maßnahmen angesehen werden.

5.3.1.1 Segmentierung

Die ICS-Komponenten werden nach sinnvollen Kriterien – etwa ihrer Kritikalität oder den Protokollen, die sie nutzen – in funktionelle Gruppen eingeteilt und das ICS-Netz entsprechend dieser Gruppen segmentiert. Jedes dieser Segmente hat so wenig Verbindungen (sowohl physische als auch logische, z.B. nur die nötigsten Protokolle) wie möglich zum restlichen Netz. Diese Schnittstellen nach außen werden Perimeter genannt. Das Vorgehen entspricht dem **Principle of Least Route**: Jeder Netzknoten hat nur die unbedingt notwendigen Verbindungen. [KL15].

Die Segmentierung hat noch einen weiteren großen Vorteil für ICS: Systeme, auf denen keine Antivirenprogramme installiert werden können oder die nicht (mehr) patchbar sind, können in einem eigenen Netzsegment mit verschärften Zugangskontrollen platziert werden und auf diese Art trotzdem geschützt sein [KL15].

5.3.1.2 Härtung

Auf den ICS-Komponenten wird jede unnötige Software entfernt. Dasselbe gilt für unnötige Dienste oder Protokolle [Lan12].

5.3.1.3 Principle of Least Privilege

Jeder Nutzer des Systems bekommt nur die Rechte, die er für seine Arbeit benötigt. Dazu können Benutzer in Gruppen eingeteilt werden und den Gruppen aufgrund ihrer Aufgaben

bestimmte Zugriffsrechte eingeräumt werden. Dieses Vorgehen wird **Role-Based Access Control (RBAC)** genannt. Nicht mehr aktive Benutzerkonten werden gelöscht. In ICS-Netzen ist RBAC nicht immer möglich, da manche Komponenten, etwa HMIs, einen schnellen Zugriff im Notfall erfordern und sich oft mehrere Nutzer ein Konto teilen [KL15].

5.3.1.4 Etablieren von Standards

Institutionsübergreifend werden sowohl standardisierte Prozesse (etwa für die Neubeschaffung eines Gerätes, das Aufspielen von Patches oder das Erstellen von Backups) als auch Standards für Architekturen, Hardware und Software eingerichtet [Lan12].

5.3.2 Zugriffsschutz

Zugriffsschutz kann den Zugang zu Systemen, die Ausführung von Programmen oder den Zugriff auf Daten verhindern. Bei der Implementierung solcher Maßnahmen ist die im vorherigen Abschnitt erläuterte Komplexitätsreduktion extrem hilfreich: Ist beispielsweise ein Netz schon in Segmente eingeteilt und die Verbindungen der Netzsegmente auf das Nötigste reduziert, ist es viel einfacher, den Zugriff auf die Segmente zu kontrollieren [KL15].

Bei der Auswahl von Zugriffsschutzmaßnahmen ist **Defense in Depth** ist ein populäres Prinzip nicht nur für ICS-Security. Es bedeutet, sich nicht auf eine Sicherheitsmaßnahme zu verlassen, sondern verschiedene Maßnahmen auf verschiedenen Schichten zu implementieren. Was unter einer Schicht verstanden wird, kann dabei variieren. Beispiele sind [KL15]:

- Schichten des OSI-Referenzmodells,
- Netze und Subnetze oder
- Hintereinanderschaltung verschiedener Security-Geräte.

Im Folgenden werden typische Maßnahmen für den Zugriffsschutz und ihre Eignung für ICS vorgestellt. Sie sind in drei Kategorien eingeteilt: Schutz vor dem Zugriff auf Netze und Hosts, vor der Ausführung von Schadprogrammen und vor Zugriff auf Daten.

5.3.2.1 Schutz vor dem Zugriff auf Netze und Hosts

Zugriffsschutz kann auf verschiedensten Ebenen stattfinden. Die offensichtlichste ist der **physische Zugangsschutz**. Er spielt in ICS eine große Rolle, etwa in Form von abschließbaren Schaltschränken und Leitständen. Wenn der Leitstand, weil ein schneller Zugriff im Notfall notwendig ist, nicht aufwendig durch Passwörter etc. geschützt werden kann, ist der physischer Zugangsschutz umso wichtiger [KL15].

Der physische Schutz wird – auf Basis des im vorigen Abschnitt vorgestellten *Principle of Least Privilege* – durch sogenannte **AAA-Dienste** ergänzt. AAA steht für Authentisierung, Autorisierung und Accounting: Die Verifikation der Nutzeridentität, das Prüfen der Zugriffsberechtigung des Nutzers und das Nachhalten von Nutzeraktivitäten. Für die Authentisierung kann auf Besitz (z.B. Schlüssel), Wissen (z.B. Passwort) oder Eigenschaften (z.B. Fingerabdruck) eines

Nutzers zurückgegriffen werden [BSI13]. Die AAA-Dienste sollten für das ICS- und Office-Netz getrennt verwaltet werden [MS12].

Wenn nicht Menschen oder Geräte, sondern Datenströme auf ihre Zugangsberechtigung kontrolliert werden sollen, bieten sich ein automatisierter, **regelbasierter Zugriffsschutz** an. Entsprechende Geräte oder Software folgen statischen Regeln, nach denen sie Datenströme erlauben oder verbieten. Gerade in ICS-Netzen, deren Zweck genau festgelegt ist, sind auch sehr restriktiven Regeln häufig gut identifizierbar und umsetzbar – etwa für **Datendioden**, die generell nur Datenströme in eine Richtung zulassen. Detailliertere Regeln erlauben **Layer-3-Firewalls (Paketfilter)**, die die IP-Header des Netzverkehrs überprüfen und die Datenpakete aufgrund der konfigurierten Regeln abweisen oder zulassen. Firewalls können sowohl an Netz(segment)zugängen als auch auf einzelnen Hosts installiert sein [KL15].

Firewalls können selbstverständliche nur solche Daten filtern, die diese Firewalls passieren müssen. Netz-Firewalls (hostbasierte Firewalls sind hier ausdrücklich nicht gemeint) werden meist an den Außengrenzen des Netzes platziert. Wenn private mobile Geräte oder Datenträger mitgebracht und mit Komponenten innerhalb des ICS-Netzes verbunden werden (Bring Your Own Device, BYOD), bleiben solche Perimeter-Firewalls ohne Effekt. Es kann deswegen sinnvoll sein, das Mitbringen privater mobiler Geräte und Datenträger zu verbieten oder limitieren [KL15; BSI13].

5.3.2.2 Schutz vor der Ausführung von Schadprogrammen

Um schädliche Programme oder schädlichen Datenverkehr zu erkennen, reicht der Blick in IP-Header nicht aus; vielmehr ist ein Zugriff auf Inhalte aus höheren Protokollschichten notwendig – also auf den Payload der IP-Pakete.

Die Analyse von Protokollinhalten der Anwendungsschicht auf Netzebene nennt man **Deep Packet Inspection (DPI)**. Firewalls, die dazu in der Lage sind, werden **Layer-7-Firewalls** oder **Application-Layer-Gateways (ALG)** genannt. Jedoch können Firewalls nur statische Regeln abarbeiten. Ein **Intrusion Prevention System (IPS)** oder **Intrusion Detection System (IDS)** kann die Analyse der von der Firewall durchgelassenen Pakete weiter verfeinern. Es inspiziert ebenfalls Paketinhalte, nutzt dafür aber ähnlich wie Antivirenprogramme Signaturen und ist damit ebenso auf Updates angewiesen [KL15].

Wenn in ICS-Netzen regelmäßige Updates nicht möglich sind, kann ein IPS / IDS trotzdem arbeiten, indem es Anomalien erkennt: Abweichungen von statistisch gesehen normalen Datenströmen. Dabei steigt jedoch das Risiko für fälschlich als gefährlich markierte Inhalte, sogenannte *False Positives*. Diese sind für ICS besonders kritisch, da durch das fälschliche Aufhalten eines legitimen Datenpakets die Verfügbarkeit oder Echtzeitfähigkeit gefährdet wird. Daher ist bei der Verwendung anomaliebasierter Filter ein IDS oft eine bessere Wahl als ein IPS: Das IDS schlägt bei potenziell gefährlichen Datenpaketen Alarm, sodass sie manuell inspiziert werden können, hält sie jedoch im Gegensatz zum IPS nicht automatisch auf [KL15].

In der Office-IT sind **Antivirenprogramme** sehr verbreitet. Da sie auf Basis von Signaturen bekannter Schadprogramme arbeiten, sind sie jedoch ebenfalls auf regelmäßige Updates angewiesen. Zudem müssen sie jede Software vor der Ausführung überprüfen. Beides kann im ICS-Umfeld zur Gefährdung der Echtzeitanforderungen führen. Da aber die notwendigen Anwendungen sich in ICS-Netzen einfacher bestimmen lassen als in Office-Netzen, ist das **Whitelisting** eine gute Alternative für echtzeitkritische ICS-Netzsegmente und -Komponenten. Dabei wird eine Liste von erlaubten Anwendungen, Protokollen und Diensten erstellt und nur die Ausführung passender Software erlaubt [KL15; Lan12].

5.3.2.3 Schutz vor dem Zugriff auf Daten

Beim Zugriff auf Daten gibt es zweierlei Szenarien, die verhindert werden sollten: Die unbefugte (und unbemerkte) Manipulation von Daten und das unbefugte Lesen von Daten. Während das unbefugte Lesen vor allem bei Kommunikation über WAN ein Problem ist, muss die Manipulation gerade auch im LAN vermieden werden.

Vor unbefugter und unbemerkter Manipulation schützen Maßnahmen zur **Authentisierung und Autorisierung**, die bereits in Abschnitt 5.3.2.1 erläutert wurden, sowie Maßnahmen, die die Datenintegrität sicherstellen, etwa die in Abschnitt 5.3.2.2 beschriebenen Signaturen. Werden die Daten verändert, passen sie nicht mehr zu ihrer Signatur, und die Veränderung wird sofort bemerkt.

Die grundsätzliche Maßnahme, die Daten vor unbefugtem Lesen schützt, ist naheliegend: **Verschlüsselung**. Selbst, wenn er (unerlaubt) Zugriff auf die Daten erlangt hat, kann ein Angreifer verschlüsselte Daten nicht lesen.

Im ICS-Umfeld spielt Verschlüsselung vor allem eine Rolle, wenn Fernzugriffe auf ICS-Komponenten existieren. Solche Zugriffe für Hersteller und Zulieferer sind in ICS-Netzen sehr üblich – auch schon vor der Verbreitung des Internets [MS12]. Wird das Internet für den Fernzugriff genutzt, steigt allerdings die Gefahr eines unbefugten Zugriffs auf die Verbindung und damit die Notwendigkeit der Verschlüsselung. **Virtual Private Network (VPN)**-Verbindungen ermöglichen eine abgeschirmte, verschlüsselte Verbindung über ein ungesichertes WAN wie das öffentliche Internet und sollten für WAN-Anschlüsse von ICS-Netzen unbedingt genutzt werden [KL15; Lan12; BSI13].

5.3.3 Systemkenntnis

Systemkenntnis ist sowohl eine wichtige Voraussetzung, um überhaupt Maßnahmen anwenden zu können als auch eine zusätzliche Maßnahme, falls Abwehrmechanismen versagen: Eine gute Dokumentation der (komplexitätsreduzierten) Netzstruktur hilft bei der Identifikation notwendiger Zugriffsschutzmaßnahmen, die Kenntnis „normaler“ Systemzustände macht es leichter, bei der Systembeobachtung Abweichungen von der Norm zu erkennen.

5.3.3.1 Dokumentation

Wichtige Systeminformationen wie die Architektur eines Systems, die notwendigen Anwendungen, Dienste und Protokolle, verwendete Betriebssysteme sowie zugelassene Nutzer und deren Rechte werden dokumentiert. Diese Dokumentation ist bei ICS-Netzen besonders wichtig, da viele der in Abschnitt 5.3.2 vorgestellten Zugriffsschutz-Maßnahmen wie Whitelisting und Firewalls darauf angewiesen sind, berechtigte Systeme und Anwendungen genau zu kennen.

Die Dokumentation von im System üblichen Datenströmen und erwünschten Konfigurationen wird als **Baselining** bezeichnet und ist eine wichtige Voraussetzung für eine effektive Beobachtung des Systems. Zu diesem Zweck ist es sinnvoll, Log-Dateien zu speichern und analysieren [KL15].

5.3.3.2 Beobachtung (Monitoring)

Auch wenn das ICS-Netz gut strukturiert, dokumentiert und mit Zugriffsschutzmaßnahmen versehen ist, können Sicherheitsvorfälle nie ganz verhindert werden. Für diese Fälle ist es wichtig, die Vorfälle früh zu erkennen. Oft äußern sich sicherheitsrelevante Vorfälle in Abweichungen vom statistisch üblichen Systemverhalten und Konfigurationen, die im Rahmen des Baselining dokumentiert wurden. Zum Beispiel kann Schadsoftware Systemkonfigurationen ändern, unübliche Protokolle nutzen oder zusätzliche Datenströme beziehungsweise Datenströme zu unüblichen Zeiten generieren [KL15].

Eine mögliche Maßnahme für die Erkennung von Anomalien ist die Implementierung von **Intrusion-Detection-Systemen (IDS)**, die schon im Zusammenhang mit Zugriffsschutz erwähnt wurden. Auch der **Historian** kann solche Funktionen beinhalten. Umfassender können dies jedoch dedizierte **Security Information and Event Management (SIEM)-Systeme** leisten; sie automatisieren sowohl das Sammeln als auch die Auswertung von relevanten Systeminformationen. Jedoch ersetzt die automatisierte Auswertung die Analyse durch einen Menschen nie komplett, da nicht alle möglichen Angriffsmuster durch Regeln und Abweichungen abgedeckt werden können [KL15; BSI13].

5.4 Maßnahmen für eine sichere ICS-Architektur (AR)

In diesem Abschnitt soll auf Basis der in Kapitel 4 vorgestellten Referenzarchitekturen der Anwendungsfallgruppe AR eine sichere ICS-Architektur entwickelt werden. Diese Architektur soll sowohl der Veranschaulichung sinnvoller Maßnehmen für die Architektur dienen als auch als Basis für die Anwendung aller weiteren Maßnahmen in anderen Unterprofilen.

Dazu werden die in Abschnitt 5.3 erläuterte Maßnahmen zur Segmentierung und zum Zugriffsschutz für die einzelnen Netzsegmente auf die bisherigen Referenzarchitekturen AR2 (gemeinsames WAN) bzw. AR3 (gemeinsames LAN) angewendet. Die Referenzarchitektur des

Anwendungsfalls AR1 (dediziertes ICS-Netz) ergibt sich aus diesen Architekturen durch Streichen der Office-IT-Komponenten. Die Ergebnisse werden in Netzplänen veranschaulicht.

5.4.1 Segmentierung

Die grundlegende Bedeutung der Netzsegmentierung und ihre besondere Eignung für ICS-Netze wurden in Abschnitt 5.3.1.1 bereits beleuchtet. Nun soll eine sinnvolle Segmentierung der bislang erarbeiteten Referenzarchitektur für die Wasserwirtschaft (Netzplan siehe Abb. 4.2) vorgeschlagen werden.

Die Einteilung in Zonen wird anhand ihrer Kritikalität vorgenommen. Kritikalität wird in diesem Zusammenhang dadurch bestimmt,

- wie wichtig die Verfügbarkeit der Komponenten ist (also wie viel Verzögerung in der Netzverbindung toleriert werden kann) und
- wie direkt von den Komponenten auf den geführten Prozess zugegriffen werden kann.

Beide Kriterien stehen in direktem Zusammenhang mit den notwendigen Sicherheitsvorkehrungen, die an den Zonengrenzen getroffen werden müssen, aber auch mit den Anwendungen und Protokollen, die innerhalb der Zone verwendet werden (echtzeitkritisch oder nicht?). Das ist vorteilhaft, weil Zonen – gemäß dem Prinzip der Komplexitätsreduktion – möglichst homogen sein sollten, um Sicherheitsmaßnahmen besser auf sie abstimmen zu können. Für eine genauere Erläuterung siehe Abschnitt 5.3.1.

Die für die Segmentierung vorgeschlagenen Zonen orientieren sich an der Purdue Enterprise Reference Architecture (PERA) und dem Buch „Industrial Network Security“ von Eric D. Knapp und Joel Thomas Langill [Wil94; KL15]. Sie sind in Abb. 5.3 eingezeichnet. Abb. 5.1 liefert eine Legende für die farbliche Markierung der Zonen in Abb. 5.2. Für jede Zone ist im segmentierten Netzplan in Abb. 5.2 ein eigenes Subnetz (mit eigenem Switch) eingeführt worden. Die Subnetze eines LANs werden von einem zentralen Router bedient.

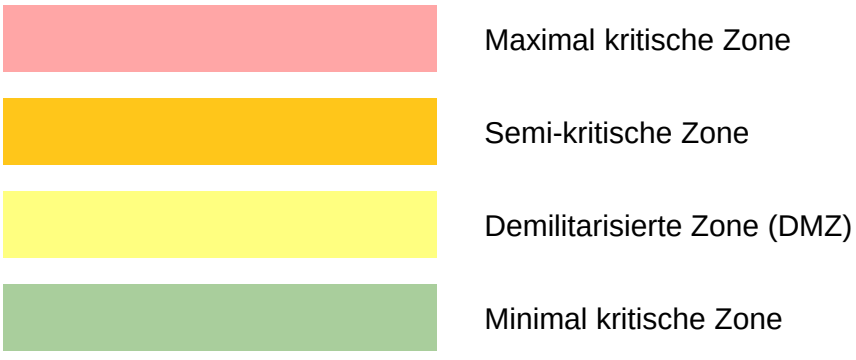


Abb. 5.1: Legende zur Zonenmarkierung (sortiert nach absteigender Kritikalität)

Die rot eingefärbte **maximal kritische Zone** umfasst alle ICS-Komponenten, die direkt mit dem zu führenden Prozess interagieren (Feldgeräte, SPS) oder direkten Zugriff auf die Pro-

zessführung haben (HMI). Diese Zone ist echtzeitkritisch. Der Control Server und die Engineering Workstations können ebenfalls zur Zone mit der höchsten Kritikalität gezählt werden, da auch sie schreibenden Zugriff auf SPSen besitzen können. Da sie jedoch weniger echtzeitkritisch sind, ist es auch möglich, die kritische Zone weiter zu unterteilen und Control Server und Engineering-WS einer **semi-kritischen Zone** (orange) zuzuordnen. Zudem ist noch anzumerken, dass die kritische Zone horizontal weiter unterteilt werden sollte, wenn es voneinander unabhängige Steuereinheiten gibt. Dies ist mit einer eigenen Zone für eine weitere verteilte SPS mit ihren Feldgeräten in Abb. 5.2 angedeutet.

Office-IT-Komponenten sind im ICS-Umfeld nicht echtzeitkritisch. Vom Blickwinkel der ICS-Security aus sind sie externe Komponenten, die für einen Schutz der ICS-Komponenten nicht besonders geschützt werden müssen. Deswegen werden sie als **minimal kritische Zone** (grün) eingestuft.

ICS-Komponenten wie Historian und Web Server haben nur lesenden Zugriff auf prozessnahe Komponenten, weshalb sie weniger kritisch sind als die anderen Komponenten. Sie werden in die gelb markierte **demilitarisierte Zone (DMZ)** eingeordnet.

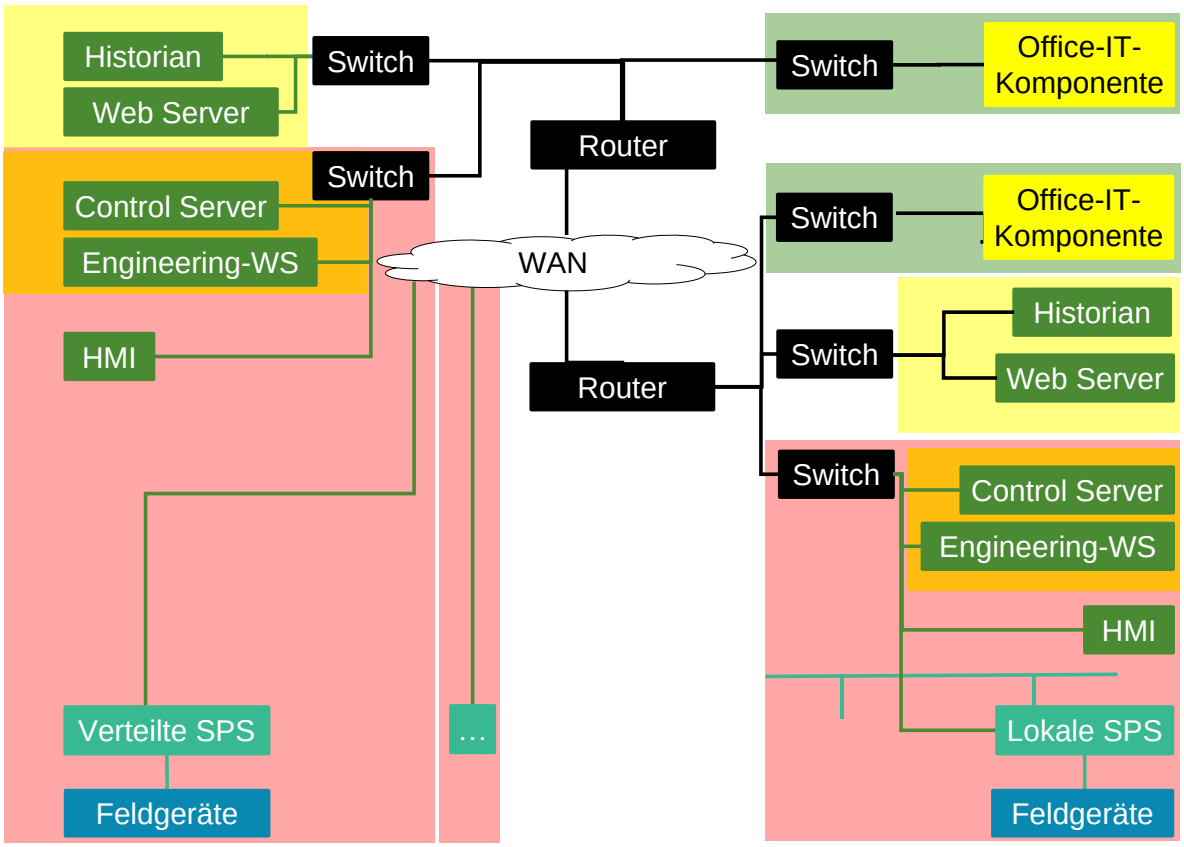


Abb. 5.2: Segmentierter Netzplan der Anwendungsfälle AR2 und AR3

Als eine demilitarisierte Zone bezeichnet man einen geschützten „Netzwerkbereich, der sich zwischen zwei physikalischen Netzwerksegmenten befindet und aus den beiden Segmenten einen kontrollierten Zugriff auf diesen geschützten Bereich ermöglicht“ [DWA11].

Technisch gesehen ist eine DMZ ein eigenes Netz(segment), das als Stellvertreter für die Kommunikation zweier benachbarter Netzsegmente dient. Sowohl vor das kritischere als auch vor das weniger kritische Segment wird je eine Layer-3-Firewall (Paketfilter) geschaltet. Vor der DMZ kann zusätzlich eine Layer-7-Firewall (Application-Layer-Gateway) eingesetzt werden (siehe Abb. 5.3). Auf diese Weise können Komponenten aus der weniger kritischen, weniger gesicherten Zone auf Komponenten der DMZ zugreifen (grüne Pfeile). Die kritische Zone ist indes durch eine weitere Firewall geschützt, die nur Zugriffe aus der DMZ (rote Pfeile), jedoch nicht direkt aus der weniger kritischen Zone erlaubt [BSI16a].

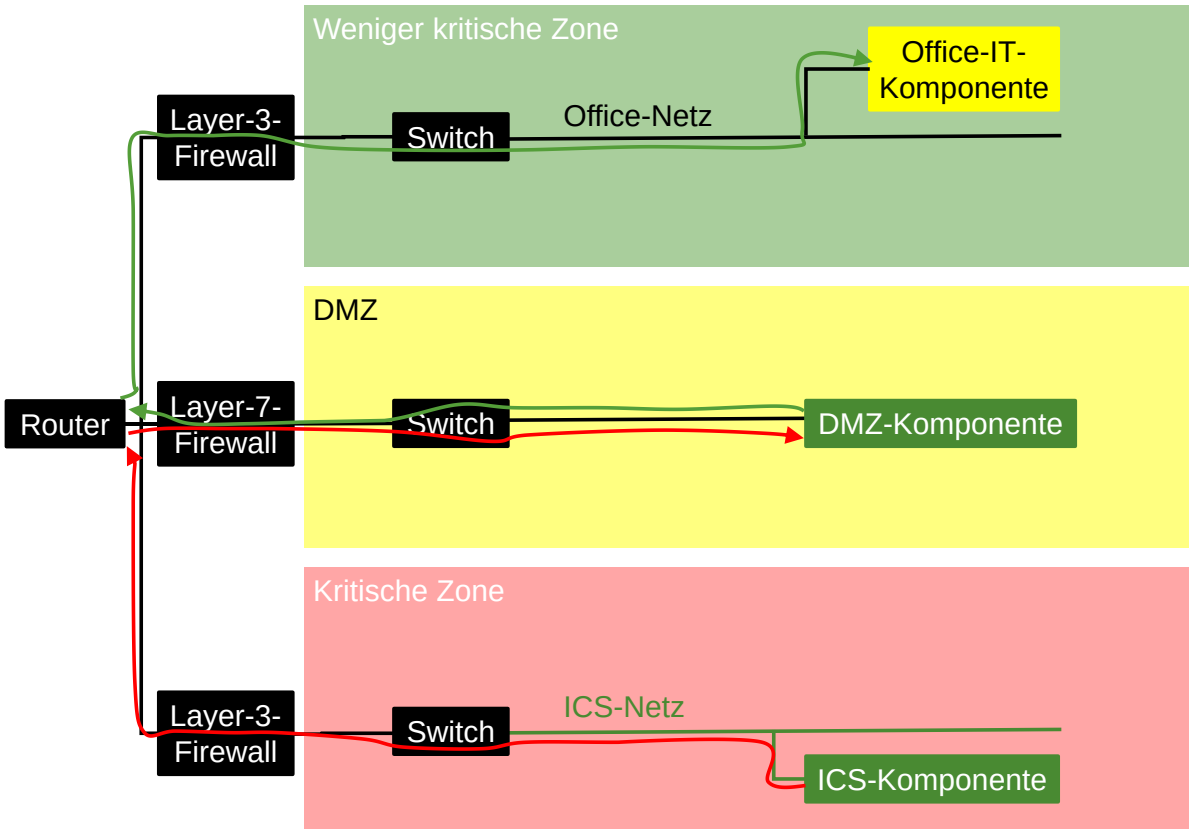


Abb. 5.3: Aufbau einer DMZ zwischen ICS-Netz und Office-Netz

Eine DMZ ist eine gute Lösung, um kontrollierten Zugriff auf ICS-Komponenten aus dem Office-Netz zu ermöglichen. In die demilitarisierte Zone (DMZ) zwischen dem Office- und dem ICS-Netz kommen deshalb ICS-Komponenten, auf die ein Zugriff von außerhalb des ICS-Netzes notwendig ist, die aber keinen schreibenden Zugriff auf ICS-Komponenten ermöglichen – andernfalls würden sie einen Eintrittsvektor in das ICS-Netz darstellen [KL15]. Sinnvolle DMZ-Komponenten aus der in dieser Arbeit betrachteten Referenzarchitektur sind

- Webserver (oder eine andere Art von Server), die lesenden Zugriff auf aktuelle Prozessdaten beispielsweise aus HMI-Anwendungen erlauben [DWA11],
- Historians, die lesenden Zugriff auf archivierte Prozessdaten erlauben [KL15].

Für genauere Informationen zu den einzelnen Komponenten siehe Abschnitte 2.1.2.1 und 4.4.

In Office-Netzen wird eine DMZ häufig zwischen das interne Netz und das öffentliche Netz (Internet) geschaltet. Dies wird in dieser Arbeit nicht berücksichtigt, da der Fokus auf den ICS-Komponenten liegt, die keinen Zugang zum Internet haben sollten. Wird das Internet für die WAN-Kommunikation genutzt, sollte stets ein verschlüsselter Zugang (VPN) eingesetzt werden (siehe den folgenden Abschnitt 5.4.2).

5.4.2 Zugangskontrollen an Zonen-Perimetern

Die Netzsegmentierung ist nur der erste Schritt zu einer sicheren ICS-Architektur. Zusätzlich müssen die Zonengrenzen, auch Perimeter genannt, vor ungewollten Zugriffen geschützt werden. Was in Abschnitt 5.3.2 über Zugriffsschutz erklärt wurde, soll nun auch im Netzplan eingezeichnet werden.

Eine Legende für die aktiven Netzkomponenten und die Sicherheitskomponenten liefert Abb. 5.4.

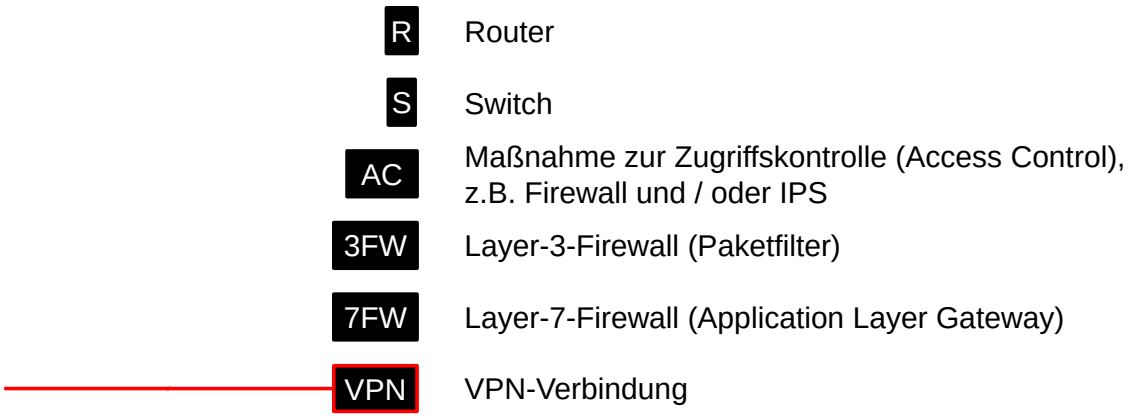


Abb. 5.4: Legende für die Sicherheitskomponenten in den Netzplänen

In der Referenzarchitektur wurde angenommen, dass Office-IT-Komponenten und ICS-Komponenten sich ein LAN und ein WAN teilen (dies entspricht den Anwendungsfällen AR2 und AR3 aus Abschnitt 4.6.3). Gibt es kein geteiltes LAN, entfällt die Zone der Office-IT-Komponenten. Die DMZ kann trotzdem Sinn ergeben, wenn ein Fernzugriff über das WAN auf ICS-Komponenten ermöglicht werden soll.

Jede Zone bekommt ihr eigenes IP-Subnetz und ihren eigenen Switch, und jede Zone ist mindestens mit einer Layer-3-Firewall gesichert. Ein Router ist für die Kommunikation zwischen den verschiedenen Subnetzen verantwortlich. Die DMZ ist entsprechend der in Abschnitt 5.4.1 vorgestellten Architektur mit einer Layer-7-Firewall versehen.

Die WAN-Kommunikation erfolgt entsprechend den Empfehlungen aus Abschnitt 5.3.2 ausschließlich über eine verschlüsselte VPN-Verbindung (in Abb. 5.5 rot dargestellt). Für die Perimeter der gesamten LANs ist ein Zugriffsschutz (Access Control, AC) vorgesehen: mindestens eine Firewall, zusätzliche Maßnahmen wie ein IDS / IPS sind je nach Größe der Institution sinnvoll.

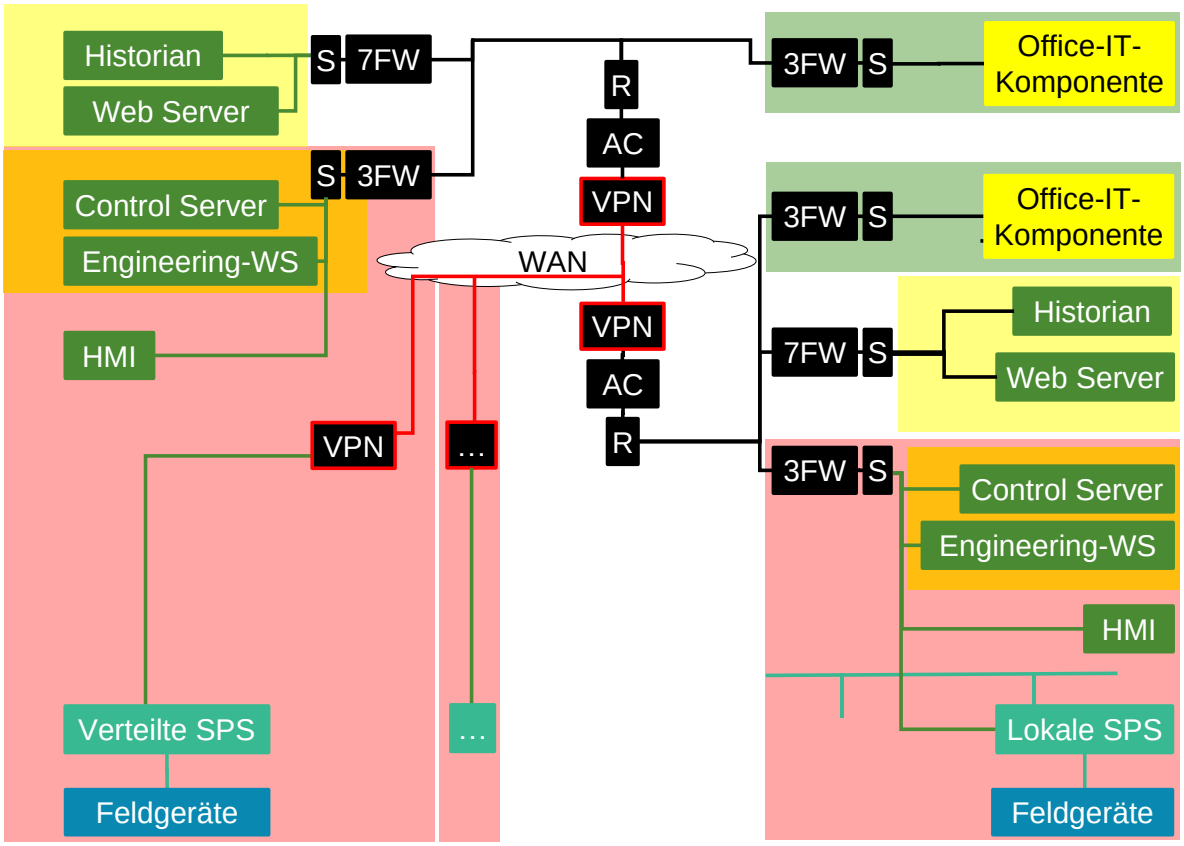
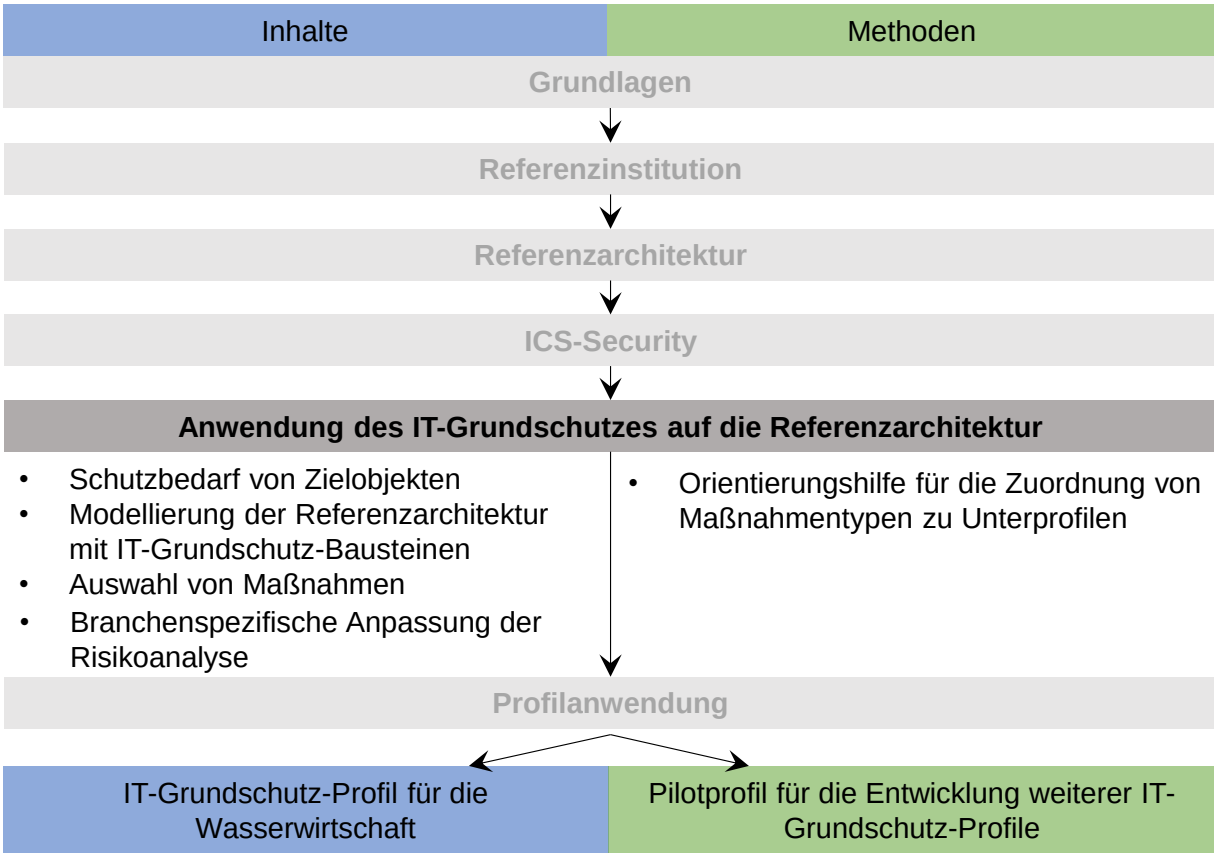


Abb. 5.5: Netzplan für die Anwendungsfälle AR2 und AR3 mit Netzsegmentierung sowie Schutzmaßnahmen an Zonenperimetern

6 Anwendung des IT-Grundschutzes auf die Referenzarchitektur



Nachdem in Kapitel 5 ein allgemeinerer Blick auf ICS-Security-Maßnahmen geworfen wurde, geht es in diesem Kapitel um die Maßnahmenauswahl nach einem spezifischen Regelwerk: dem IT-Grundschutz.

Das Kapitel umfasst die Schritte

- Schutzbedarfsfeststellung der Zielobjekte (Abschnitt 6.1) und
- Modellierung (Abschnitte 6.3 und 6.4), bestehend aus
  - Auswahl von IT-Grundschutz-Bausteinen für die Zielobjekte (Abschnitte 6.3.1 und 6.4.1) und
  - Auswahl von Maßnahmen / Anforderungen aus den IT-Grundschutz-Bausteinen (Abschnitte 6.3.2 und 6.4.2).

Diese Schritte müssen für jeden Anwendungsfall und die dazugehörigen Zielobjekte, also für jedes Unterprofil, gesondert durchgeführt. Die Zielobjekte der Kategorie „Organisation“ sind anwendungsfall- und architekturunabhängig und somit für jeden Profilanwender relevant. Ihre Modellierung wird deswegen im Hauptprofil vorgenommen. In dieser Arbeit werden die Schutzbedarfsfeststellung und Modellierung der Zielobjekte für das Hauptprofil (HP) sowie beispielhaft für das Unterprofil AR (Architektur) durchgeführt.

Um eine Richtlinie für die Modellierung und Maßnahmenauswahl für die übrigen Unterprofile zu geben, enthält Abschnitt 6.2 eine Orientierungshilfe, die die Zuordnung von Maßnahmen zu den einzelnen Unterprofilen erleichtert.

Zum Zeitpunkt der Niederschrift dieser Arbeit lagen noch nicht genügend Bausteine des modernisierten IT-Grundschutzes vor, um die Modellierung mit neuen Bausteinen sinnvoll zu ermöglichen. Aus diesem Grund wird auf die alten Bausteine zurückgegriffen. Dies bedeutet auch, dass nicht wie im modernisierten IT-Grundschutz eine Auswahl von *Anforderungen* stattfindet, sondern eine Auswahl von *Maßnahmen*. Wenn die modernisierten Bausteine vollständig sind, wird es eine Migrationstabelle geben, anhand derer die bisherigen Bausteine und Maßnahmen den Bausteinen und Anforderungen des modernisierten IT-Grundschutz zugeordnet werden können.

Da die Struktur der Bausteine und Maßnahmen grundlegend überarbeitet wird (siehe Abschnitt 2.2), wird sich jedoch die Liste der Maßnahmen (modernisiert: Anforderungen) für jeden *einzelnen* Baustein signifikant ändern. Um keine unnötigen Überarbeitungsschleifen herbeizuführen, wird deshalb die Begründung der Maßnahmenauswahl aus einem konkreten Baustein in dieser Arbeit nicht für alle Bausteine durchgeführt. Stattdessen soll die Maßnahmenauswahl für zwei Bausteine Erstellern künftiger Profile als Beispiel dienen:

- Baustein B 1.0: Sicherheitsmanagement (verwendet unter anderem im Hauptprofil).
- Baustein B 3.302: Router und Switches (verwendet unter anderem im Unterprofil AR).

Die beiden Bausteine sind gut geeignete Beispiele, da sie zum einen grundlegend sind und auch Bestandteil des modernisierten IT-Grundschutzes sein werden und zum anderen die beiden Bausteinkategorien des modernisierten IT-Grundschutzes repräsentieren: *Sicherheitsmanagement* wird zu den Prozessbausteinen gehören, *Router und Switches* hingegen zu den Systembausteinen.

6.1 Schutzbedarf der Zielobjekte

Der Schutzbedarf der Geschäftsprozesse und zugehörigen Anlagen richtet sich, wie in Abschnitt 3.4 erläutert, nach der Klassifizierung für kritischen Infrastrukturen in der BSI-KritisV [KritisV16].

Auf Basis dieser Einschätzung werden die Zielobjekte betrachtet, die für die jeweiligen Geschäftsprozesse relevant sind. Jedoch ist der Schutzbedarf der Zielobjekte stark anwendungsfallabhängig: Beispielsweise kann der Schutzbedarf für ein Mobilgerät höher sein, wenn es für die SPS-Programmierung verwendet wird, als wenn es nur Nachrichten empfängt. Deswegen muss der Schutzbedarf für einzelne Zielobjekte spezifisch für einzelne Anwendungsfälle und damit in den Unterprofilen festgelegt werden. Die Schutzbedarfsfeststellung für das in dieser Arbeit erstellte Unterprofil AR erfolgt in diesem Abschnitt.

Für die einzelnen Zielobjekte wird der Schutzbedarf wie folgt festgelegt:

- Grundsätzlich erben die Zielobjekte den Schutzbedarf von dem Geschäftsprozess, für dessen Erfüllung sie (bzw. die Anlage, zu der sie gehören) benötigt werden. Das bedeutet insbesondere, dass ihr Schutzbedarf nicht höher als der dieses Geschäftsprozesses (bzw. dieser Anlage) sein kann.
- Gehört der Geschäftsprozess zu keiner kritischen Infrastruktur, haben alle dazugehörigen Zielobjekte einen normalen Schutzbedarf.
- Bei Geschäftsprozessen einer kritischen Infrastruktur (mit hohem Schutzbedarf) können die Zielobjekte hohen oder normalen Schutzbedarf haben. Die Schutzbedarfszuweisung hängt von dem Anwendungsfall ab, in dem die Zielobjekte verwendet werden.
- Ist in einem Anwendungsfall das Zielobjektes für die Erbringung des kritischen Geschäftsprozesses (oder den Schutz anderer Zielobjekte) besonders wichtig, erhält das Zielobjekt die Schutzbedarfskategorie „hoch“.

Die Schutzbedarfskategorie ist insofern relevant, dass für Zielobjekte mit erhöhtem Schutzbedarf im in dieser Arbeit erstellten IT-Grundschutz-Profil zusätzliche Maßnahmen ausgewählt werden.

Im Folgenden wird den Zielobjekten des Hauptprofils (Tab. 6.1) sowie des Unterprofils AR (Tab. 6.2) ein Schutzbedarf zugewiesen. Haben Zielobjekte (in einem bestimmten Anwendungsfall) einen hohen Schutzbedarf, wird das betreffende Tabellenfeld schwarz eingefärbt, bei einem normalen Schutzbedarf bleibt es weiß.

Es ist zu beachten, dass die Schutzbedarfe in Tab. 6.1 und Tab. 6.2 nur gelten, wenn der übergeordnete Geschäftsprozess (bzw. die übergeordnete Anlage) einen hohen Schutzbedarf zugewiesen bekommen hat. Andernfalls haben alle Zielobjekte normale Schutzbedarfe.

Tab. 6.1: Schutzbedarfstabelle für Zielobjekte des Hautprofils

Legende für den Schutzbedarf:		**normal**	**hoch**
Nr.	**Zielobjekt**		
Organisation			
O1	Sicherheitsmanagement		
O2	Notfallmanagement		

Für das Hauptprofil gestaltet sich die Schutzbedarfszuweisung einfach, da es nicht weiter in Anwendungsfälle untergliedert ist und nur zwei Zielobjekte umfasst. Das erste Zielobjekt, *Sicherheitsmanagement,* ist von grundlegender Wichtigkeit für die Etablierung, Aufrechterhaltung und Weiterentwicklung aller Maßnahmen zur Informationssicherheit im täglichen Betrieb und bekommt deswegen einen hohen Schutzbedarf zugewiesen. Das zweite Zielobjekt, *Notfallmanagement*, ist weniger relevant für den täglichen Betrieb; ein normaler Schutzbedarf ist deswegen ausreichend.

Das Unterprofil AR hat eine größere Anzahl von Zielobjekten und besteht aus den drei Anwendungsfällen AR1: dediziertes ICS-Netz, AR2: Gemeinsames WAN und AR3: Gemeinsames

LAN. Tab. 6.2 zeigt die Schutzbedarfszuweisung der spezifischen Zielobjekte für alle drei Anwendungsfälle.

Die Komponenten, die den Zugang zum ICS-Netz erlauben, namentlich Router und Switches, haben unabhängig vom Anwendungsfall einen hohen Schutzbedarf. Sie sind elementar sowohl für die Aufrechterhaltung der Kommunikation zwischen einzelnen ICS-Komponenten als auch für den Zugang zum ICS-Netz und damit für den Schutz von ICS-Komponenten.

Beim Anwendungsfall AR2: Gemeinsames WAN ist eine Anbindung nach außen vorhanden. In diesem Fall erhöht sich der Schutzbedarf für die kritischsten ICS-Komponenten. Als kritischste Komponenten werden in Anlehnung an die Überlegungen aus Kapitel 5 und das PERA-Modell die echtzeitrelevanten Komponenten und solche, die direkten Zugriff auf den Prozess ermöglichen, gewertet. Dies umfasst die Zielobjekte Feldgerät, SPS, HMI, Engineering-Workstation und Control Server sowie den Feldbus. Router und Switches unterliegen ohnehin hohem Schutzbedarf.

Tab. 6.2: Schutzbedarfstabelle für Zielobjekte des Unterprofils AR (Architektur)

Legende für den Schutzbedarf:		**normal**		**hoch**
	Anwendungsfall:	**AR1**	**AR2**	**AR3**
Nr.	**Zielobjekt**			
IT-Systeme				
IT1	Feldgerät		■	
IT2	SPS		■	
IT3	HMI		■	
IT4	Historian			
IT5	Engineering-Workstation		■	
IT6	Control Server		■	
IT7	Webserver			
IT8	Mobilgerät			
IT9	Externe Komponente			
IT10	Office-IT-Komponente			
Netzkomponenten				
N1	Switch	■	■	■
N2	Router	■	■	■
N3	Modem			
N4	IT-Verkabelung			
N5	Feldbus		■	
N6	Fernwartung			
Sicherheit				
S1	Firewall		■	
S2	VPN			
S3	IDS / IPS			

6.2 Orientierungshilfe für die Zuordnung von Maßnahmentypen zu den Unterprofilen

Da in dieser Arbeit nur ein Unterprofil erstellt werden kann, soll dieser Abschnitt eine Orientierung bieten, wie die restlichen Unterprofile gegeneinander abzugrenzen sind; konkret: Was für Maßnahmentypen für welche Zielobjekte in welches Unterprofil passen.

Werden Anwendungsfälle in Unterprofilen mit bestimmten Bausteinen modelliert, müssen nicht alle Maßnahmen (bzw. Anforderungen) der Bausteine ausgewählt werden. Bei einer Nichtauswahl einer Maßnahme sind folgende Szenarien möglich:

- Die Maßnahme (Anforderung) wird für die Zielgruppe des Profils insgesamt nicht ausgewählt. In diesem Fall sollte die Nichtauswahl begründet werden.
- Die Maßnahme (Anforderung) wird für die Zielgruppe des Profils ausgewählt, aber nicht für diesen Anwendungsfall. Stattdessen wird sie in einem anderen Anwendungsfall ausgewählt. Hierfür ist keine gesonderte Begründung notwendig.

Aus diesem Grund ist es während der Profilerstellung sinnvoll, einen Überblick zu haben, welche Maßnahmentypen zu welchen Anwendungsfällen (und damit Unterprofilen) gehören. Im Folgenden werden dazu zum Hauptprofil sowie zu jedem Unterprofil Faustregeln für geeignete Maßnahmentypen gegeben. Dabei wird auch angegeben, auf welche Zielobjekte sich die Maßnahmen jedes Unterprofils konzentrieren sollten. Zur Veranschaulichung der Faustregeln dienen konkrete Maßnahmen als Beispiele; sie werden mit Hilfe der in Abschnitt 5.3 erarbeiteten drei Grundprinzipien kategorisiert:

1. **Komplexitätsreduktion**
    a. Segmentierung
    b. Härtung
    c. Principle of Least Privilege (RBAC)
    d. Etablieren von Standards
2. **Zugriffsschutz**
    a. Schutz vor Zugriff auf Netze und Hosts
    b. Schutz vor Ausführung von Schadprogrammen
    c. Schutz vor Zugriff auf Daten
3. **Systemkenntnis**
    a. Dokumentation und Baselining
    b. Beobachtung (Monitoring)

Bei der Lektüre der Orientierungshilfe ist zu beachten, dass *mögliche* Maßnahmen den passenden Unterprofilen zugeordnet werden. Dies soll eine Hilfestellung für Anwender des Pilotprofils sein, die auf Basis ähnlicher Anwendungsfallkategorien ein eigenes IT-Grundschutz-Profil für ihre Branche bzw. Zielgruppe erstellen möchten. Es wird explizit keine Aussage darüber getätigt, *welche* dieser Maßnahmen für ein konkretes IT-Grundschutz-Profil empfehlenswert sind. Auch erhebt die Übersicht keinen Anspruch auf Vollständigkeit; vielmehr soll sie die Zuordnung weiterer Maßnahmen zu den richtigen Unterprofilen erleichtern.

6.2.1 Hauptprofil (Organisation)

Das Hauptprofil enthält nur Maßnahmen, die für jede Institution, die das Profil anwendet, gelten – unabhängig von der Ausgestaltung ihres ICS-Netzes. Das sind Maßnahmen, die das Erstellen von Leitlinien, Konzepten, Strategien, Prozessen und Notfallkonzepten zur Aufrechterhaltung der Sicherheit und der Verteilung der Verantwortung umfassen.

6.2.2 Unterprofil AR (Architektur)

Für das Unterprofil AR sind alle Maßnahmen relevant, die mit dem grundlegenden Aufbau des ICS-Netzes und der Absicherung seiner Außengrenzen (Perimeter) zu tun hat. Faustregeln für geeignete Maßnahmen:

- Für Netzkomponenten und Sicherheitskomponenten: Spezifische Maßnahmen für einzelne Komponenten, vor allem für die Hardware, Anschaffung und grundlegende Implementierung der Komponenten. Maßnahmen, die Software und Betrieb der Komponenten betreffen, gehören eher ins Unterprofil NM.
- Für ICS-Komponenten: Keine spezifischen Maßnahmen. ICS-Komponenten sind nur insofern relevant, weil der Aufbau einer geeigneten Architektur sich an ihren Anforderungen orientiert (Netzsegmentierung!).
- Maßnahmen der Netzsicherheit ja, Sicherheitsmaßnahmen auf einzelnen Hosts eher nicht.

Konkret ist in der Kategorie der **Komplexitätsreduktion** die Netzsegmentierung eine mögliche Maßnahme. Für die Konfiguration von Routern und Switches kann die Entwicklung von Standards sinnvoll sein.

Der **Zugriffsschutz** konzentriert sich vor allem auf Netzkomponenten an den Segmentgrenzen. Beispielsweise können dort Switch-Ports gesichert und Firewalls sowie Intrusion Detection / Prevention Systeme (IDS / IPS) eingerichtet werden. Bei WAN-Nutzung können weiterhin die Einrichtung eines DNS-Servers und die Nutzung von VPN-Verschlüsselung sinnvoll sein. Voreingestellte Passwörter auf Routern und Switches sollten geändert werden. Auch physischer Zugangsschutz gehört zu den möglichen Maßnahmen dieses Unterprofils.

Hinsichtlich der **Systemkenntnis** ist es wichtig, die Standardkonfigurationen von Routern und Switches zu kennen, um unbefugte Änderungen bemerken zu können.

6.2.3 Unterprofil NM (Netzmanagement)

Die Maßnahmen des Unterprofils NM betreffen – genau wie die des Unterprofils AR – eher Netzkomponenten als ICS-Komponenten. Im Unterschied zum Unterprofil AR geht es jedoch weniger um eine sichere *Architektur* und die Sicherung der Zonengrenzen, sondern um einen sicheren *Betrieb* der Netzkomponenten. Faustregeln für geeignete Maßnahmen:

- Komponentenübergreifend: Maßnahmen für Dokumentation der Netz- und Systemkonfiguration.

- Für Netz- und Sicherheitskomponenten: Spezifische Maßnahmen für Administration, Betrieb, Dokumentation, Notfallvorsorge und Updates.
- Bei der Maßnahmenauswahl steht nicht die Hardware, sondern Software und Prozesse im Fokus.

Komplexitätsreduktion kann erreicht werden, indem ein Netzmanagementsystem eingeführt wird (zum Beispiel auf Basis von SNMP) und die Netzkomponenten gehärtet werden (also alle nicht benötigten Anwendungen, Dienste und Protokolle eliminiert werden).

Beim **Zugriffsschutz** spielen vor allem softwareseitige Maßnahmen eine Rolle: Die sichere Konfiguration von Routern, Switches und WLAN-Access Points, die Implementierung von Access Control Lists (ACL) auf Routern.

Systemkenntnis ist für das Unterprofil NM besonders relevant: Für gutes Netzmanagement ist eine Dokumentation des Netzes sowie aller Geräte hilfreich, auch Baselines für die Konfigurationen sind sinnvoll, um Manipulationen erkennen zu können. Administratoren sollten entsprechend geschult sein.

6.2.4 Unterprofil UA (Benutzerzugang)

Das Unterprofil UA umfasst solche Maßnahmen, die den Zugriff auf das ICS und insbesondere den vom ICS geführten Prozess schützen. Faustregeln für geeignete Maßnahmen:

- Das wichtigste zu schützende Zielobjekt dieses Unterprofils ist das HMI, da es direkten, manuellen Prozesszugriff erlaubt.
- Es geht um den *Zugang* von Menschen (ggf. mit Geräten), weniger um den *Zugriff* durch Programme.
- Maßnahmen, die den physischen Zugang zur Anlage regeln, gehören hierher.
- Auch mobile Geräte und Datenträger können auf physischem Wege in die Anlage gelangen. Maßnahmen, um dies zu unterbinden, gehören in dieses Unterprofil.
- Der automatisierte Zugriff mittels SPSen wird im Unterprofil PLC abgedeckt; dafür sind hier keine Maßnahmen erforderlich.
- Maßnahmen, die den Zugriff auf das gesamte ICS-Netz erschweren, werden bereits im Unterprofil AR abgedeckt.

Die **Komplexitätsreduktion** umfasst ähnliche Maßnahmen wie für SPSen: Es können Maßnahmen ergriffen werden, die der Härtung des HMI-Systems und die ausschließliche Nutzung freigegebener Hard- und Software bewirken. Zudem sind Maßnahmen zur Klärung von Verantwortlichkeiten (und Vertretungen) und Nutzerrechten sinnvoll (RBAC, Least Privilege). Auch Regeln zum Gebrauch von Passwörtern sind denkbar.

Der **Zugriffsschutz** ähnelt ebenfalls dem der SPS-Programmierung, nur dass diesmal das HMI das Zielobjekt ist: Passwortschutz, gesichertes Login, Schutz vor Schadprogrammen, geeignete Regeln für Mobilgeräte, mobile Datenträger und Fremdpersonen gehören zu den klas-

sischen Maßnahmen. Auch beim HMI ist ein Fernzugriff, oft über das Internet, verbreitet, sodass Maßnahmen wie Firewalls, VPN und Schutz vor Inhalten aus dem Internet angebracht seinen können.

Das HMI als Bedienschnittstelle des Prozesses muss fehlerfrei und vorhersehbar funktionieren, weshalb **Systemkenntnis** wichtig ist: Dazu gehört, Veränderungen am System stets zu dokumentieren und Handbücher bereitzuhalten. Das Personal, dass das HMI bedient, sollte geschult sein. Auch Datensicherung kann eine Maßnahme sein, die in dieses Unterprofil passt.

6.2.5 Unterprofil PA (Programmzugriff)

Das Unterprofil PA beschäftigt sich mit den ICS-Komponenten und insbesondere mit deren Software. Faustregeln für sinnvolle Maßnahmen sind

- Für IT-System-Komponenten: Maßnahmen, die die Software aller IT-Systeme betreffen, insbesondere Historian und Webserver.
- Ausgenommen sind Maßnahmen zum Programmieren von SPSen und für den Zugriff auf den Prozess (HMI), für die es eigene Unterprofile gibt (PLC, UA).
- Komponentenübergreifend: Maßnahmen, die den Zugriff auf Software regeln.

Zur **Komplexitätsreduktion** ist auch hier der Einsatz eines Netzmanagementsystems möglich. Es ist zudem sinnvoll, Nutzer in Gruppen einzuteilen, um ihnen nur die nötigen Zugriffsrechte für die Ausführung Rollen zuweisen zu können (RBAC, Principle of Least Privilege).

Auch Maßnahmen zur **Zugriffskontrolle** konzentrieren sich auf Anwendungen. Dazu können Layer-7-Firewalls gehören, aber auch Zugriffskontrollen für einzelne Anwendungen, etwa den Historian. Der Einsatz von Virenschutzprogrammen mitsamt regelmäßiger Patches gehören ebenfalls zu den Maßnahmen des Unterprofils PA. Da die echtzeitkritischen Anwendungen nicht Teil des Unterprofils sind, spricht wenig gegen den Einsatz konventionelle Virenschutzprogramme.

Zur Verbesserung der **Systemkenntnis** kann das Sammeln und Auswerten von Log-Dateien sinnvoll sein. Eine Datensicherung, vor allem bei Datenbanken wie dem Historian, ist ratsam. Die Nutzerrollen und ihre Rechte können dokumentiert werden.

6.2.6 Unterprofil PLC (SPS-Programmierung und -Wartung)

In diesem Unterprofil dreht sich alles um den Zugriff auf die SPSen. Da sie direkt auf den zu leitenden Prozess einwirken, sollte der Zugang zu SPSen besonders geschützt sein. Faustregeln:

- Für ICS-Komponenten: Maßnahmen, die den Zugriff auf und die Integrität von (Daten auf) SPSen und Engineering-Workstations betreffen.
- Komponentenübergreifend: Besonders Maßnahmen für Mobilgeräte wie zum Beispiel Laptops, die auf SPSen zugreifen können und für die Kommunikation von SPSen mit externen Komponenten.

Die **Komplexitätsreduktion** spielt dabei insofern eine Rolle, als dass SPSen gehärtet werden sollten; dazu kann auch die Einschränkung der Benutzerumgebung gehören. Auch Standards können sinnvoll sein: Der Passwortgebrauch kann Regeln unterliegen um Missbrauch zu vermeiden. Es kann Standards geben, die die Freigabe von Hard- und Software regeln und die Nutzung aller anderen Komponenten untersagen.

Zugriffsschutz ist aus oben genanntem Grund für die SPSen fundamental: Von Bildschirmsperren über Passwortschutz bis hin zu lokalen Firewalls und VPN bei Fernzugriff sind viele Maßnahmen denkbar. Die Ausführung von Schadprogrammen sollte unterbunden werden; sei es durch Virenschutzprogramme oder Whitelisting. Ein großes Risiko stellen Mobilgeräte und mobile Datenträger dar, die mit den SPSen verbunden werden; aus diesem Grund können für solche Geräte verschärfte Zugriffsschutzmaßnahmen ergriffen werden. Fremdpersonen sollten keine Möglichkeit bekommen, unbeaufsichtigt auf SPSen zuzugreifen.

Die **Systemkenntnis** spielt vor allem zur Vermeidung von Sicherheitsrisiken durch Bedienfehler eine Rolle. Eine mögliche Maßnahme ist die Schulung von Personal, die mit SPSen arbeiten. Das umfasst auch eine Schärfung des Bewusstseins für Auffälligkeiten, die auf sicherheitsrelevante Vorfälle hinweisen (Security Awareness). Eine Datensicherung ist ratsam.

6.3 Modellierung für das Hauptprofil

Im Hauptprofil werden die beiden Zielobjekte Sicherheitsmanagement und Notfallmanagement modelliert. Beide sollten in jeder Institution, die das IT-Grundschutz-Profil anwendet, vorhanden sein; ebenso sollten auch die in Abschnitt 6.3.2 ausgewählten Maßnahmen stets umgesetzt werden.

6.3.1 Auswahl von IT-Grundschutz-Bausteinen

Die Modellierung der beiden Organisations-Zielobjekte mit Bausteinen ist in Tab. 6.3 veranschaulicht. In den Zeilen finden sich die zu modellierenden Zielobjekte, in den Spalten die ausgewählten Bausteine. Wird ein Baustein für die Modellierung eines Zielobjekts verwendet, wird das entsprechende Feld eingefärbt. Ein Zielobjekt kann dabei durchaus durch mehrere Bausteine abgebildet werden.

Tab. 6.3: Modellierungstabelle für die anwendungsfallunabhängigen Zielobjekte des Hauptprofils

Nr.	**Zielobjekt**	**Modellierung mit Bausteinen**		
		B 1.0 Sicherheits-management	B 1.3 Notfall-management	B 1.8 Behandlung von Sicherheitsvorfällen
Organisation				
O1	Sicherheitsmanagement			
O2	Notfallmanagement			

Sowohl für das allgemein gehaltene Sicherheitsmanagement, also den Teil des Managements, der sich mit der Informationssicherheit einer Institution befasst, als auch für das etwas spezifischere Notfallmanagement, das die Kontinuität des Betriebs in Notfällen sicherstellen soll, gibt es explizit Bausteine im (bisherigen) IT-Grundschutz: Die Bausteine **B 1.0: Sicherheitsmanagement** sowie **B 1.3: Notfallmanagement**.

Um die Modellierung zu vervollständigen, wird für beide Zielobjekte zusätzlich der Baustein **B 1.8: Behandlung von Sicherheitsvorfällen** ausgewählt. Während sich Bausteine B 1.0 und B 1.3 eher mit dem übergeordneten Management befassen, beinhaltet dieser Baustein konkretere operative Maßnahmen.

Mögliche passende Bausteine des modernisierten IT-Grundschutzes sind die Bausteine aus den Kategorien ISMS, ORP.1: Organisation und DER.2: Security Incident Management. Jedoch liegen diese Bausteine zum Zeitpunkt der Niederschrift dieser Arbeit noch nicht vor und auch ihre Titel und Nummerierung sind noch vorläufig, sodass keine verbindliche Aussage getroffen werden kann. Für eine verbindliche Zuordnung neuer Bausteine zu den bisherigen wird auf die Migrationstabellen verwiesen, die es für die Umstellung auf den modernisierten IT-Grundschutz geben wird.

6.3.2 Auswahl umzusetzender Maßnahmen (Anforderungen) am Beispiel des Bausteins B 1.0

Wie in der Einleitung zu diesem Kapitel begründet, wird an dieser Stelle beispielhaft eine Maßnahmenauswahl für einen Baustein des Hauptprofils vorgenommen. Es wird der Baustein B 1.0: Sicherheitsmanagement betrachtet. Für eine vollständige Profilerstellung muss die Maßnahmenauswahl für jeden verwendeten Baustein durchgeführt und begründet werden.

In dem in dieser Arbeit erstellten Profil werden, wie bereits erwähnt, verschiedene Anwendungsfallgruppen in Unterprofilen zusammengefasst. IT-Grundschutz-Bausteine können in mehreren Unterprofilen gleichzeitig verwendet werden; es werden dann jedoch nur die zum jeweiligen Unterprofil passenden Maßnahmen (modernisiert: Anforderungen) ausgewählt (siehe Orientierungshilfe in Abschnitt 6.2).

Aus diesem Grund muss die Auswahl von Maßnahmen eines Bausteins für alle relevanten Anwendungsfälle – über alle Unterprofile hinweg – gemeinsam betrachtet werden. Häufig lässt sich so die Nichtauswahl einer Maßnahme für einen Anwendungsfall damit begründen, dass sie nur bei Zutreffen eines anderen Anwendungsfalls relevant ist.

In Tab. 6.4 wurde die unterprofilübergreifende Maßnahmenauswahl am Beispiel des Bausteins B 1.0 durchgeführt. Dabei sind in den Tabellenzeilen alle Maßnahmen des Bausteins aufgelistet. Es wird die Nummer der Maßnahme, ihr Titel sowie ihre Qualifizierungsstufe angegeben. Mögliche Qualifizierungsstufen sind A (Einstieg), B (Aufbau), C (Zertifikat), Z (zusätzlich) und W (Wissen). Nur die Stufen A bis C sind für eine Qualifizierung nach IT-Grundschutz bzw. ISO 27001 notwendig.

In den Tabellenspalten sind die Anwendungsfälle aufgeführt, für die mindestens eine Maßnahme des Bausteins ausgewählt wurde. Ein grün eingefärbtes Feld kennzeichnet die Auswahl der Maßnahme für den Anwendungsfall. Ist das Feld zusätzlich mit einem „K“ gekennzeichnet, wurde die Maßnahme nur dann ausgewählt, wenn das mit dem Baustein modellierte Zielobjekt einen hohen Schutzbedarf hat. Da das Kriterium für einen hohen Schutzbedarf in dem in dieser Arbeit erstellten Profil die Zugehörigkeit zu den kritischen Infrastrukturen ist (siehe Abschnitte 3.4 und 6.1), werden mit „K“ gekennzeichnete Maßnahmen nur für kritische Infrastrukturen (KRITIS) ausgewählt.

Tab. 6.4: Maßnahmenauswahltabelle am Beispiel des Bausteins B 1.0: Sicherheitsmanagement

Maßnahmen des Bausteins B 1.0: Sicherheitsmanagement: = Im Hauptprofil (HP) oder im Unterprofil UA ausgewählt K = Nur für KRITIS / hohen Schutzbedarf ausgewählt			**Anwendungsfälle:**			
			HP	**UA3**	**UA4**	**UA5**
M 2.192	A	Erstellung einer Leitlinie zur Informationssicherheit				
M 2.193	A	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit				
M 2.195	A	Erstellung eines Sicherheitskonzeptes				
M 2.197	A	Integration der Mitarbeiter in den Sicherheitsprozess				
M 2.199	A	Aufrechterhaltung der Informationssicherheit				
M 2.200	C	Management-Berichte zur Informationssicherheit	K			
M 2.201	C	Dokumentation des Sicherheitsprozesses	K			
M 2.335	A	Festlegung der Sicherheitsziele und -strategie				
M 2.336	A	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene				
M 2.337	A	Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse				
M 2.338	Z	Erstellung von zielgruppengerechten Sicherheitsrichtlinien				
M 2.339	Z	Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit				
M 2.475	A	Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten				
M 6.16	Z	Abschließen von Versicherungen				

Die Auswahl der Maßnahmen orientiert sich am branchenspezifischen Sicherheitsstandard Wasser / Abwasser (B3S WA) für die Wasserwirtschaft. Sie wurde im Rahmen der Gremienarbeit der DWA und des DVGW durch „Fachleute aus den Bereichen Trinkwasserversorgung und Abwasserentsorgung“ durchgeführt [B3S17b].

6.3.2.1 Begründung der Nichtauswahl von Maßnahmen für den Baustein B 1.0

Es gibt vier mögliche Gründe für die Nichtauswahl von Maßnahmen durch den B3S WA, auf die im Folgenden durch Nennung der vorangestellten Kennziffer Bezug genommen wird:

1. **Für Zielgruppe nicht relevant.** Die Maßnahme ist für die Zielgruppe (Wasserwirtschaft) i.A. nicht relevant.
2. **Redundant zu anderen Regelwerken.** Die Maßnahme wurde bereits im Merkblatt zum B3S WA beschrieben bzw. wird durch andere Regelwerke von DWA / DVGW abgedeckt.
3. **Qualifizierungsstufe Z.** Die Maßnahme hat die Qualifizierungsstufe Z und ist somit für die Qualifizierung nach IT-Grundschutz oder ISO 27001 nicht notwendig; sie stellen Ergänzungen dar [BSI16a]. Diese Maßnahmen wurden i.A. nicht ausgewählt.
4. **Durch übergeordnete Maßnahme abgedeckt.** Die Maßnahme ist ein Spezialfall einer übergeordneten Maßnahme, die ausgewählt wurde.

In Tab. 6.5 sind die Begründungen für alle nicht ausgewählten Maßnahmen des Bausteins B 1.0 im Einzelnen aufgeführt.

Tab. 6.5: Begründung der Nichtauswahl von Maßnahmen für den Baustein B 1.0

Nicht ausgewählte Maßnahme	Begründung (Kennziffer)
M 2.338: Erstellung von zielgruppengerechten Sicherheitsrichtlinien	**Qualifizierungsstufe Z (3)**
M 2.339: Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit	**Qualifizierungsstufe Z (3)**
M 2.475: Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten	**Für Zielgruppe nicht relevant (1)**: Für die Zielgruppe der Wasserwirtschaft wird i.A. kein externer IT-Sicherheitsbeauftragter bestellt. Sollte dies im Einzelfall dennoch der Fall sein, sollte die Maßnahme zusätzlich ausgewählt werden.
M 6.16: Abschließen von Versicherungen	**Qualifizierungsstufe Z (3)**

Was im in dieser Arbeit erstellten Profil anwendungsfallübergreifende Zielobjekte sind, ist im B3S WA als zusätzlicher Anwendungsfall *Organisation und Management (OM)* zusammengefasst. Die Maßnahmen M 2.193: Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit und M 2.336: Übernahme der Gesamtverantwortung für Informationssicherheit

durch die Leitungsebene werden sowohl für diesen Anwendungsfall OM als auch für die Anwendungsfälle UA3 bis UA5 ausgewählt [B3S17a]. UA3 bis UA5 sind die Anwendungsfälle, bei denen der Benutzerzugang aus der Ferne möglich ist.

Für das in dieser Arbeit erstellte IT-Grundschutz-Profil ist dies eine redundante Auswahl, da die Maßnahmen des B3S-Anwendungsfalls OM innerhalb des Profils dem Hauptprofil zugeordnet werden und damit für jede Institution durchzuführen sind – egal, welche Anwendungsfälle in den Unterprofilen ausgewählt werden. Für das IT-Grundschutz-Profil wird deswegen von der erneuten Auswahl der beiden Maßnahmen im Unterprofil UA abgesehen.

Anmerkung: Änderungen durch die Modernisierung des IT-Grundschutzes:

Im modernisierten IT-Grundschutz wird es keine übergreifenden Maßnahmen mehr geben, die in verschiedenen Bausteinen empfohlen werden; vielmehr werden die Maßnahmen für jeden Baustein spezifisch sein. Auch werden keine konkreten Maßnahmen, sondern Anforderungen formuliert. Ebenso wird es die Qualifizierungsstufen nicht mehr geben; stattdessen werden die Anforderungen in Basisanforderungen, Standardanforderungen und Anforderungen für erhöhten Schutzbedarf eingeteilt (siehe Abschnitt 2.2; insbesondere Tab. 2.1 und Tab. 2.2).

Die Maßnahmen- beziehungsweise Anforderungslisten der neuen Bausteine werden sich somit von den bisherigen erheblich unterscheiden – folglich muss bei Verwendung modernisierter Bausteine auch die Anforderungsauswahl erneut begründet werden. Da zum Zeitpunkt der Niederschrift dieser Arbeit die neuen Bausteine jedoch nicht vollständig vorlagen, kann in dieser Arbeit lediglich das Prinzip der Maßnahmenauswahl an Bausteinen des bisherigen IT-Grundschutzes beispielhaft erläutert werden.

6.3.2.2 Nicht berücksichtigte Gefährdungen für den Baustein B 1.0

Während der Profilerstellung sollten für jeden Baustein eventuelle nicht berücksichtigte Gefährdungen mitsamt der Begründung für die Nichtberücksichtigung notiert werden. Diese werden später für die Risikobehandlung benötigt. In der vorliegenden Arbeit wird die Identifikation nicht berücksichtigter Gefährdungen für die beispielhaft ausgewählten Bausteine B 1.0 und B 3.302 durchgeführt.

Die folgende Identifikation der nicht berücksichtigten Gefährdungen dient allein der Profilerstellung, nicht aber der Profilanwendung, und findet sich somit nicht in dem im Rahmen dieser Arbeit erstellen IT-Grundschutz-Profil wieder. Ihre Ergebnisse werden jedoch im Abschnitt *Risikobehandlung* des Hauptprofils aufgegriffen (siehe Abschnitt 6.6.2 dieser Arbeit).

Die Entscheidung, welche Gefährdungen für die Wasserwirtschaft relevant sind, hat für den B3S WA – genau wie die Auswahl der relevanten Maßnahmen – eine Befragung von Fachleuten aus der Wasserwirtschaft ergeben [B3S17b].

Eine nicht berücksichtigte Gefährdung eines Bausteins ist eine Gefährdung,

- deren zugeordnete Maßnahme nicht ausgewählt wurde und
- die durch keine andere, ausgewählte Maßnahme des Bausteins abgedeckt wird.

Eine Zuordnung der Maßnahmen zu den Gefährdungen findet sich (für den bisherigen IT-Grundschutz) in den Kreuzreferenztabellen [BSI16c].

Tab. 6.6 zeigt die Kreuzreferenztabelle für den Baustein B 1.0: Sicherheitsmanagement.

Die Maßnahmen stehen in den Zeilen, die Gefährdungen in den Spalten. Ein Kreuz kennzeichnet die Zuordnung einer Maßnahme zu einer Gefährdung. Die für dieses Profil ausgewählten Maßnahmen sind grün hinterlegt. Eine nicht berücksichtigte Gefährdung ist demnach dadurch gekennzeichnet, dass in ihrer Spalte KEIN Kreuz im grün hinterlegten Gebiet liegt. Für nicht berücksichtigte Gefährdungen ist in Tab. 6.6 eine orangefarbene Hinterlegung vorgesehen.

Den vier nicht ausgewählten Maßnahmen sind jedoch lediglich Gefährdungen zugeordnet, die bereits durch andere, ausgewählte Maßnahmen des Bausteins B 1.0 abgedeckt werden. Somit ergeben sich durch die Nichtauswahl für diesen Baustein keine nicht berücksichtigten Gefährdungen.

Tab. 6.6: Kreuzreferenztabelle mit Markierung ausgewählter Maßnahmen für den Baustein B 1.0: Sicherheitsmanagement (nach [BSI16c], farbliche Hinterlegung durch die Verfasserin)

B 1.0	G 2.66	G 2.105	G 2.106	G 2.107
M 2.192	X	X	X	
M 2.193	X			X
M 2.195	X			
M 2.197	X			
M 2.199	X	X		X
M 2.200	X			
M 2.201	X			
M 2.335	X		X	X
M 2.336	X	X	X	X
M 2.337	X			
M 2.338	X			
M 2.339		X		X
M 2.475	X			X
M 6.16		X	X	

6.4 Modellierung für das Unterprofil AR (Architektur)

Analog zu Abschnitt 6.3, in dem die Zielobjekte des Hauptprofils mit Bausteinen modelliert und für einen Baustein beispielhaft die Maßnahmenauswahl vorgeführt wurde, soll dies nun für das Unterprofil AR (Architektur) geschehen. Das Vorgehen und der Aufbau der Tabellen entsprechen Abschnitt 6.3, weshalb sie in diesem Abschnitt nicht erneut erläutert werden.

6.4.1 Auswahl von IT-Grundschutz-Bausteinen

Tab. 6.7 zeigt die Bausteinmodellierung der für das Unterprofil AR ausgewählten Zielobjekte (siehe Abschnitt 4.6.3, Tab. 4.4).

Für das Unterprofil AR sind Maßnahmen für die Netzkomponenten und die Sicherheitskomponenten vorrangig, wie in Abschnitt 6.2.1 erläutert. Diese Komponenten wurden deswegen mit den für sie spezifischen Bausteinen **B 3.302: Router und Switches**, **B 3.301: Firewall**, **B 4.4: VPN** und **B 5.18: DNS-Server** modelliert, um spezifische Maßnahmen auswählen zu können.

Tab. 6.7: Modellierungstabelle für die Zielobjekte des Unterprofils AR

Nr.	Zielobjekt	Modellierung mit Bausteinen					
		B 4.1 Lokale Netze	B 1.9 Hard-/Software-management	B 3.302 Router und Switches	B 3.301 Firewall	B 4.4 VPN	B 5.18 DNS-Server
IT-Systeme							
IT1	Feldgerät						
IT2	SPS						
IT3	HMI						
IT4	Historian						
IT5	Engineering-WS						
IT6	Control Server						
IT7	Webserver						
IT8	Mobilgerät						
IT9	Externe Komponente						
IT10	Office-IT-Komponente						
Netzkomponenten							
N1	Switch						
N2	Router						
N3	Modem						
N4	IT-Verkabelung						
N5	Feldbus						
N6	Fernwartung						
Sicherheit							
S1	Firewall						
S2	VPN						
S3	IDS / IPS						

Die IT-System-Komponenten, darunter insbesondere alle ICS-Komponenten, sind im Unterprofil AR nur insofern relevant, dass der Aufbau einer geeigneten Architektur sich an ihren Anforderungen orientiert. Sie werden deshalb von den komponentenübergreifenden Bausteinen **B 4.1: Lokale Netze** und **B 1.9: Hard- und Softwaremanagement** modelliert (so wie die Netz- und Sicherheitskomponenten auch), jedoch nicht mit spezifischen Bausteinen. Dies erfolgt in anderen Unterprofilen, in denen spezifische Maßnahmen für die IT-Systeme empfohlen werden (siehe Abgrenzung der Maßnahmentypen für die Unterprofile in Abschnitt 6.2).

Dieses Vorgehen lässt sich für die Erstellung weiterer Profilge zu einer Faustformel verallgemeinern: *Ein Zielobjekt sollte in einem Unterprofil nur dann mit seinem spezifischen Baustein modelliert werden, wenn im Unterprofil spezifische Maßnahmen für dieses Zielobjekt ergriffen werden sollen*.

6.4.2 Auswahl umzusetzender Maßnahmen (Anforderungen) am Beispiel des Bausteins B 3.302

In Tab. 6.8 findet sich die Maßnahmenauswahl am Beispiel des Bausteins B 3.302: Router und Switches. Die Auswahl orientiert sich am branchenspezifischen Sicherheitsstandard Wasser / Abwasser (B3S WA) [B3S17a].

Der Baustein wird neben dem Unterprofil AR (Architektur) auch im Unterprofil NM (Netzmanagement) verwendet. Die ausgewählten Maßnahmen verteilen sich über alle sechs Anwendungsfälle der beiden Unterprofile.

Entsprechend der Orientierungshilfe in Abschnitt 6.2 wurden Maßnahmen, bei denen es um die Funktion der Router und Switches für den Aufbau und die Absicherung der Architektur geht, dem Unterprofil AR zugeordnet. Maßnahmen, bei denen der Betrieb der Router und Switches selbst im Vordergrund steht, gehören zum Unterprofil NM.

Tab. 6.8: Maßnahmenauswahltabelle am Beispiel des Bausteins B 3.302: Router und Switches

Maßnahmen des Bausteins B 3.302: Router und Switches:			**Anwendungsfälle:**				
		= In einem Unterprofil ausgewählt	**AR 1**	**AR 2,3**	**NM 1**	**NM 2**	**NM 3**
K		= Nur für KRITIS / hohen Schutzbedarf ausgewählt					
M 1.43	A	Gesicherte Aufstellung aktiver Netzkomponenten					
M 2.276	Z	Funktionsweise eines Routers					
M 2.277	Z	Funktionsweise eines Switches					
M 2.278	Z	Typ. Einsatzszenarien v. Routern/Switches					
M 2.279	A	Erstellung einer Sicherheitsrichtlinie für Router und Switches					
M 2.280	C	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches	K	K			
M 2.281	A	Dokumentation der Systemkonfiguration von Routern und Switches					
M 2.282	A	Regelmäßige Kontrolle von Routern und Switches					
M 2.283	B	Software-Pflege auf Routern und Switches					K
M 2.284	C	Sichere Außerbetriebnahme von Routern und Switches				K	K
M 3.38	B	Administratorenschulung für Router und Switches			K	K	K
M 4.201	A	Sichere lokale Grundkonfiguration von Routern und Switches					
M 4.202	A	Sichere Netz-Grundkonfiguration von Routern und Switches					
M 4.203	A	Konfigurations-Checkliste für Router und Switches					
M 4.204	C	Sichere Administration von Routern und Switches				K	K
M 4.205	C	Protokollierung bei Routern und Switches				K	K
M 4.206	C	Sicherung von Switch-Ports		K			
M 5.111	C	Einrichtung von Access Control Lists auf Routern					K
M 5.112	C	Sicherheitsaspekte von Routing-Protokollen					
M 6.91	C	Datensicherung und Recovery bei Routern und Switches	K	K			
M 6.92	C	Notfallvorsorge bei Routern und Switches			K	K	K

6.4.2.1 Begründung der Nichtauswahl von Maßnahmen für den Baustein B 3.302

Es gibt vier mögliche Gründe für die Nichtauswahl von Maßnahmen durch den B3S WA, auf die im Folgenden durch Nennung der vorangestellten Kennziffer Bezug genommen wird:

1. **Für Zielgruppe nicht relevant.** Die Maßnahme ist für die Zielgruppe (Wasserwirtschaft) i.A. nicht relevant.
2. **Redundant zu anderen Regelwerken.** Die Maßnahme wurde bereits im Merkblatt zum B3S WA beschrieben bzw. wird durch andere Regelwerke von DWA / DVGW abgedeckt.
3. **Qualifizierungsstufe Z.** Die Maßnahme hat die Qualifizierungsstufe Z und ist somit für die Qualifizierung nach IT-Grundschutz oder ISO 27001 nicht notwendig; sie stellen Ergänzungen dar [BSI16a]. Diese Maßnahmen wurden i.A. nicht ausgewählt.
4. **Durch übergeordnete Maßnahme abgedeckt.** Die Maßnahme ist ein Spezialfall einer übergeordneten Maßnahme, die ausgewählt wurde.

In Tab. 6.9 sind die Begründungen für alle nicht ausgewählten Maßnahmen des Bausteins B 3.302 im Einzelnen aufgeführt.

Tab. 6.9: Begründung der Nichtauswahl von Maßnahmen für den Baustein B 3.302

Nicht ausgewählte Maßnahme	Begründung (Kennziffer)
M 2.276: Funktionsweise eines Routers	**Qualifizierungsstufe Z (3)**
M 2.277: Funktionsweise eines Switches	**Qualifizierungsstufe Z (3)**
M 2.278: Typische Einsatzszenarien von Routern und Switches	**Qualifizierungsstufe Z (3)**
M 2.279: Erstellung einer Sicherheitsrichtlinie für Router und Switches	**Durch übergeordnete Maßnahme abgedeckt (4)**: M 2.192: Erstellung einer Leitlinie zur Informationssicherheit (Baustein B 1.0)
M 4.201: Sichere lokale Grundkonfiguration von Routern und Switches	**Durch übergeordnete Maßnahme abgedeckt (4)**: M 4.202: Sichere Netz-Grundkonfiguration von Routern und Switches (Baustein B 3.302)
M 5.112: Sicherheitsaspekte von Routing-Protokollen	**Durch übergeordnete Maßnahme abgedeckt (4)**: M 5.39: Sicherer Einsatz der Protokolle und Dienste (Baustein B 3.301)

6.4.2.2 Nicht berücksichtigte Gefährdungen für den Baustein B 3.302

Tab. 6.10 ist die Kreuzreferenztabelle für den Baustein B 3.302: Router und Switches. Die Maßnahmen stehen in den Zeilen, die Gefährdungen in den Spalten. Ein Kreuz kennzeichnet die Zuordnung einer Maßnahme zu einer Gefährdung. Die für dieses Profil ausgewählten Maßnahmen sind grün hinterlegt. Eine nicht berücksichtigte Gefährdung ist demnach dadurch gekennzeichnet, dass in ihrer Spalte KEIN Kreuz im grün hinterlegten Gebiet liegt. Nicht berücksichtigte Gefährdungen sind orange hinterlegt.

Die meisten der nicht ausgewählten Maßnahmen sind Gefährdungen zugeordnet, die auch durch andere, ausgewählte Maßnahmen des Bausteins abgedeckt werden. Es gibt zwei Ausnahmen:

- Die Nichtauswahl der Maßnahme M 2.279: Erstellung einer Sicherheitsrichtlinie für Router und Switches führt zur Nichtberücksichtigung der Gefährdung **G 2.1: Fehlende oder unzureichende Regelungen** für den Baustein B 3.302: Router und Switches.
- Die Nichtauswahl der Maßnahme M 5.112: Sicherheitsaspekte von Routing-Protokollen führt zur Nichtberücksichtigung der Gefährdung **G 5.51: Missbrauch der Routing-Protokolle** für den Baustein B 3.302: Router und Switches.

Beide Gefährdungen werden innerhalb des B3S WA auch durch keine ausgewählte Maßnahme eines anderen Bausteins behandelt.

Diese nicht berücksichtigten Gefährdungen sollten für die Erstellung des Profilabschnitts zur ergänzenden Risikoanalyse für das Restrisiko (Abschnitt 6.6.2) notiert werden.

Tab. 6.10: Kreuzreferenztabelle mit Markierung ausgewählter Maßnahmen und nicht berücksichtigter Gefährdungen für den Baustein B 3.302: Router und Switches (nach [BSI16c], farbliche Hinterlegung durch die Verfasserin)

B 3.302	G 2.1	G 2.3	G 2.4	G 2.22	G 2.27	G 2.44	G 2.54	G 2.98	G 3.64	G 3.65	G 4.49	G 5.4	G 5.51	G 5.66	G 5.112	G 5.113	G 5.114	G 5.115
M 1.43												X						
M 2.276								X										
M 2.277								X										
M 2.278								X										
M 2.279	X																	
M 2.280		X				X		X										
M 2.281					X													
M 2.282			X															
M 2.283						X			X	X	X							
M 2.284							X											
M 3.38									X	X								
M 4.201									X		X							
M 4.202									X		X				X	X		X
M 4.203									X		X							
M 4.204										X					X		X	X
M 4.205				X														
M 4.206														X				
M 5.111										X								
M 5.112													X					
M 6.91										X								
M 6.92										X								

6.5 Umsetzungsvorgaben

Nachdem bei der Erstellung eines IT-Grundschutz-Profils Anforderungen ausgewählt wurden, können Vorgaben gemacht werden, wie diese Anforderungen zu erfüllen sind. In der Regel sind dies Verweise auf geeignete Maßnahmen. Dabei bestehen grundsätzlich drei Möglichkeiten:

- Kein Hinweis: Wie die Anforderung erfüllt wird, liegt im Ermessen der Anwender.
- Referenzierung eines Umsetzungshinweises innerhalb des IT-Grundschutzes.
- Referenzierung einer Quelle außerhalb des IT-Grundschutzes oder eigene Maßnahmenempfehlung.

Umsetzungshinweise sind ein Konzept des modernisierten IT-Grundschutzes, um zu den Anforderungen der Bausteine konkrete Maßnahmen zu empfehlen. Die bisherigen IT-Grundschutz-Bausteine enthalten keine Anforderungen, sondern direkt konkrete Maßnahmen. Aus diesem Grund sind im Rahmen dieser Arbeit, in der noch nicht mit modernisierten Bausteinen gearbeitet werden kann, Umsetzungsvorgaben in der Regel nicht notwendig. Trotzdem soll im folgenden Abschnitt 6.5.1 ein Beispiel gegeben werden, wie Netzpläne Umsetzungsvorgaben veranschaulichen können.

6.5.1 Netzpläne zur Veranschaulichung von Umsetzungsvorgaben

Netzpläne können nicht nur der Veranschaulichung des Status Quo zur Identifikation zutreffender Anwendungsfälle dienen, sondern auch der Veranschaulichung einer wünschenswerten Architektur als Orientierungshilfe oder Umsetzungsvorgabe.

Ein Beispiel für das in dieser Arbeit erstellte Unterprofi AR: In Abschnitt 5.4 wurde eine empfehlenswerte Architektur anhand der Referenzarchitekturen des Anwendungsfalls AR entwickelt. Das Ergebnis wurde am Ende des Abschnitts 5.4.2 in Abb. 5.5 bereits vorgestellt. Der Netzplan dieser Architektur kann als anschauliche Umsetzungsvorgabe für diejenigen Maßnahmen dienen, die sich mit der Netzsegmentierung und der Absicherung der Segmentgrenzen befassen. Dies sind – im bisherigen IT-Grundschutz – die für das Unterprofil AR ausgewählten Maßnahmen M 5.61: Geeignete physische Segmentierung, M 5.77: Bildung von Teilnetzen und M 2.204: Verhinderung ungesicherter Netzzugänge.

Die Netzpläne der Umsetzungsvorgaben können bei der Erstellung des Gesamt-Netzplans auf Basis der ausgewählten Anwendungsfälle (siehe Abschnitt 6.6) berücksichtigt werden.

6.6 Branchenspezifische Anpassung der Risikoanalyse

Das im Rahmen dieser Arbeit erstellte IT-Grundschutz-Profil hat das vorherrschende Ziel, für Anwender aus kleineren Institutionen gut handhabbar zu sein.

Eine umfassende Risikoanalyse ist gerade für kleine Unternehmen eine Herausforderung. Aus diesem Grund wird für das in dieser Arbeit erstellte Profil angestrebt, eine Risikoanalyse nur im Ausnahmefall notwendig zu machen. Der IT-Grundschutz ist dafür eine gute Grundlage, da die Bausteine Risikoanalysen bereits implizit enthalten. Wenn der abzusichernde Informationsverbund mit IT-Grundschutz-Bausteinen vollständig modelliert werden kann, ist somit keine Risikoanalyse erforderlich (siehe Abschnitt 2.2.1.3).

Das IT-Grundschutz-Profil basiert auf der Modellierung mit IT-Grundschutz-Bausteinen und folgt somit diesem Prinzip. Im Rahmen des Profils wurden (in Anlehnung an den B3S WA) Maßnahmen aus den Bausteinen ausgewählt, die für eine Institution der Wasserwirtschaft, die normalen Gefährdungen ausgesetzt ist, als notwendig erachtet werden. Eine Nichtauswahl von Maßnahmen der IT-Grundschutz-Bausteine wird explizit begründet.

In der Konsequenz ist für Institutionen, deren ICS-Anlagen das IT-Grundschutz-Profil vollständig abdeckt, keine Risikoanalyse notwendig. Dies gilt unabhängig von der Tatsache, ob die Anlage zu den kritischen Infrastrukturen zählt (also hohen Schutzbedarf hat) oder nicht, denn der hohe Schutzbedarf kritischer Infrastrukturen wurde in der Maßnahmenauswahl des IT-Grundschutz-Profils bereits berücksichtigt. Ob das IT-Grundschutz-Profil die ICS-Anlagen der Anwender vollständig abdeckt, wird durch einen Realitätsabgleich während der Profilanwendung ermittelt (siehe Abschnitt 7.1.1).

Selbst wenn der Realitätsabgleich ein fehlendes Zielobjekt oder einen fehlenden Anwendungsfall offenbart, ist nicht zwingend eine ergänzende Risikoanalyse notwendig. In vielen Fällen reicht die zusätzliche Auswahl eines Bausteins oder die zusätzliche Auswahl einer bisher nicht ausgewählten Maßnahme aus (für genauere Informationen zum Vorgehen bei Abweichungen siehe Abschnitt 7.1.2).

Sollte die ergänzende Risikoanalyse sich dennoch nicht vermeiden lassen, wird im Rahmen des IT-Grundschutz-Profils auf die ergänzende Risikoanalyse verwiesen, die im BSI-Standard 200-3 erläutert ist. Bevor im Rahmen der ergänzenden Risikoanalyse zusätzliche Maßnahmen identifiziert werden können, sind einige Vorarbeiten erforderlich: Das Erstellen einer Gefährdungsübersicht, die Identifikation zusätzlicher Gefährdungen und die Einstufung von Gefährdungen in Risikostufen.

Um Profilanwendern die ergänzende Risikoanalyse möglichst einfach zu machen, werden im Profil branchenspezifische Hilfestellungen zu diesen Vorarbeiten gegeben. Sie sind in den folgenden Abschnitten 6.6.1 bis 6.6.3 aufgeführt.

6.6.1 Gefährdungsübersicht

Die Risikoanalyse soll die im bisherigen Verlauf ausgewählten Anforderungen (Maßnahmen) nur ergänzen. Sind für eine bestimmte Gefährdung bereits ausreichende Maßnahmen gewählt worden, muss sie in der Risikoanalyse nicht mehr berücksichtigt werden. Aus diesem Grund ist für eine ergänzende Risikoanalyse eine Übersicht über im Profil berücksichtigte Gefährdungen wichtig.

Die Information, für welche Gefährdungen die während der Profilanwendung ausgewählten Maßnahmen geeignet sind, findet sich in den Kreuzreferenztabellen am Ende jedes IT-Grundschutz-Bausteins [BSI16a].

Um dem Profilanwender einen mühsamen Abgleich mit den Kreuzreferenztabellen zu ersparen, enthält das Profil für jeden Baustein eine Gefährdungstabelle. In der Tabelle werden alle in der Maßnahmenauswahltabelle des Bausteins gewählten Maßnahmen den Gefährdungen zuordnet, gegen die sie wirken sollen. An dieser Stelle werden – wie schon bei der Maßnahmenauswahl – beispielhaft die Tabellen für die Bausteine B 1.0: Sicherheitsmanagement (Tab. 6.11) und B 3.302: Router und Switches (Tab. 6.12) gezeigt.

Die Legende für die Gefährdungstabellen entspricht der für die Maßnahmenauswahltabellen. Nicht ausgewählte Maßnahmen wurden jedoch aus den Gefährdungstabellen entfernt und jede Maßnahme einer oder mehreren orangefarben hinterlegten Gefährdungen zugeordnet.

Durch orangefarben hinterlegte Felder am rechten Tabellenrand ist gekennzeichnet, in welchen Anwendungsfällen eine Gefährdung relevant ist (orange) und welche Maßnahmen dagegen ausgewählt wurden (grün). Wurden für eine Gefährdung nur für kritische Infrastrukturen (KRITIS) Gegenmaßnahmen gewählt, sind auch die orangefarbenen Felder zusätzlich mit einem „K“ gekennzeichnet.

Auf diese Weise lassen sich mit den Gefährdungstabellen die berücksichtigten Gefährdungen für die individuell ausgewählten Anwendungsfälle schnell erfassen, sodass mit der Identifikation zusätzlicher Gefährdungen begonnen werden kann.

Tab. 6.11: Gefährdungstabelle für den Baustein B 1.0: Sicherheitsmanagement

Gefährdungen des Bausteins B 1.0: Sicherheitsmanagement: = Gefährdung für das Hauptprofil (HP) K = Gegenmaßnahme nur für KRITIS / hohen Schutzbedarf		**HP**
G 2.66	Unzureichendes Sicherheitsmanagement	
M 2.192	Erstellung einer Leitlinie zur Informationssicherheit	
M 2.193	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	
M 2.195	Erstellung eines Sicherheitskonzeptes	
M 2.197	Integration der Mitarbeiter in den Sicherheitsprozess	
M 2.199	Aufrechterhaltung der Informationssicherheit	
M 2.200	Management-Berichte zur Informationssicherheit	K
M 2.201	Dokumentation des Sicherheitsprozesses	K
M 2.336	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	
M 2.337	Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	
G 2.106	Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen	
M 2.335	Festlegung der Sicherheitsziele und -strategie	

Tab. 6.12: Gefährdungstabelle für den Baustein B 3.302: Router und Switches

Gefährdungen des Bausteins B 3.302: Router und Switches: = Gefährdung in einem Unterprofil K = Gegenmaßnahme nur für KRITIS / hohen Schutzbed.		**Anwendungsfälle:**				
		AR 1	**AR 2,3**	**NM 1**	**NM 2**	**NM 3**
G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	K	K			
M 2.280	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches	K	K			
G 2.4	Unzureichende Kontrolle der Sicherheitsmaßnahmen					
M 2.282	Regelmäßige Kontrolle von Routern und Switches					

G 2.22	Fehlende oder unzureichende Auswertung von Protokolldaten				K	K
M 4.205	Protokollierung bei Routern und Switches				K	K
G 2.27	Fehlende oder unzureichende Dokumentation					
M 2.281	Dokumentation der Systemkonfiguration von Routern und Switches					
G 2.44	Inkompatible aktive Netzkomponenten					K
M 2.283	Software-Pflege auf Routern und Switches					K
G 2.54	Vertraulichkeitsverlust durch Restinformationen				K	K
M 2.284	Sichere Außerbetriebnahme von Routern und Switches				K	K
G 3.64	Fehlerhafte Konfiguration von Routern und Switches			K	K	K
M 3.38	Administratorenschulung für Router und Switches			K	K	K
M 4.202	Sichere Netz-Grundkonfiguration von Routern und Switches					
M 4.203	Konfigurations-Checkliste für Router und Switches					
G 3.65	Fehlerhafte Administration von Routern und Switches	K	K	K	K	K
M 4.204	Sichere Administration von Routern und Switches				K	K
M 5.111	Einrichtung von Access Control Lists auf Routern					K
M 6.91	Datensicherung und Recovery bei Routern und Switches	K	K			
M 6.92	Notfallvorsorge bei Routern und Switches			K	K	K
G 5.4	Diebstahl					
M 1.43	Gesicherte Aufstellung aktiver Netzkomponenten					
G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz		K			
M 4.206	Sicherung von Switch-Ports		K			

6.6.2 Nicht behandelte Gefährdungen und Restrisiko

Einige Gefährdungen werden durch das in dieser Arbeit erstellte IT-Grundschutz-Profil explizit nicht behandelt. Diese Gefährdungen können anhand der Gründe für ihre Nichtbehandlung in folgende **drei Kategorien** unterteilt werden:

1. Die Gefährdungen fallen **nicht in den Geltungsbereich** des Profils beziehungsweise treffen auf die Zielgruppe des Profils nicht zu.
2. Die Gefährdungen fallen in den Geltungsbereich des Profils, werden jedoch bereits **in anderen Regelwerken behandelt**, deren Implementierung vorausgesetzt wird.
3. Die Gefährdungen fallen in den Geltungsbereich des Profils, gegen sie werden jedoch **keine Maßnahmen** unternommen. Stattdessen werden die damit verbundenen Risiken akzeptiert (**Restrisiko**).

Diese Gefährdungen aus den **Kategorien 1 und 2** müssen auch in einer ergänzenden Risikoanalyse nicht berücksichtigt werden. Dazu zählen:

- Gefährdungen, die keine Auswirkungen auf die Erbringung der kritischen Dienstleistung haben. Die Einschränkung des Anlagenbetriebs ist die einzig relevante Schadenskategorie bei der Risikoeinstufung. (Für die Schutzbedarfsfeststellung der Anlage gilt dasselbe, siehe Abschnitt 3.4.1).
- Gefährdungen für die Vertraulichkeit von Daten. Datenschutz ist nicht Ziel des Profils.
- Gefährdungen, die den Zugang zu den (ab)wassertechnischen Anlagen, die Stromversorgung der (ab)wassertechnischen Anlagen und Planung, Bau, Betrieb und Instandhaltung der (ab)wassertechnischen Anlagen betreffen. Für diese Gefährdungen existieren bereits Richtlinien in anderen branchenspezifischen Regelwerken der Wasserwirtschaft. Für ICS-Anlagen, also die Automatisierungstechnik für die (ab)wassertechnischen Anlagen, werden diese Aspekte jedoch berücksichtigt [B3S17c; B3S17b].
- Gefährdungen, die aus mangelnder Qualifikation und Organisation von Mitarbeitern sowie mangelhaftem Risikomanagement entstehen. Auch diese Aspekte sind bereits im Regelwerk der DWA beziehungsweise des DVGW abgedeckt [B3S17c; B3S17b].

Gefährdungen der **dritten Kategorie** können in einer ergänzenden Risikoanalyse berücksichtigt werden, wenn der Profilanwender das mit ihnen verbundene Restrisiko nicht tragen möchte und Gegenmaßnahmen möglich sind.

Die Entscheidung, welche Gefährdungen für die Wasserwirtschaft relevant sind, hat für den B3S WA – genau wie die Auswahl der relevanten Maßnahmen – eine Befragung von Fachleuten ergeben [B3S17b]. Das Ergebnis ist für die beiden in dieser Arbeit exemplarisch behandelten Bausteine (siehe Abschnitte 6.3.2.2, Tab. 6.6 für Baustein B 1.0 und Abschnitt 6.4.2.2, Tab. 6.10 für Baustein B 3.302):

- G 2.1: Fehlende oder unzureichende Regelungen und
- G 5.51: Missbrauch der Routing-Protokolle

Nach der Zusammenstellung aller nicht berücksichtigten Gefährdungen für die einzelnen Bausteine sollte geprüft werden, ob die Gefährdung durch eine ausgewählte Maßnahme in einem

anderen Baustein innerhalb des Profils abgedeckt wird. Dies trifft auf Gefährdung G 2.1 zu, sodass als nicht berücksichtigte Gefährdung für die exemplarisch betrachteten Bausteine nur G 5.51 übrig bleibt.

Eine vollständige Liste der nicht berücksichtigten Gefährdungen unter Berücksichtigung aller Bausteine des Hauptprofils und des Unterprofils AR befindet sich im Anhang des Hauptprofils (im kostenpflichtigen Anhang des IT-Grundschutz-Profils für die Wasserwirtschaft). Sie sollte nach der Erstellung der anderen Unterprofile ergänzt werden.

Es sind Gefährdungen denkbar, die zur dritten Kategorie zählen, weil es keine (ausreichenden) Maßnahmen gegen sie gibt und die resultierenden Risiken deswegen akzeptiert werden *müssen*. Auch solche Gefährdungen sollten im Profil benannt sein. Speziell für die Wasserwirtschaft sind im B3S WA keine solche Gefährdungen angegeben. Jedoch gibt es unabhängig von der Branche Gefährdungen, für die stets ein Restrisiko akzeptiert werden muss:

- Advanced Persistent Threats (APT), also elaborierte, zielgerichtete Angriffe. Sie können präventiv nicht völlig ausgeschlossen werden; ihre Auswirkungen jedoch durch eine schnelle Detektion und Reaktion abgemildert.
- Social Engineering, also das Ausnutzen einer Vertrauensbasis zu Mitarbeitern der zu schützenden Institution. Awareness-Training helfen, Mitarbeiter für solche Angriffe zu sensibilisieren, können sie jedoch nicht komplett ausschließen.

Für die ergänzende Risikoanalyse von ICS-Netzen sei zudem erwähnt, dass Safety-Mechanismen kein adäquater Ersatz für Security-Maßnahmen sind (und umgekehrt). Durch einen Angriff auf (oder ein Versagen von) ICS-Netzen können Safety-Mechanismen außer Kraft gesetzt werden. Aus diesem Grund sollten Safety-Mechanismen einerseits durch Security-Maßnahmen zusätzlich abgesichert werden, andererseits jedoch möglichst wenig auf die Security der ICS-Netze angewiesen sein [KL15].

6.6.3 Risikomatrix

Der nächste Schritt nach der Identifikation von Gefährdungen ist ihre Einstufung in Risikokategorien. Dafür wird im BSI-Standard 200-3 eine Risikomatrix verwendet, wie sie in Abb. 6.1 dargestellt ist.

Die Einstufung erfolgt in Abhängigkeit von Eintrittswahrscheinlichkeit und potenzieller Schadenshöhe einer Gefährdung. Gefährdungen mit einer hohen Eintrittswahrscheinlichkeit und einer hohen Schadenshöhe werden in der Risikomatrix rechts oben verordnet und bekommen somit ein hohes Risiko zugeordnet (rot). Mit sinkender Schadenshöhe und / oder Eintrittswahrscheinlichkeit sinkt auch die Risikoeinstufung zu mittlerem (gelb) oder niedrigem (grün) Risiko.

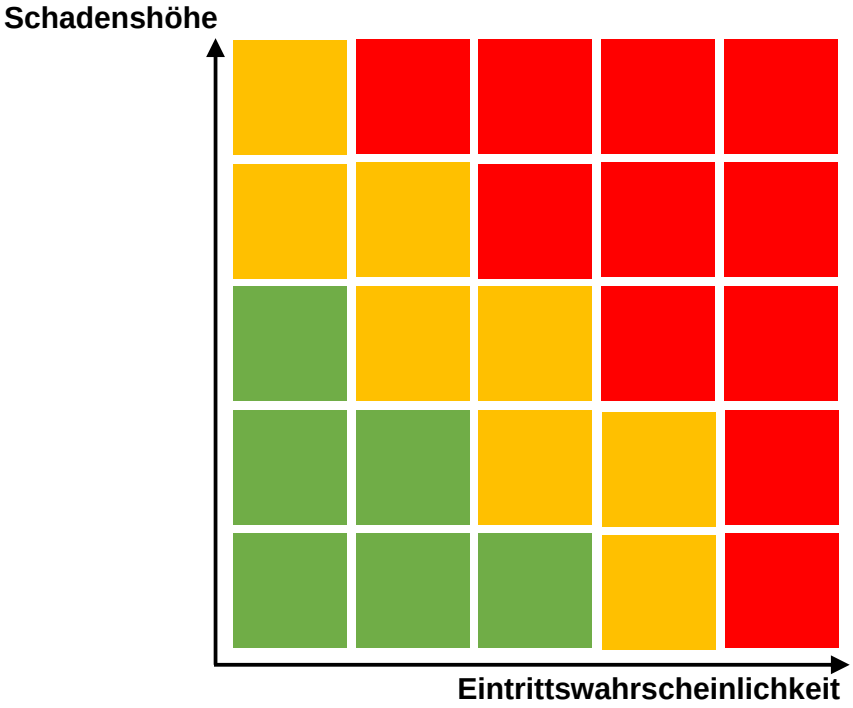


Abb. 6.1: Allgemeine Risikomatrix (angelehnt an [BSI16e])

Der BSI-Standard 200-3 schlägt für die Risikoeinschätzung sowohl für die Eintrittswahrscheinlichkeit als auch für die Schadenshöhe Kategorien vor, die jedoch individuell an die eigene Institution angepasst werden sollten [BSI16e].

In Anlehnung an den B3S WA wird speziell für die Wasserwirtschaft die folgende Anpassung der Risikomatrixdimensionen vorgeschlagen (siehe Abb. 6.2) [B3S17b; B3S17c]:

- **Eintrittswahrscheinlichkeit:**
  - Sehr gering (seltener als einmal in fünf Jahren)
  - Gering (seltener als einmal in zwei Jahren)
  - Mittel (bis zu einmal im Jahr)
  - Hoch (bis zu dreimal im Jahr)
  - Sehr hoch (mehr als dreimal im Jahr)

- **Schadenshöhe = Grad der Einschränkung des Anlagenbetriebs:**
  - Geringe Einschränkung (Anlage mindestens im Standardmodus betreibbar, geringe Einschränkung der Dienstleistungsqualität)
  - Spürbare Einschränkung (Anlage mit geringen Einschränkungen betreibbar, spürbare Einschränkung der Dienstleitungsqualität innerhalb der zulässigen Grenzen)
  - Deutliche Einschränkung (Anlage nicht mehr vollständig betreibbar, Dienstleistungsqualität ist merklich eingeschränkt, die Qualität liegt unterhalb der vorgegebenen Grenzen)

- Erhebliche Einschränkung (Anlage nur noch teilweise betreibbar, Erbringung der Dienstleitung nur noch teilweise möglich, Qualität liegt erheblich unter den vorgegebenen Grenzen)
- Totalausfall (Anlage nicht mehr betreibbar, Dienstleistung kann nicht mehr erbracht werden)

- **Risiko:**
  - Rot (deutlich zu minderndes Risiko)
  - Gelb (einzugrenzendes Risiko)
  - Grün (akzeptables Risiko)
  -

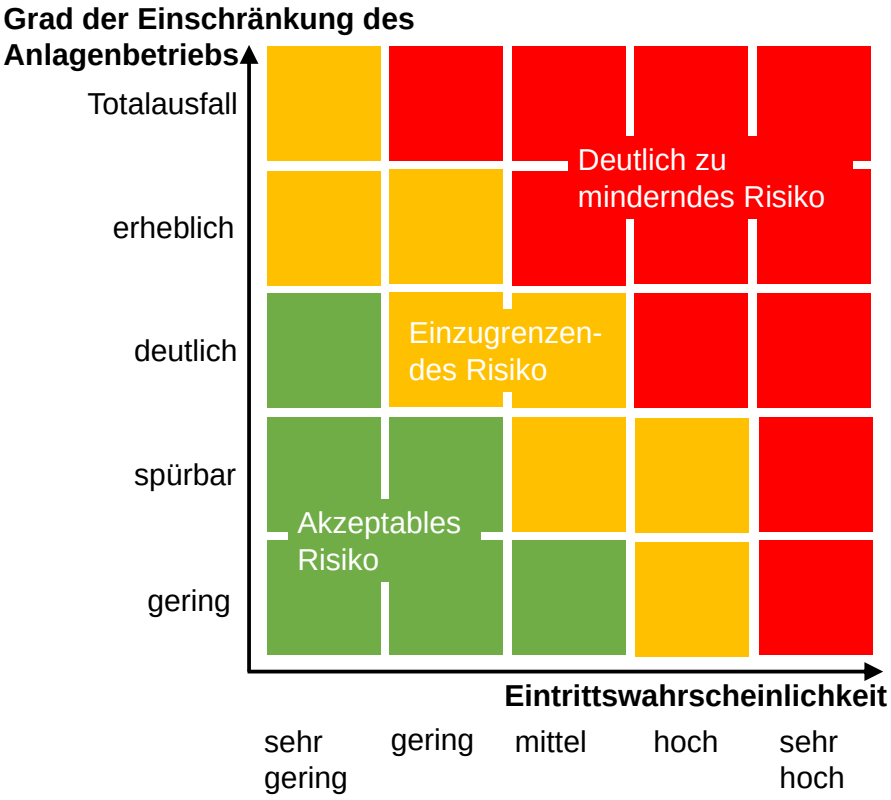
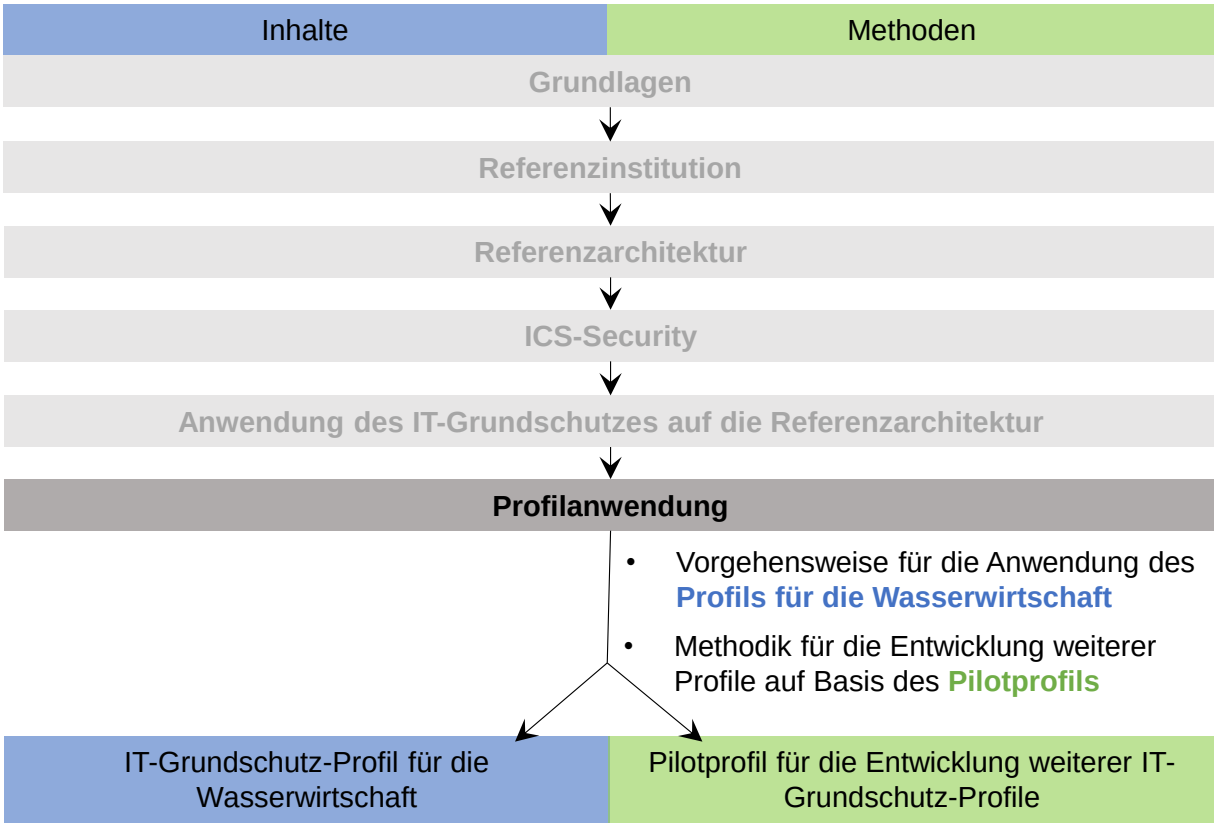


Abb. 6.2: Risikomatrix für die Wasserwirtschaft (angelehnt an [B3S17b])

7 Profilanwendung



Das Profil erfüllt zwei verschiedene Aufgaben. Zum einen soll es ein Pilotprofil sein und damit eine Blaupause für andere Branchen, die ein eigenes IT-Grundschutz-Profil erstellen möchten. Zum anderen soll es den Grundstein für das IT-Grundschutz-Profil für die Wasserwirtschaft legen.

Als Pilotprofil soll das Dokument anhand eines Beispiels aufzeigen, wie ein Profil strukturiert sein kann. Details und Branchenspezifika dienen als anschauliche Beispiele, stehen jedoch nicht im Vordergrund.

Als Profil für die Wasserwirtschaft hingegen ist die Profilstruktur bloß Mittel zum Zweck. Im Vordergrund stehen die branchenspezifischen Details; allen voran die konkreten Maßnahmen (modernisiert: Anforderungen), die die Institutionen der Branche umsetzen sollten, um ein Informationssicherheitskonzept nach Stand der Technik aufzubauen.

Die branchenspezifischen Details enthalten unter anderem Informationen aus dem Branchenspezifischen Sicherheitsstandard Wasser / Abwasser (B3S WA). Der B3S WA ist Teil der Gremienarbeit der DWA, unterliegt somit einer Sperrklausel und ist kostenpflichtig. Profilinhalte, für die Informationen aus dem B3S WA verwendet werden, sind deswegen nicht im Pilotprofil enthalten. Sie werden in einem Anhang zur Verfügung gestellt, der nur für Anwender des konkreten Wasser-Profils, nicht aber für Interessenten des allgemeinen Pilotprofils relevant ist.

Dieses Kapitel erläutert sowohl die Vorgehensweise, um das Profil auf Institutionen der Wasserwirtschaft anzuwenden (Abschnitt 7.1), als auch die Methodik für die Erstellung weiterer Profile auf Basis des Pilotprofils (Abschnitt 7.2).

7.1 Anwendung des IT-Grundschutz-Profils auf eine Institution

In diesem Abschnitt soll mit Hilfe von Fließbildern eine Übersicht gegeben werden, wie das im Rahmen dieser Arbeit erstellte IT-Grundschutz-Profil für die Wasserwirtschaft auf eine konkrete Institution anzuwenden ist.

Des Weiteren wird in den Fließbildern durch farbige Umrandung gekennzeichnet, ob der betreffende Anwendungsschritt mit Hilfe des Hauptprofils (blau) oder Unterprofils (grün) erfolgt. Die Herkunft konkreter verwendeter Dokumente (Tabellen, Listen, Abbildungen oder Erklärungen) ist durch bunte Schriftfarbe gekennzeichnet. Außer Dokumenten aus dem Haupt- und Unterprofil werden auch solche aus dem IT-Grundschutz verwendet (orange). Einige Dokumente müssen vom Anwender selbst erstellt werden (grau). Dokumente mit B3S-Inhalten sind mit einem roten [B3S WA] versehen – sie fallen unter die Sperrklausel und sind im Pilotprofil nur exemplarisch enthalten. Die vollständige Legende der farblichen Kennzeichnung ist in Abb. 7.1 gegeben.

Abb. 7.1: Legende zur Anwendung des IT-Grundschutz-Profils: Unterstützende Dokumente

7.1.1 Vorgehensweise für die Anwendung des Profils

In Abb. 7.2 wird ein Fließbild gegeben, in dem die Vorgehensweise für die Anwendung des IT-Grundschutz-Profils dargestellt ist.

Der erste Schritt bei der Anwendung ist die Auswahl der **Geschäftsprozesse und Anlagen** der eigenen Institution, die durch das Profil abgedeckt werden sollen. Dabei hilft Abschnitt 5 des Hauptprofils.

Danach folgt im zweiten Schritt eine **Schutzbedarfszuweisung** für die betrachteten Anlagen. Diese wird im IT-Grundschutz-Profil in Analogie zur Unterscheidung zwischen KRITIS- und

Nicht-KRITIS-Anlagen in der BSI-KritisV [KritisV16] vorgenommen. Genauere Erläuterungen gibt Abschnitt 5.3 des Hauptprofils.

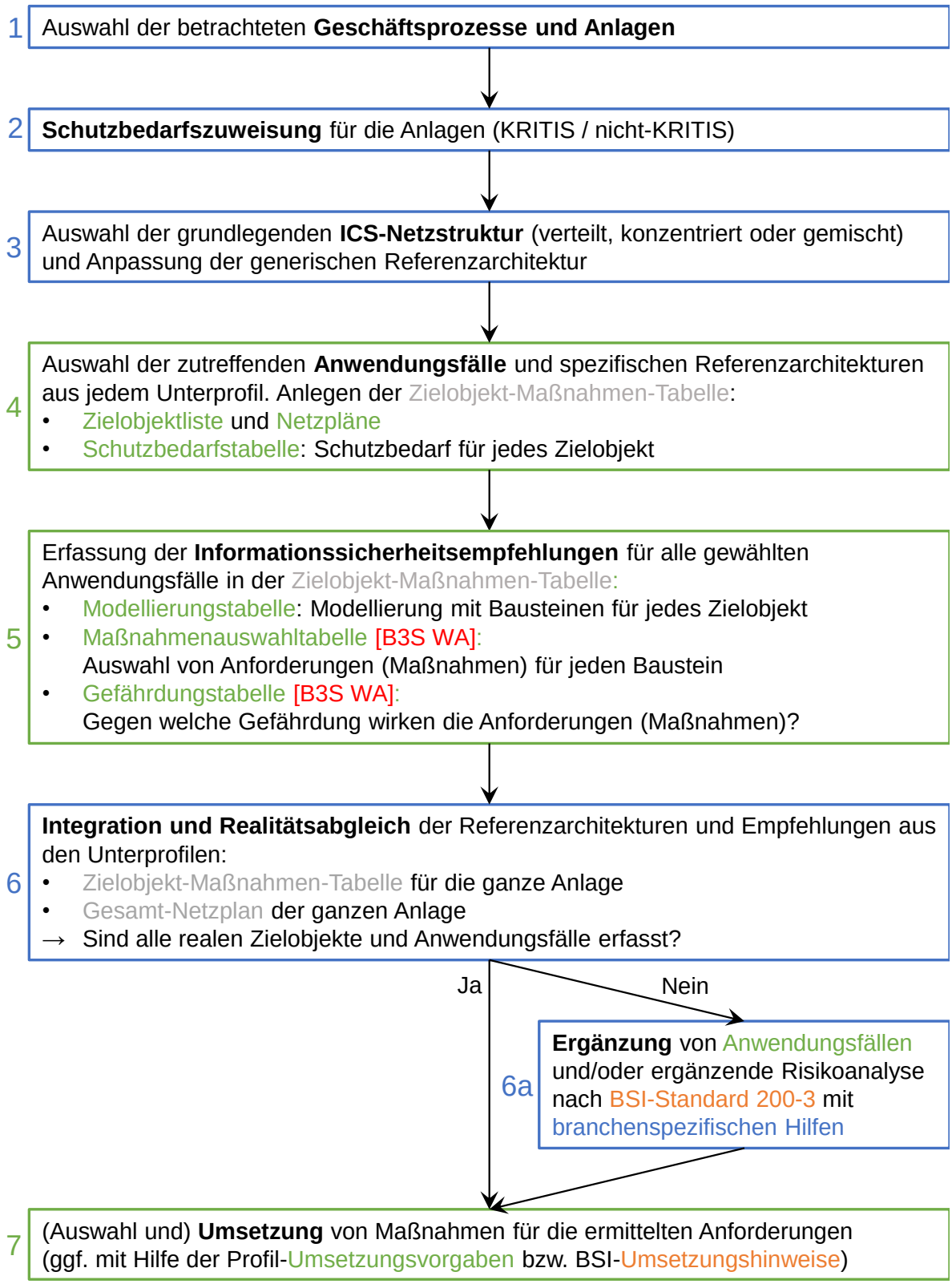


Abb. 7.2: Vorgehensweise für die Anwendung des IT-Grundschutz-Profils

Der dritte und vierte Schritt dienen der genaueren Erfassung der ICS-Anlagenstruktur der eigenen Institution in einer Referenzarchitektur. Dazu wird zunächst die grundlegende **ICS-Netzstruktur** ausgewählt, die der eigenen Anlage am nächsten kommt. Dies kann eine verteilte oder konzentrierte Struktur sein oder auch eine Mischung aus beiden. Die Beschreibung der ICS-Netzstrukturtypen erfolgt in Abschnitt 5.4 des Hauptprofils.

Im vierten Schritt folgt die Auswahl der zutreffenden **Anwendungsfälle** für die eigene Institution, sodass die Details der Referenzarchitektur angepasst werden können. Die Anwendungsfälle sind in Unterprofile gruppiert, die jeweils einen Aspekt der Gesamtanlage abdecken. In der Regel sollte aus jedem Unterprofil mindestens ein Anwendungsfall ausgewählt werden. Dabei hilft Abschnitt UP6 der Unterprofile. Für jeden Anwendungsfall wird im Unterprofil eine Referenzarchitektur, bestehend aus einer Zielobjektliste und einem Netzplan gegeben. In der Schutzbedarfstabelle wird jedem Zielobjekt ein Schutzbedarf zugewiesen.

Im fünften Schritt folgt die Erfassung der **Informationssicherheitsempfehlungen** für die an die eigene Institution angepasste Referenzarchitektur: In jedem Unterprofil gibt es eine Modellierungstabelle, die den Zielobjekten passende IT-Grundschutz-Bausteine zuordnet. Maßnahmenauswahltabellen geben für jeden Baustein – in Abhängigkeit von Anwendungsfall und Schutzbedarf – eine Auswahl der relevanten Anforderungen (bisheriger IT-Grundschutz: Maßnahmen) an.

Die Informationen des vierten und fünften Schritts sollten in einer Zielobjekt-Maßnahmen-Tabelle gesammelt werden. Am Ende der Profilanwendung enthält diese Tabelle in strukturierter Form alle relevanten Informationen für die Maßnahmenumsetzung und potenzielle Risikoanalysen. Ihr Aufbau ist in Tab. 7.1 erklärt.

Tab. 7.1: Aufbau der Zielobjekt-Maßnahmen-Tabelle

Zielobjekt	Anwendungsfall	Baustein	Anforderung (Maßnahme)
1) Aus den spezifischen **Zielobjektlisten**: Alle relevanten Zielobjekte **1b)** Aus den **Schutzbedarfstabellen**: Schutzbedarf der Zielobjekte	**1)** Aus den spezifischen **Zielobjektlisten**: Alle Anwendungsfälle, in denen die Zielobjekte vorkommen	**2)** Aus den **Modellierungstabellen**: Bausteine für die Zielobjekte	**3)** Aus den **Maßnahmenauswahltabellen**: Maßnahmen, die für jeden Baustein (also jedes Zielobjekt) empfohlen sind

Der sechste Schritt besteht aus einer **Integration der Referenzarchitekturen** aus den Unterprofilen und einem **Realitätsabgleich.** Dabei unterstützt Abschnitt 8.1 des Hauptprofils. Zuerst wird die Zielobjekt-Maßnahmen-Tabelle unter Berücksichtigung der anwendungsfallunabhängigen Zielobjekte aus dem Hauptprofil komplettiert. Mit Hilfe der anwendungsfallspezifischen

Netzpläne wird ein Gesamt-Netzplan erstellt. Damit sind alle Voraussetzungen für den anschließenden Realitätsabgleich geschaffen, dessen Ziel eine Überprüfung ist: Sind alle relevanten Zielobjekte der eigenen ICS-Anlage in der Zielobjekt-Maßnahmen-Tabelle erfasst? Sind für alle Zielobjekte alle relevanten Gefährdungen berücksichtigt?

Ist dies nicht der Fall, muss das Profil **ergänzt** werden. Dies kann durch Modifikation eines bestehenden Anwendungsfalls oder Ergänzung eines neuen Anwendungsfalls erfolgen, falls der IT-Grundschutz passende Bausteine enthält. Decken die IT-Grundschutz-Bausteine die fehlenden Zielobjekte oder Gefährdungen nicht ab, kann eine ergänzende Risikoanalyse nach BSI-Standard 200-3 durchgeführt werden. Detaillierte Informationen zur Ergänzung des IT-Grundschutz-Profils enthält Abschnitt 8.2 des Hauptprofils. Abschnitt 8.3 gibt einige Hilfestellungen für den Fall, dass eine ergänzende Risikoanalyse erforderlich ist. Mit den dort gegebenen Gefährdungstabellen kann die Zielobjekt-Maßnahmen-Tabelle um eine Gefährdungsspalte ergänzt werden (siehe Tab. 7.2).

Tab. 7.2: Ergänzung von Gefährdungen in der Zielobjekt-Maßnahmen-Tabelle

Zielobjekt	Anwendungsfall	Gefährdung	Baustein	Anforderung (Maßnahme)
…	…	**4)** Aus den **Gefährdungstabellen**: Gefährdungen, gegen die die empfohlenen Maßnahmen wirken	…	…

Der letzte Schritt gehört nicht mehr zur Anwendung des Profils im engeren Sinne. Er umfasst die (Auswahl und) **Umsetzung** von Maßnahmen, die die ermittelten Anforderungen erfüllen können. Dabei können die Umsetzungshinweise des BSI unterstützen; es können jedoch auch Umsetzungsvorgaben für einzelne Maßnahmen im Abschnitt UP7.3 des zugehörigen Unterprofils angegeben sein.

7.1.2 Vorgehensweise bei Abweichungen vom IT-Grundschutz-Profil

Das IT-Grundschutz-Profil, so wie es in dieser Arbeit konzipiert ist, ermöglicht durch die Vielzahl der Anwendungsfälle in den Unterprofilen eine große Flexibilität für die Anpassung der Profilinhalte an die Institutionen der Anwender. Trotzdem muss die Möglichkeit berücksichtigt werden, dass einzelne Anwender Zielobjekte oder Anwendungsfälle in ihren eigenen ICS-Anlagen identifizieren, die das Profil nicht abdeckt.

In diesem Fall ist bereits im allgemeinen Fließbild in Abb. 7.2 der Schritt 6a für die Ergänzung des Profils vorgesehen. In diesem Abschnitt soll der Schritt 6a mithilfe des Fließbilds in Abb. 7.3 genauer erläutert werden.

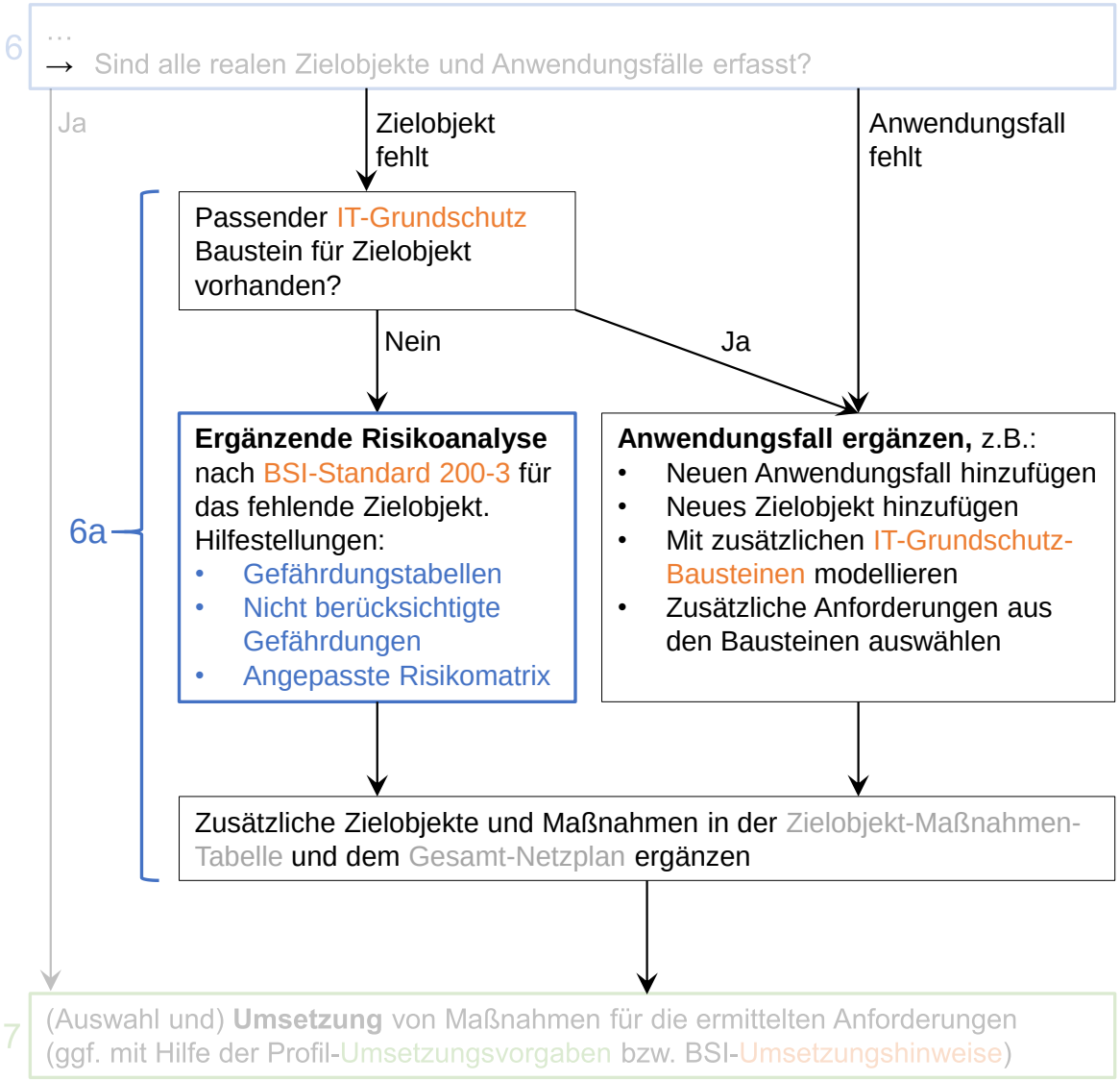


Abb. 7.3: Vorgehensweise bei Abweichung der eigenen ICS-Anlagen von den im Profil wählbaren Referenzarchitekturen

Ob der zusätzliche Arbeitsschritt notwendig ist, zeigt der Realitätsabgleich in Schritt 6. Schritt 6a wird durchgeführt, wenn die ICS-Anlage des Profilanwenders Zielobjekte, Gefährdungen oder Anwendungsfälle aufweist, die das IT-Grundschutz-Profil nicht berücksichtigt. Das Vorgehen unterscheidet sich je nachdem, ob ein fehlender Anwendungsfall oder ein fehlendes Zielobjekt identifiziert wurde:

- Fehlt ein Anwendungsfall, kann er im am ehesten passenden Unterprofil ergänzt werden. Die **Anwendungsfallergänzung** kann aus einem völlig neuen Anwendungsfall bestehen; in den meisten Fällen sollte jedoch die Modifikation eines bestehenden Falles ausreichen. Sie kann darin bestehen, dem Anwendungsfall ein zusätzliches Zielobjekt hinzuzufügen – dies zieht dann auch die Wahl passender IT-Grundschutz-Bausteine für die Modellierung und die Auswahl von nötigen Anforderungen aus die Bau-

steinen nach sich. Möglich sind aber auch die Modellierung eines Zielobjektes mit zusätzlichen Bausteinen oder die Auswahl von zusätzlichen Anforderungen aus bereits zur Modellierung verwendeten Bausteinen.

- Fehlt ein Zielobjekt oder eine Gefährdung, ist es ratsam, zunächst einen Blick ins IT-Grundschutz-Kompendium zu werfen: Gibt es für das fehlende Zielobjekt einen passenden Baustein?
    - Falls ja, kann der Baustein in den relevanten Anwendungsfällen in den Unterprofilen ergänzt werden – dies entspricht der bereits vorgestellten Vorgehensweise zur Anwendungsfallergänzung.
    - Hilft das IT-Grundschutz-Kompendium nicht weiter, muss für das fehlende Zielobjekt oder die zusätzliche Gefährdung eine **ergänzende Risikoanalyse** durchgeführt werden, um eventuell notwendige zusätzliche Maßnahmen zu identifizieren. Dazu bietet der BSI-Standard 200-3 eine detaillierte Anleitung. Dabei unterstützen die branchenspezifischen Hilfestellungen für die Risikoanalyse in Abschnitt 6.6 dieser Arbeit bzw. Abschnitt 8.3 des Hauptprofils.

In jedem Fall sollten zum Abschluss der Ergänzung die zusätzlichen Maßnahmen (modernisiert: Anforderungen) und ggf. zusätzlichen Zielobjekte, Anwendungsfälle oder Bausteine in der Zielobjekt-Maßnahmen-Tabelle ergänzt werden. Mit der nun vollständigen Liste kann zur Umsetzung der Anforderungen in konkrete Maßnahmen in Schritt 7 übergegangen werden. Dabei dient die im Profilverlauf erstellte Zielobjekt-Maßnahmen-Tabelle als individuell an den Profilanwender angepasste Leitlinie, die für jedes Zielobjekt alle umzusetzenden Maßnahmen enthält.

7.1.3 Zugrundeliegende IT-Grundschutz-Vorgehensweise und angestrebtes Schutzniveau

Grundlage für das in dieser Arbeit erstellte IT-Grundschutz-Profil ist die in Abschnitt 2.2.1.2 (Abb. 2.3) vorgestellte IT-Grundschutz-Vorgehensweise der **Standardabsicherung.** Jedoch werden nicht alle Maßnahmen (modernisiert: Basis- und Standard-Anforderungen) empfohlen, sondern eine für die Zielgruppe angemessene Auswahl getroffen.

Institutionen, die nach der BSI-KritisV [KritisV16] zu den kritischen Infrastrukturen (KRITIS) gehören, benötigen für die Erfüllung der Vorgaben des IT-Sicherheitsgesetzes (siehe Abschnitt 3.1.2.3) einen regelmäßigen Nachweis für die Absicherung ihrer IT-Infrastruktur nach Stand der Technik. Die beiden Vorgehensweisen *Basisabsicherung* und *Kernabsicherung* verfolgen zu Anfang der Absicherung eine andere Strategie als die Standardabsicherung; jedoch garantieren sie nur dann eine umfassende Absicherung nach Stand der Technik, wenn sie in der Standardabsicherung münden. Daher bieten sie für eine Branche, die ohnehin in regelmäßigen Abständen eine umfassende Absicherung nachweisen muss, keinen Mehrwert.

Das IT-Grundschutz-Profil betrachtet durch die Eingrenzung seines Geltungsbereichs auf ICS ohnehin schon bevorzugt die „Kronjuwelen“, nämlich die IT, die für die Erbringung der kriti-

schen Dienstleistungen der Wasserwirtschaft verantwortlich ist. Aus diesem Grund ist die Vorgehensweise der **Kernabsicherung**, die die Priorisierung der Absicherung besonders wichtiger IT ermöglicht, in diesem Fall nicht sinnvoll.

Die Vorgehensweise der **Basisabsicherung** (eine schnelle Eliminierung der größten Risiken) ist speziell für kleinere Institutionen der Wasserbranche, die nicht unter die Nachweispflicht der kritischen Infrastrukturen fallen und bislang gar kein Informationssicherheitskonzept haben, grundsätzlich sinnvoll. Dieses IT-Grundschutz-Profil ist jedoch so konzipiert, dass auch bei der Verwendung der Vorgehensweise *Standardabsicherung* kleine Institutionen einen erleichterten Einstieg haben: Gerade weil sie nicht zu den kritischen Infrastrukturen zählen, bekommen sie einen geringeren Schutzbedarf zugeordnet. Die Folge: Sie müssen nur eine eingeschränkte Anzahl von Maßnahmen umsetzen.

Diese Unterscheidung zwischen KRITIS- und Nicht-KRITIS-Anwendern beruht auf unterschiedlichen Schutzbedarfseinschätzungen für die beiden Anwendergruppen im Rahmen der Standardabsicherung. Aus diesem Grund wird sowohl für KRITIS-Institutionen als auch für Nicht-KRITIS-Institutionen ein Schutzniveau erreicht, das der Standardabsicherung entspricht.

Da zum Zeitpunkt der Niederschrift dieser Masterarbeit die Bausteine des modernisierten IT-Grundschutzes noch nicht fertiggestellt waren, wurde die Vorgehensweise zwar an die der Standardabsicherung angenähert, jedoch mussten die Bausteine des bisherigen IT-Grundschutzes verwendet werden. Bei diesen Bausteinen sind die Maßnahmen nicht in die Kategorien *Basis, Standard* und *erhöhter Schutzbedarf* eingeteilt, die für die Bewertung des Schutzniveaus nach der modernisierten Vorgehensweise erforderlich wären. Eine abschließende Beurteilung des erreichten Schutzniveaus nach dem modernisierten BSI-Standard 200-2 ist somit nicht möglich. Perspektivisch sollte bei der Migration zu den Anforderungen des modernisierten IT-Grundschutzes darauf geachtet werden, dass das Schutzniveau der Standardabsicherung erreicht wird.

7.1.4 ISO 27001-Kompatibilität

Das BSI hat ein „Zertifizierungsschema für Informationssicherheit entwickelt, das die Anforderungen an Managementsysteme für die Informationssicherheit aus ISO/IEC 27001 berücksichtigt und als Prüfkataloge das IT-Grundschutz-Kompendium zugrunde legt.“ Dies wird als ISO 27001-Zertifizierung auf Basis IT-Grundschutz bezeichnet [BSI17b].

Die Zertifizierung ist möglich, wenn mindestens die IT-Grundschutz-Vorgehensweise „Standardabsicherung“ umgesetzt wird. Damit ist das vorliegende Profil, sofern die Migration zu den modernisierten IT-Grundschutz-Bausteinen erfolgt ist, ISO 27001-kompatibel.

7.2 Verwendung des IT-Grundschutz-Profils als Pilotprofil

Das in dieser Arbeit erstellte IT-Grundschutz-Profil kann als Grundlage für die Erarbeitung weiterer Profile durch andere Branchen oder Anwendergruppen dienen. Dieser Abschnitt erläutert das Vorgehen zur Erstellung eines eigenen Profils nach Vorlage des Pilotprofils.

Der IT-Grundschutz bietet durch seinen modularen Aufbau Anwendern die Möglichkeit, ein Sicherheitskonzept für ihre Institution auszuarbeiten, auch wenn sie selbst wenig Vorwissen über IT-Sicherheit haben.

Das IT-Grundschutz-Profil geht noch einen Schritt weiter: Profilanwender sollen ein Sicherheitskonzept für ihre Institution erhalten, auch wenn sie wenig Vorwissen über IT-Sicherheit *und* den IT-Grundschutz haben.

Während für Profil*anwender* möglichst wenig Wissen vorausgesetzt werden sollte, müssen *Ersteller* eines IT-Grundschutz-Profils mit dem IT-Grundschutz vertraut sein. Die Profilerstellung ist in weiten Teilen eine Anwendung des IT-Grundschutzes, nur eben nicht für eine konkrete Institution, sondern für eine verallgemeinerte Gruppe von Institutionen. Die wesentliche Aufgabe der Profilerstellung liegt deswegen in der Auswahl und Aufbereitung der IT-Struktur einer allgemeinen Anwendergruppe, sodass die Anwendung des IT-Grundschutzes wie für eine konkrete, einzelne Institution durchgeführt werden kann. Konkret bedeutet dies die Erarbeitung eines Geltungsbereichs, Informationsverbunds und schließlich einer Referenzarchitektur, die mit IT-Grundschutz-Bausteinen modelliert werden kann.

Die Qualität des Profils steht und fällt deswegen mit der Realitätsnähe der Referenzarchitektur, denn jede Abweichung der Anwenderanlagen gegenüber der Referenzarchitektur des Profils erfordert einen Mehraufwand (und zusätzliche Kenntnisse) des Profilanwenders.

Die hier vorgestellte Methodik für die Profilerstellung beinhaltet zwei Strategien, um eine möglichst passgenaue Referenzarchitektur zu erhalten:

1. Auswahl eines möglichst homogenen Geltungsbereichs und innerhalb dieses Geltungsbereichs klare Abgrenzung eines homogenen Informationsverbunds.
2. Erarbeitung nicht *einer* Referenzarchitektur, sondern *mehrerer* Variationen in Form von Anwendungsfällen, die für den Profilanwender intuitiv auswählbar sind.

7.2.1 Allgemeine Methodik

Abb. 7.4 zeigt die Methodik zur Erstellung eines neuen IT-Grundschutz-Profils nach Vorbild des Pilotprofils. Stellen, an denen Methoden des IT-Grundschutzes (IT-GS) angewendet werden, sind orangefarben markiert.

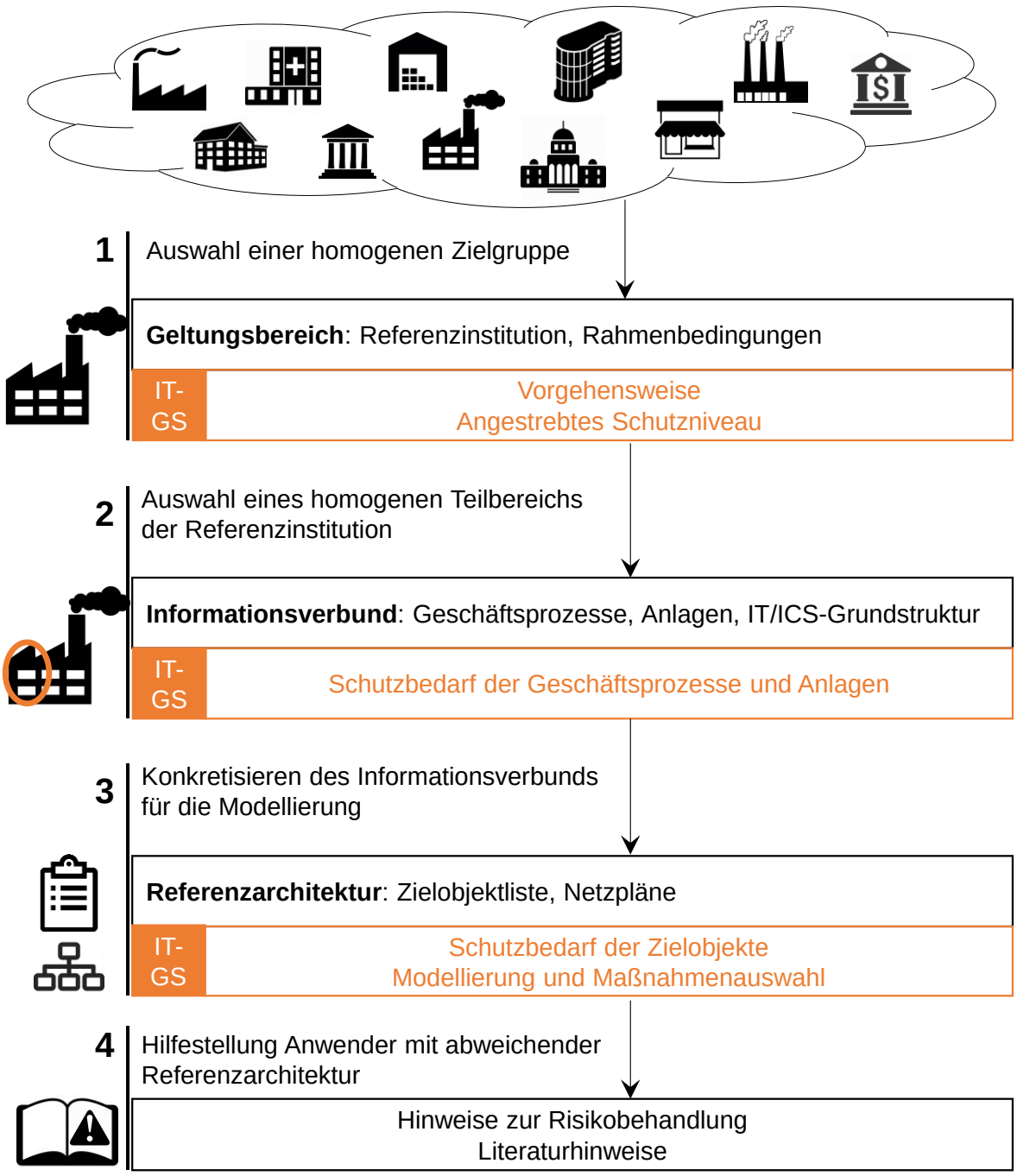


Abb. 7.4: Methodik zur Erstellung eines IT-Grundschutz-Profils nach Vorbild des Pilotprofils

In **Schritt 1** müssen die potenziellen Profilanwender ausgewählt werden. Die Zielgruppe kann eine ganze Branche oder nur Teilbereiche einer Branche enthalten; wichtig ist jedoch, dass sie so homogen wie möglich bezüglich aller Eingrenzungskriterien ist. Gute Eingrenzungskriterien können sich je nach Branche unterscheiden und sowohl organisatorischer als auch technischer Natur sein. Beispiele sind Unternehmensstruktur, Rahmenbedingungen, in der Branche übliche IT beziehungsweise OT oder Netzstrukturen. Am Ende dieses Schrittes sollte ein klar definierter **Geltungsbereich** stehen. Die Zielgruppe kann als eine Referenzinstitution be-

schrieben werden; auch sollten ihre Rahmenbedingungen (Gesetze, Richtlinien) genannt werden. Aus der Perspektive der IT-Grundschutz-Methodik sollten an dieser Stelle die Vorgehensweise nach Standard 200-2 und das angestrebte Schutzniveau ausgewählt werden.

Aus der eingegrenzten Referenzinstitution muss in **Schritt 2** ein konkreter Teilbereich von Geschäftsprozessen ausgewählt werden, die im Rahmen des Profils betrachtet werden sollen. Dazu müssen für die Geschäftsprozesse ggf. die relevanten Anlagen, in jedem Fall jedoch die IT-Grundstruktur erfasst werden (**Informationsverbund**). Die IT-Struktur des gewählten Teilbereichs sollte möglichst homogen innerhalb der Anwendergruppe sein – und nicht zu umfangreich. Vonseiten der IT-Grundschutz-Methodik werden die ausgewählten Geschäftsprozesse an dieser Stelle mit einem Schutzbedarf versehen. Zur Profilerstellung gehört deshalb auch die sinnvolle Einteilung von Schutzbedarfskategorien. Die Schutzbedarfs- und Schadenskategorien des BSI-Standards 200-2 [BSI17b] sind dafür ein guter Ausgangspunkt.

Der folgende **Schritt 3** ist die weitere Konkretisierung des Informationsverbunds zu einer **Referenzarchitektur**. Die Referenzarchitektur, bestehend aus einer Zielobjektliste und einem Netzplan, stellt innerhalb des IT-Grundschutz-Profils das Pendant zu den abzusichernden Objekten einer konkreten Institution dar, die den IT-Grundschutz anwendet. In vielen Fällen wird es nicht möglich sein, eine einzelne Referenzarchitektur festzulegen, da sich die Architekturen selbst innerhalb sehr homogener Anwenderzielgruppen stark unterscheiden. Der folgende Abschnitt 7.2.2 erläutert eine Methodik für die Erstellung einer Referenzarchitektur, die diesen Variationen gerecht wird.

Die Referenzarchitektur ist aus IT-Grundschutz-Perspektive die Grundlage für die Modellierung mit IT-Grundschutz-Bausteinen (im Pilotprofil: Modellierungstabellen) und die Auswahl von Maßnahmen (im Pilotprofil: Maßnahmenauswahltabellen) zur Erstellung eines Sicherheitskonzepts. Die Nichtauswahl von Maßnahmen aus ausgewählten Bausteinen sollte begründet werden. Nicht berücksichtigte Gefährdungen sollten notiert werden, um als Hilfestellung für die ergänzende Risikoanalyse ins Profil einfließen zu können.

Natürlich kann bei der Profilerstellung nicht ignoriert werden, dass es trotz aller Bemühungen Profilanwender geben wird, deren Institution mit den Referenzarchitekturen unzureichend abgebildet wird. Wenn das erstellte Profil von der IT/OT-Architektur einer Institution zu sehr abweicht, müssen Profilanwender eine ergänzende Risikoanalyse nach BSI-Standard 200-3 durchführen.

Für diese Fälle sollte das Profil den Anspruch haben, den Zusatzaufwand auf ein Minimum zu beschränken. Im abschließenden **Schritt 4** sollte der Profilersteller deswegen **Hinweise zur Risikobehandlung** geben, die die Risikoanalyse erleichtern (im Pilotprofil: Abschnitt 8.3) – beispielsweise sinnvolle Matrixdimensionen für die Risikomatrix oder Hinweise auf berücksichtigte Gefährdungen (im Pilotprofil: Gefährdungstabellen), nicht berücksichtigte oder gegebenenfalls zu berücksichtigende Gefährdungen. Für alle Profilanwender können zudem **Literaturhinweise** hilfreich sein.

7.2.2 Methodik zur Berücksichtigung von Variationen in der Referenzarchitektur

In den meisten Fällen wird es nicht möglich sein, einer Profilanwendergruppe mit einer einzigen Referenzarchitektur gerecht zu werden. Das in dieser Arbeit erstellte Pilotprofil sowie diese Methodik bieten deswegen eine Möglichkeit an, mit Variationen in der Referenzarchitektur umzugehen. Die Vorgehensweise dazu ist in Abb. 7.5 veranschaulicht.

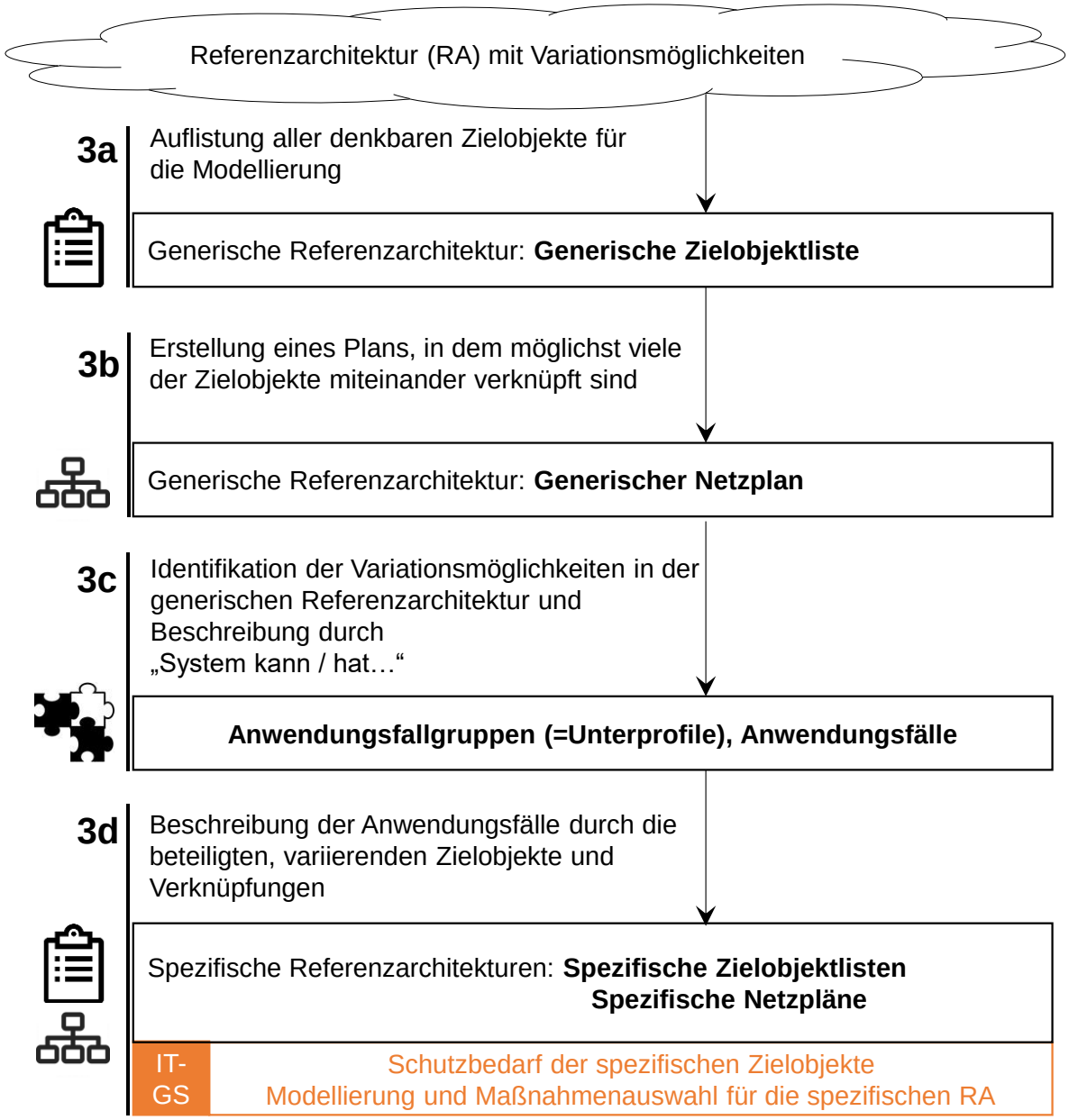


Abb. 7.5: Methodik für die Berücksichtigung von Variationsmöglichkeiten in der Referenzarchitektur anhand von Anwendungsfällen

Die Grundidee für den Umgang mit Variationen ist die Aufteilung des Profils in ein Hauptprofil und mehrere Unterprofile. Jedes Unterprofil ist auf einen Aspekt der Referenzarchitektur fo-

kussiert und bietet verschiedene Teilreferenzarchitekturen für Variationen an, sodass die zutreffenden Teilarchitekturen ausgewählt und zu einer Gesamt-Referenzarchitektur zusammengesetzt werden können.

Um das umzusetzen, sollte der Profilersteller zunächst eine generische Referenzarchitektur erstellen. Dazu muss er alle denkbaren Zielobjekte auflisten, die in einer Referenzarchitektur eines Profilanwenders maximal enthalten sein könnten – damit erhält er in **Schritt 3a** die **generische Zielobjektliste**. Außerdem sollte ein **generischer Netzplan** erstellt werden, in dem möglichst viele der generischen Zielobjekte enthalten sind (**Schritt 3b**).

Der Netzplan stellt die Konfiguration und Verbindungen der Zielobjekte dar. Da sich Variationsmöglichkeiten in Konfiguration und Verbindungen oft gegenseitig ausschließen, müssen bei der Erstellung des generischen Netzplans mit hoher Wahrscheinlichkeit einzelne Variationen ausgewählt werden. Auf welche Variationen die Wahl konkret fällt, ist an dieser Stelle von untergeordneter Bedeutung; sie sollten jedoch mitsamt ihrer nicht gewählten Alternativen klar benannt werden. Der Zweck des generischen Netzplans liegt darin, dem Profilanwender einen beispielhaften Netzplan des *gesamten* Netzes an die Hand zu geben. Im Gegensatz dazu werden die im weiteren Verlauf erarbeiteten spezifischen Netzpläne nur Teilaspekte des Gesamtnetzplans beinhalten.

Nun müssen in **Schritt 3c** Variationsmöglichkeiten der Referenzarchitektur identifiziert und in Gruppen eingeteilt werden. An dieser Stelle wird deutlich, warum eine sorgfältige Auswahl eines homogenen Geltungsbereichs und eng abgegrenzten Informationsverbunds fundamental ist: Die Zahl der Variationsmöglichkeiten würde anderenfalls schnell unbeherrschbar.

Gemäß der Zielsetzung, dass der Profilanwender möglichst wenig Vorkenntnisse benötigen sollte (und entsprechend der Erfahrung, dass Netzpläne in Institutionen häufig nicht vorhanden sind), sollten die Variationsmöglichkeiten so beschrieben werden, dass der Profilanwender leicht beantworten kann, welche Variante für seine Institution zutrifft. Sinnvoll sind Formulierungen wie „Das System kann / hat…“. Dies resultiert in der Benennung von **Anwendungsfällen**, die – je nachdem, welcher Aspekt in den Anwendungsfallen variiert wird – zu **Anwendungsfallgruppen (= Unterprofilen)** zusammengefasst werden. Sinnvolle Beispiele finden sich im Pilotprofil, das im Verlauf dieser Arbeit erstellt wurde.

Im letzten **Schritt 3d** muss der Profilersteller nun für jeden der Anwendungsfälle prüfen, welche Zielobjekte der generischen Liste für eine Anwendungsfallgruppe relevant sind (**spezifische Zielobjektlisten**) und für jeden Anwendungsfall einen Netzplan erstellen (**spezische Netzpläne**). Das Resultat sind spezifische Referenzarchitekturen, die die Referenzarchitektur des Profils für eine große Zahl von Profilanwendern möglichst passgenau machen sollten. Vonseiten des IT-Grundschutzes kann nun mit der Schutzbedarfsfeststellung der einzelnen Zielobjekte (für jeden Anwendungsfall!) und der Modellierung und Maßnahmenauswahl fortgefahren werden.

Bei der Bausteinmodellierung eines in Unterprofile gesplitteten Profils können Bausteine in mehreren Unterprofilen eingesetzt, aber jeweils nur ein Teil der Maßnahmen ausgewählt werden. Dabei gilt die Faustregel: Ein Zielobjekt sollte in einem Unterprofil nur dann mit seinem

speziellen Baustein (also beispielsweise der Baustein „SPS“ für eine SPS) modelliert werden, wenn im Unterprofil spezifische Maßnahmen für dieses Zielobjekt ergriffen werden sollen. Eine Orientierungshilfe für die Zuordnung von Maßnahmen zu den einzelnen Unterprofilen gibt Abschnitt 6.2 dieser Arbeit.

8 Fazit und Ausblick

Das Ziel dieser Arbeit war die Erstellung eines gut durchdachten IT-Grundschutz-Pilotprofils, das möglichst wenig Fachkenntnis, wenig Aufwand und wenig bereits vorhandene Dokumentation aufseiten der Profilanwender erfordert. Dies sind die drei Ziele, die hinter allen konzeptionellen Entscheidungen während der Profilentwicklung standen.

Ihre Erfüllung spiegelt sich in den folgenden Profilaspekten wider:

1. Möglichst wenig Security-Fachkenntnis nötig:
    - Die meiste Fachkenntnis bei der Erstellung einer Informationssicherheitskonzeption erfordern die Risikoanalyse und die Maßnahmenauswahl.
    - Das Profil basiert auf dem IT-Grundschutz. Das Grundkonzept des IT-Grundschutzes nimmt dem Anwender sowohl Risikoanalyse als auch Maßnahmenauswahl ab: Im Vorhinein wird ein Schutzniveau festgelegt und dafür fertige Maßnahmenpakete empfohlen.
    - IT-Grundschutz-Anwender müssen nur dann eine ergänzende Risikoanalyse durchführen, wenn eine unübliche IT-Infrastruktur oder ein besonders hoher Schutzbedarf vorliegen. Dafür bietet der BSI-Standard 200-3 eine umfangreiche Anleitung.
    - Profilanwendern soll die ergänzende Risikoanalyse weiter erleichtert werden, indem das Profil branchenspezifische Hilfestellungen zur Risikoanalyse gibt: Eine angepasste Risikomatrix sowie Listen berücksichtigter und nicht berücksichtigter Gefährdungen.
2. Möglichst wenig Zeitaufwand nötig:
    - Der Zeitaufwand für den Anwender ist genau dann gering, wenn das Profil auf seine IT-Infrastruktur gut passt (dann sind wenig Anpassungen und keine Risikoanalyse notwendig).
    - Erste Voraussetzung für eine gute Passgenauigkeit ist die Auswahl eines homogenen Geltungsbereichs. Im Pilotprofil wurde dies mit der Beschränkung auf die Leitsysteme bei Betreibern der Wasserwirtschaft erreicht.
    - Weil auch bei einer homogenen Branche zu viele Variationsmöglichkeiten bestehen, als dass eine einheitliche Referenzarchitektur möglich wäre, wurde das Profil in mehrere Unterprofile unterteil. In den Unterprofilen behandeln differenzierte Anwendungsfälle Variationen eines bestimmten Aspektes der ICS-Netze. Auf diese Weise sollten möglichst viele Anwender ihre IT-Infrastruktur mit dem Profil abbilden können.
3. Möglichst wenig vorhandene Dokumentation nötig:
    - Das IT-Grundschutz-Konzept, bei dem die IT-Infrastruktur des Anwenders mit Bausteinen modelliert wird, erfordert gute Dokumentation der IT-Infrastruktur in Form von Asset Lists (Zielobjektlisten) und Netzplänen. Gerade kleinere Betriebe haben solch eine Dokumentation meist nicht.

- Das Profil setzt deswegen die Dokumentation nicht voraus, sondern schafft sie: Durch die Auswahl der grundlegenden Netzstruktur und danach der zutreffenden Anwendungsfälle erstellen die Profilanwender sich während der Anwendung ohne Zusatzaufwand eine Zielobjektliste und einen Netzplan ihrer IT-Infrastruktur.
- Die Zielobjektliste ist gleichzeitig das wichtigste Ergebnis der Profilanwendung, da sie alle wichtigen Informationen zur IT-Infrastruktur und dem Informationssicherheitskonzept des Anwenderbetriebes übersichtlich zusammenfasst.

Das im Rahmen dieser Arbeit erstellte Pilotprofil kann in seinem jetzigen Zustand bereits als Leitfaden für die Erstellung weiterer Profile verwendet werden. Dazu wurden Vorgehensweisen und Fließbilder sowohl für die Anwendung des Profils als auch für die Erstellung weiterer Profile nach seinem Vorbild entwickelt.

Eine Einschränkung besteht jedoch: Da bis zum Abschluss dieser Arbeit die modernisierten IT-Grundschutz-Bausteine noch nicht vorlagen, verwendet das Profil die bisherigen Bausteine. Sobald die neuen Bausteine verfügbar sind, sollten die alten Bausteine ersetzt werden. Dazu wird das BSI Migrationstabellen zur Verfügung stellen, die die Umstellung erleichtern.

Das Profil für die Wasserwirtschaft, das als zweites Ergebnis entstanden ist, konnte aufgrund der zeitlichen Beschränkung dieser Arbeit nicht vollendet werden. Das Hauptprofil sowie das Unterprofil AR (Architektur), das beispielhaft für das Pilotprofil erstellt wurde, sind jedoch vollständig. Zur Vervollständigung des „Wasser“-Profils sollten die übrigen Unterprofile analog zum Unterprofil AR erstellt werden. Dazu müssen folgende Tabellen für die verbleibenden Anwendungsfallgruppen NM (Netzmanagement), UA (Benutzerzugang), PA (Programmzugriff) und PLC (SPS-Programmierung und -Wartung) mit Informationen aus dem branchenspezifischen Sicherheitsstandard Wasser / Abwasser (B3S WA) ergänzt werden:

- Modellierungstabellen
- Maßnahmenauswahltabellen (und deren Begründung)
- Gefährdungstabellen (und Liste nicht berücksichtigter Gefährdungen)

Die Zielobjektlisten und Netzpläne für die einzelnen Anwendungsfälle sind in dieser Arbeit bereits erstellt worden.

Das Hauptergebnis dieser Arbeit – das Konzept für ein IT-Grundschutz-Profil – wurde unter größtmöglichem Einbezug der Praxis erarbeitet. Trotzdem sollte es als Vorschlag verstanden werden, der sich in der praktischen Anwendung bewähren muss. Ein Konzept, das vor allem eine Arbeitserleichterung für Anwender bezweckt, lebt von der Rückmeldung seiner tatsächlichen Anwender und sollte niemals unverrückbar feststehen. Der nächste sinnvolle Schritt für das in dieser Arbeit entwickelte Pilotprofil ist deswegen, es von Anwendern auf Herz und Nieren in der Praxis testen zu lassen und ohne Zögern Änderungen vorzunehmen, wo sie sinnvoll sind.

Die übergeordnete Thematik der vorliegenden Arbeit ist die ICS-Security. Das Thema besetzt im Vergleich zu der „gewöhnlichen“ IT-Security bislang eine Nische. Vor allen produzierende Unternehmen und Betreiber kritischer Infrastrukturen müssen sich damit befassen – Otto Normalverbraucher bekäme zwar die Auswirkungen eines *Security Incidents* potenziell zu spüren, hat aber keinen direkten Einfluss auf die ICS-Netze und deren Sicherheit.

Dies kann sich grundlegend ändern, wenn das Internet of Things von der Zukunftsmusik zum Alltag wird. Internet of Things bedeutet, dass wir in allen Lebensbereichen wie selbstverständlich von kleinen Sensoren, Aktoren und Reglern – also ICS – umgeben sein werden. Als Konsequenz kann es auch auf alle Lebensbereiche physische Auswirkungen haben, wenn diese Mini-ICS nicht funktionieren, wie sie sollen.

ICS-Security würde damit nicht mehr nur relevant für industrielle ICS-Betreiber, sondern für private Heim-ICS-Betreiber. Das Eingangszitat zu dieser Arbeit hat das Postulat in den Raum gestellt, ICS würden nicht mehr hinreichend verstanden. Nun, wenn das für Unternehmen gilt, dann für Heimanwender umso mehr. Gut, wenn es bis dahin Möglichkeiten gibt, ICS sicher zu betreiben, ohne IT-Experte sein zu müssen. Ein bescheidener Anfang ist mit dieser Arbeit gemacht.

„Could it be that our home networks are in fact the ICS of the future?“

Tyson Macaulay und Bryan Singer in ihrem Buch
Cybersecurity for Industrial Control Systems [MS12]

9 Literaturverzeichnis

[ABB13] ABB: *System 800xA Network Configuration : System Version 5.1.* 2013.
URL library.e.abb.com/public/9c8b6c0dc8bdfe16c1257b400026feb3/3BSE034463-510_E_en_System_800xA_5.1_Network_Configuration.pdf
Überprüfungsdatum 2017-01-27

[AbwV97] *Verordnung über Anforderungen an das Einleiten von Abwasser in Gewässer (Abwasserverordnung - AbwV)* (1997-03-21).
URL www.gesetze-im-internet.de/bundesrecht/abwv/gesamt.pdf
Überprüfungsdatum 2017-02-22

[Aut12] Automation.at: *Frühjahrs-Diät für die Automatisierungspyramide.*
URL www.automation.at/detail/fruehjahrs-diaet-fuer-die-automatisierungspyramide_74018
Überprüfungsdatum 2017-05-10

[AWRL91] *Richtlinie 91/271/EWG über die Behandlung von kommunalem Abwasser.*
In: *Amtsblatt der Europäischen Gemeinschaften* (1991-05-21).
URL eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1991:135:0040:0052:DE:PDF
Überprüfungsdatum 2017-02-22

[AWWA14] American Water Works Association (AWWA):
Process Control System Security Guidance for the Water Sector. 2014 (1).
URL www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf
Überprüfungsdatum 2017-02-07

[AWWA17a] American Water Works Association (AWWA): *About us.*
URL www.awwa.org/about-us.aspx
Überprüfungsdatum 2017-03-20

[AWWA17b] American Water Works Association (AWWA): *Cybersecurity Guidance & Tool.*
URL www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx
Überprüfungsdatum 2017-03-30

[AWWA17c] American Water Works Association (AWWA):
Process Control System Security Guidance for the Water Sector. 2017.
URL www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx
Überprüfungsdatum 2017-03-17

[B3S17a] Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) ; Deutscher Verein des Gas- und Wasserfaches (DVGW):
Branchenspezifischer Sicherheitsstandard Wasser/Abwasser : IT-Sicherheitsleitfaden. 2017

[B3S17b] Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) ; Deutscher Verein des Gas- und Wasserfaches (DVGW): *Branchenspezifischer Sicherheitsstandard Wasser/Abwasser : Handbuch zum IT-Sicherheitsleitfaden.* 2017

[B3S17c] Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) ; Deutscher Verein des Gas- und Wasserfaches (DVGW): *M 1060 bzw. W 1060 (M) : IT-Sicherheit - Branchenstandard Wasser/Abwasser.* 2017

[Bau09] BAUMANN, Peter: *MSR-Technik in abwassertechnischen Anlagen : Mit 19 Tabellen.* Renningen : Expert-Verl., 2009 (Kontakt & Studium Bd. 664)

[BBK16] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): *Sicherheit in der Trinkwasserversorgung : Teil 1: Risikoanalyse.* 2016.
URL www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band-15_Praxis_BS_Trinkwasserversorgung.pdf?__blob=publicationFile
Überprüfungsdatum 2017-03-23

[BMI09] Bundesministerium des Innern (BMI): *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).* 2009.
URL www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf;jsessionid=32AA6FEA813259E0BA0A82AACEB7325A.2_cid287?__blob=publicationFile
Überprüfungsdatum 2017-01-31

[BNetzA17a] Bundesnetzagentur (BNetzA): *Allgemeinzuteilungen.*
URL www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Allgemeinzuteilungen/allgemeinzuteilungen-node.html
Überprüfungsdatum 2017-03-21

[BNetzA17b] Bundesnetzagentur (BNetzA): *Bündelfunk.*
URL www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Firmennetze/Buendelfunk/buendelfunk-node.html
Überprüfungsdatum 2017-03-21

[BNetzA17c] Bundesnetzagentur (BNetzA): *Betriebsfunk.*
URL www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Firmennetze/Betriebsfunk/betriebsfunk-node.html
Überprüfungsdatum 2017-03-21

[Bor16] BORCHERS, Detlef: *IT-Sicherheitsgesetz: Wer was wann zu melden hat.*
URL www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html.
– Aktualisierungsdatum: 2016-02-08 Überprüfungsdatum 2017-02-18

[BSI08a] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 100-1 : Managementsysteme für Informationssicherheit ISMS.* 2., überarb. Aufl. Köln : Bundesanzeiger-Verl., 2008 (Unternehmen und Wirtschaft)

[BSI08b] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 100-3 : Risikoanalyse auf der Basis von IT-Grundschutz.* 2., überarb. Aufl. Köln : Bundesanzeiger-Verl., 2008 (Unternehmen und Wirtschaft)

[BSI08c] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 100-2 : IT-Grundschutz-Vorgehensweise.* 2., überarb. Aufl. Köln : Bundesanzeiger-Verl., 2008 (Unternehmen und Wirtschaft)

[BSI09] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 100-4 : Notfallmanagement.* [Version 1.0, Stand: November 2008]. Köln : Bundesanzeiger, 2009 (Unternehmen und Wirtschaft)

[BSI13] Bundesamt für Sicherheit in der Informationstechnik (BSI): *ICS-Security-Kompendium.* 2013. URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=2 Überprüfungsdatum 2016-12-22

[BSI14a] Bundesamt für Sicherheit in der Informationstechnik (BSI): *ICS-Security-Kompendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten.* 2014. URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf?__blob=publicationFile&v=1 Überprüfungsdatum 2016-12-22

[BSI14b] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Light and Right Security ICS: Benutzerhandbuch : Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security.* 2014. URL www.allianz-fuer-cybersicherheit.de/ACS/DE/_/zusatzinfos_angebote/141124_Handbuch_LARS.pdf?__blob=publicationFile&v=1 Überprüfungsdatum 2016-12-22

[BSI15] Bundesamt für Sicherheit in der Informationstechnik (BSI): *KRITIS Sektorstudie : Ernährung und Wasser.* 2015. URL www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_Ern%C3%A4hrung_Wasser.pdf?__blob=publicationFile Überprüfungsdatum 2017-02-07

[BSI16a] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Kataloge: Standardwerk zur IT-Sicherheit : 15. Ergänzungslieferung 2016.* Bonn : Bundesanzeiger Verlag, 2016

[BSI16b] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IND.1: Betriebs- und Steuerungstechnik (Entwurf) : IT-Grundschutz-Baustein.* Bonn, 2016.
URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_ICS_Betrieb.pdf?__blob=publicationFile&v=6
Überprüfungsdatum 2016-12-22

[BSI16c] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Kreuzreferenztabellen der IT-Grundschutz-Kataloge : Stand: 15. Ergänzungslieferung.* 2016.
URL www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Download/download_node.html
Überprüfungsdatum 2017-04-26

[BSI16d] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Profil eCommerce (Entwurf).* 2016

[BSI16e] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 200-3 (Community Draft) : Risikoanalyse auf der Basis von IT-Grundschutz.* 2016. URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BSI_Standard_200-3.pdf?__blob=publicationFile&v=3
Überprüfungsdatum 2016-12-22

[BSI16f] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Das BSI: Historie.*
URL www.bsi.bund.de/DE/DasBSI/Historie/historie_node.html
Überprüfungsdatum 2017-01-25

[BSI16g] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Das IT-Sicherheitsgesetz : Kritische Infrastrukturen schützen.* 2016.
URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=5
Überprüfungsdatum 2017-02-02

[BSI16h] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Die Modernisierung des IT-Grundschutz : Informationssicherheit im Cyber-Raum – aktuell, flexibel, praxisnah.* 2016.
URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Flyer_Modernisierung_des_IT-Grundschutzes.pdf?__blob=publicationFile&v=3
Überprüfungsdatum 2017-01-10

[BSI17a] SCHILDT, Holger ; Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Profile: Strukturbeschreibung (Working Draft).* 2017

[BSI17b] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 200-2 (Community Draft) : IT-Grundschutz-Methodik.* 2017

[BSI17c] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Struktur der Modernisierung.* URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Struktur_Modernisierung.pdf?__blob=publicationFile&v=6 Überprüfungsdatum 2017-02-26

[BSIG16] *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* (2016) URL www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html Überprüfungsdatum 2017-06-12

[Con15] Control Real: *DCS or PLC or PAC or RTU?* URL controlreal.com/en/dcs-or-plc-or-pac-or-rtu/ Überprüfungsdatum 2017-05-12

[Destatis11] Statistisches Bundesamt (Destatis): *Produzierendes Gewerbe : Beschäftigung, Umsatz, Investitionen und Kostenstruktur der Unternehmen in der Energieversorgung, Wasserversorgung, Abwasser- und Abfallentsorgung, Beseitigung von Umweltverschmutzungen.* Wiesbaden, 2011 (Fachserie 4 Reihe 6.1 - 2009). URL www.destatis.de/DE/Publikationen/Thematisch/Energie/Struktur/BeschaeftigungUmsatzKostenstruktur2040610097004.pdf?__blob=publicationFile Überprüfungsdatum 2017-02-18

[Destatis15a] Statistisches Bundesamt (Destatis): *Unternehmen, Tätige Personen, Umsatz, Investitionen, Bruttowertschöpfung nach Unternehmensgröße : Deutschland.* URL www-genesis.destatis.de/genesis/online/link/tabelleErgebnis/48121-0001 Überprüfungsdatum 2017-05-04

[Destatis15b] Statistisches Bundesamt (Destatis): *Strukturdaten zur Wasserwirtschaft.* Fachserie 19 Reihe 2.1.3. Wiesbaden, 2015. – Fachserie 19 Reihe 2.1.3. URL www.destatis.de/DE/Publikationen/Thematisch/UmweltstatistischeErhebungen/Wasserwirtschaft/Wasserwirtschaft2190213139004.pdf?__blob=publicationFile Überprüfungsdatum 2017-02-02

[Destatis17a] Statistisches Bundesamt (Destatis): *Beschäftigung und Einstellung von IT-Fachkräften nach Beschäftigtengrößenklassen im Jahr 2016 : Deutschland.* URL www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/IKTUnternehmen/Tabellen/05_IT_Fachkraefte_IKT_Unternehmen.html Überprüfungsdatum 2017-05-04

[Destatis17b] Statistisches Bundesamt (Destatis): *Beschäftigte, Umsatz, Produktionswert und Wertschöpfung der Unternehmen in der Energie- und Wasserversorgung: Deutschland, Jahre, Wirtschaftszweige.*
URL www-genesis.destatis.de/genesis/online;jsessionid=5C28D8AA890877F7D097C979D37665E8.tomcat_GO_2_2?operation=previous&levelindex=2&levelid=1496575008821&step=2
Überprüfungsdatum 2017-06-04

[DHS16] Department of Homeland Security (DHS): *About DHS.*
URL www.dhs.gov/about-dhs
Überprüfungsdatum 2017-03-30

[DIN16323] DIN EN 16232:2014-07 *Wörterbuch für Begriffe der Abwassertechnik; Dreisprachige Fassung EN 16232:2014*

[DIN4045] DIN 4045:2003-08 *Abwassertechnik - Grundbegriffe*

[DIN4046] DIN 4046:1983-09 *Wasserversorgung: Begriffe*

[DWA07] Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA): *Informations- und Kommunikationsnetzwerke für die Abwassertechnik.* Hennef (Sieg) : DWA, 2007 (DWA-Regelwerk M 207)

[DWA11] Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA): *Leit- und Automatisierungstechnik auf Abwasseranlagen.* Hennef (Sieg) : DWA, 2011 (DWA-Regelwerk M 253)

[DWA15] Arbeitsgemeinschaft Trinkwassertalsperren (ATT) ; Bundesverband der Energie- und Wasserwirtschaft (BDEW) ; Landesverband der Wasser- und Bodenverbände (DBVW) ; Deutscher Verein des Gas- und Wasserfaches (DVGW) ; Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) ; Verband kommunaler Unternehmen (VKU):
Branchenbild der deutschen Wasserwirtschaft 2015. Bonn : Wirtschafts- und Verlagsgesellschaft Gas und Wasser, 2015

[EM07] ENSTE, Udo ; MÜLLER, Jochen: *Datenkommunikation in der Prozessindustrie : Darstellung und anwendungsorientierte Analyse.* München : Oldenbourg Industrieverlag, 2007

[ENISA14] European Agency for Network and Information Security (ENISA): *Smart grid security certification in Europe : Challenges and recommendations.* 2014.
URL www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe
Überprüfungsdatum 2017-06-10

[EU17] Europäische Kommission: *What is an SME?*
URL ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_de
Überprüfungsdatum 2017-04-19

[FA09] FRÜH, Karl Friedrich (Hrsg.); AHRENS, Wolfgang (Hrsg.): *Handbuch der Prozessautomatisierung : Prozessleittechnik für verfahrenstechnische Anlagen.* 4., überarb. Aufl. München : Oldenbourg, 2009

[Fle17] Technisches Betriebszentrum Flensburg: *Organigramm.* URL www.tbz-flensburg.de/Informationen/%C3%9Cber-uns/Organigramm Überprüfungsdatum 2017-02-21

[Fra10] FRANKENSTEIN, Ronny: *ISO 27001 mit oder ohne IT-Grundschutz?* 2010. URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/2GS_Tag_2010/Ronny_Frankenstein_Hi_Solution.pdf?__blob=publicationFile Überprüfungsdatum 2017-06-10

[Her16] Stadtwerke Bad Herrenalb: *Organigramm.* URL www.stw-badherrenalb.de/cms/Organigramm%20Stadtwerke%20_23112016.pdf Überprüfungsdatum 2017-02-21

[ICS-CERT17a] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): *The Industrial Control Systems Cyber Emergency Response Team.* URL ics-cert.us-cert.gov/ Überprüfungsdatum 2017-03-30

[ICS-CERT17b] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): *Recommended Practices.* URL ics-cert.us-cert.gov/Recommended-Practices Überprüfungsdatum 2017-03-30

[IEC15] International Electrotechnical Commission (IEC): *Functional Safety : Essential to overall safety.* Geneva, Switzerland, 2015. URL www.iec.ch/about/brochures/pdf/technology/functional_safety.pdf Überprüfungsdatum 2017-04-19

[IEC17] International Electrotechnical Commission (IEC): *About the IEC.* URL www.iec.ch/about/?ref=menu Überprüfungsdatum 2017-03-30

[IEC61508] IEC 61508:2010-04 *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*

[IEC61511] IEC 61511:2016-07 *Functional safety - Safety instrumented systems for the process industry sector*

[IfM16] Institut für Mittelstandforschung Bonn (IfM Bonn): *KMU-Definition des IfM Bonn.* URL www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ Überprüfungsdatum 2017-02-01

[ISA10] International Society of Automation (ISA): *The 62443 series of standards : Industrial Automation and Control Systems Security.* 2010.
URL isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf
Überprüfungsdatum 2017-06-10

[ISA17] International Society of Automation (ISA): *About ISA.*
URL www.isa.org/about-isa/
Überprüfungsdatum 2017-03-30

[ISO17] International Organization for Standardization (ISO): *About us.*
URL www.iso.org/about-us.html
Überprüfungsdatum 2017-03-30

[ISO27001] DIN/ISO/IEC 27001:2015-03 *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Management- systeme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

[IT-SiG15] *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme.* In: *Bundesgesetzblatt* 2015 Teil I (2015-07-17), Nr. 31, S. 1324–1331.
URL www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf –
Überprüfungsdatum 2017-02-02

[Kar14] Stadtwerke Karlstadt: *Organigramm.*
URL www.stadtwerke-karlstadt.de/Eigene_Dateien/stadtwerke/organigramm_stadtwerke_karlstadt_13.11.2014.pdf
Überprüfungsdatum 2017-02-21

[KL15] KNAPP, Eric D. ; LANGILL, Joel Thomas: *Industrial network security : Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems.* 2. ed. Amsterdam : Syngress Elsevier, 2015

[Kre15] KREMPL, Stefan: *IT-Sicherheit für den Mittelstand: Besser nach ISO/IEC 27001 oder IT-Grundschutz zertifizieren?* 2015.
URL www.sued-it.de/unternehmen/news-presse/52-it-sicherheit-fuer-den-mittelstand-besser-nach-iso-iec-27001-oder-it-grundschutz-zertifizieren
Überprüfungsdatum 2017-06-10

[KritisV16] *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz.* In: *Bundesgesetzblatt* 2016 Teil I (2016-04-22), Nr. 20, S. 958–969.
URL www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s0958.pdf
Überprüfungsdatum 2017-02-02

[KWS] KW Software GmbH:
Einführung in die IEC 1131-Programmierung mit MULTIPROGwt. Hannover.
URL www.u-ohm.de/Multiprog_3.pdf
Überprüfungsdatum 2017-03-10

[Lan12] LANGNER, Ralph: *Robust control system networks :*
How to achieve reliable control after Stuxnet.
New York : Momentum Press, 2012

[Mat09] Matrikon Inc.: *OPC: The Ins and Outs to What It's About :*
The Every Man's Guide to OPC. 2009.
URL www.automation.com/pdf_articles/Guide_to_OPC.pdf
Überprüfungsdatum 2017-03-08

[MBS11] MERSCH, Henning ; BEHNEN, Daniel ; SCHMITZ, Dominik ; EPPLE, Ulrich ; BRECHER, Christian ; JARKE, Matthias: *Gemeinsamkeiten und Unterschiede der Prozess- und Fertigungstechnik : Interdisziplinäre Aspekte der Produktionsmodellierung.* In: *at - Automatisierungstechnik* 59 (2011), Nr. 1

[MS05] MAURO, Douglas ; SCHMIDT, Kevin: *Essential SNMP.*
2nd ed. Sebastopol : O'Reilly Media, Inc, 2005

[MS11] MUTSCHMANN, Johann ; STIMMELMAYR, Fritz; FRITSCH, Peter (Mitarb.); KNAUS, Werner (Mitarb.); MERKL, Gerhard (Mitarb.); PREININGER, Erwin (Mitarb.); RAUTENBERG, Joachim (Mitarb.); WRICKE, Burkhard (Mitarb.); WEIß, Matthias (Mitarb.) : *Taschenbuch der Wasserversorgung.* 15., vollst. überarb. u. akt. Aufl.
Wiesbaden : Vieweg + Teubner, 2011 (Praxis)

[MS12] MACAULAY, Tyson ; SINGER, Bryan: *Cybersecurity for Industrial Control Systems : SCADA, DCS, PLC, HMI, and SIS.* Boca Raton, Fla. : CRC Press, 2012

[MS16] MÜNCH, Isabel ; SCHILDT, Holger: *Profile im modernisierten IT-Grundschutz : Schablonen für die Informationssicherheit.* In: *kes* 24 (2016), Nr. 4, S. 36–40.
URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/KES_2016_4_Profile.pdf?__blob=publicationFile&v=2
Überprüfungsdatum 2016-12-22

[MSW16] MÜNCH, Isabel ; SCHILDT, Holger ; WIEMERS, Christoph: *Die Modernisierung des IT-Grundschutzes (*IT-Grundschutz-Tag). Nürnberg, 19.10.2016.
URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/3GS_Tag_2016/BSI_GS.pdf?__blob=publicationFile&v=1
Überprüfungsdatum 2017-02-08

[Mün16] MÜNCH, Isabel: *Informationssicherheit im Unternehmen : IT-Grundschutz adressiert mit neuen Angeboten verstärkt KMU.* In: *comply* (2016), Nr. 3, S. 28–31. URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Comply_2016_Informationssicherheit_in_Unternehmen.pdf Überprüfungsdatum 2016-12-22

[NERC16] North American Electric Reliability Corporation (NERC): *About NERC.* URL www.nerc.com/AboutNERC/Pages/default.aspx Überprüfungsdatum 2017-03-30

[NIST13] National Institute of Standards and Technology (NIST): *Special Publication 800-53 (Revision 4) : Security and Privacy Controls for Federal Information Systems and Organizations.* 2013

[NIST14] National Institute of Standards and Technology (NIST): *Framework for Improving Critical Infrastructure Cybersecurity.* 2014. URL www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf Überprüfungsdatum 2017-03-30

[NIST15a] National Institute of Standards and Technology (NIST): *Special Publication 800-82 (Revision 2) : Guide to Industrial Control Systems (ICS) Security.* Revision 2 : National Institute of Standards and Technology, 2015

[NIST15b] National Institute of Standards and Technology (NIST): *NIST Releases Update of Industrial Control Systems Security Guide.* 2015. URL www.nist.gov/news-events/news/2015/06/nist-releases-update-industrial-control-systems-security-guide Überprüfungsdatum 2017-06-10

[NIST16] National Institute of Standards and Technology (NIST): *About NIST.* URL www.nist.gov/about-nist Überprüfungsdatum 2017-03-30

[Nor16] Stadtentwässerungsbetrieb Nordhausen: *Organigramm.* URL abwasser-nordhausen.de/unternehmerisches-organigramm.html Überprüfungsdatum 2017-02-21

[Pep17] Pepperl+Fuchs GmbH: *Remote-I/O-Systeme.* URL www.pepperl-fuchs.de/germany/de/classid_259.htm Überprüfungsdatum 2017-05-12

[Sch13] Stadtentwässerung Schweinfurt: *Organigramm.*
URL www.schweinfurt.de/rathaus-politik/stadtentwaesserung/ueber-uns1/m_17325
Überprüfungsdatum 2017-02-21

[Sie06] Siemens AG: *Communication with SIMATIC : System Manual.* 2006.
URL cache.industry.siemens.com/dl/files/686/1254686/att_46478/v1/S7komm_e.pdf
Überprüfungsdatum 2017-01-02

[Sie10] Siemens AG: *Integrated automation for discrete manufacturing.* 2010.
URL www.click4business-supplies.com/resources/articles/e20001-a830-p200-x-7600.pdf
Überprüfungsdatum 2017-02-01

[Sie16] SIEBER, Peter:
IT-Security als Säule für Funktionale Sicherheit in Prozessanlagen : Whitepaper. 2016.
URL www.process.vogel.de/index.cfm?pid=2791&pk=36050&cmp=nl-207&uuid=54283B8B-E960-6509-59CB6A1931D5BA24
Überprüfungsdatum 2017-01-02

[StEB14] Stadtentwässerungsbetriebe Köln (StEB Köln): *Organigramm.*
URL www.steb-koeln.de/Redaktionell/Downloads/Unternehmen/Organigramm-der-StEB-04_2014.pdf
Überprüfungsdatum 2017-02-21

[Stei17] Stadt Steinheim: *Organigramm.*
URL www.steinheim.de/Stadt-Rathaus/Rathaus/Organisation
Überprüfungsdatum 2017-02-21

[Ter16] TERHART, Ludger: *Der modernisierte IT-Grundschutz: Chancen für den Branchenstandard (*1. IT-Grundschutztag). 2016.
URL www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_2016/04_Dr_Terhart_Chancen_fuer_den_Branchenstandard.pdf?__blob=publicationFile&v=1
Überprüfungsdatum 2017-02-07

[TrinkwV01] *Verordnung über die Qualität von Wasser für den menschlichen Gebrauch (Trinkwasserverordnung - TrinkwV 2001)* (2001-05-21).
URL www.gesetze-im-internet.de/bundesrecht/trinkwv_2001/gesamt.pdf
Überprüfungsdatum 2017-02-22

[TWRL98] *Richtlinie 98/83/EG über die Qualität von Wasser für den menschlichen Gebrauch.* In: *Amtsblatt der Europäischen Gemeinschaften* (1998-11-03).
URL eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:330:0032:0054:DE:PDF
Überprüfungsdatum 2017-02-22

[VDE17] Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE): *VDE: Netzwerk Zukunft.*
URL www.vde.com/de/ueber-uns
Überprüfungsdatum 2017-03-30

[VDI17] Verein Deutscher Ingenieure (VDI): *Das Leitbild des VDI.*
URL www.vdi.de/nc/ueber-uns/unser-leitbild/
Überprüfungsdatum 2017-03-30

[VDI2182-1] VDI/VDE 2182:2011-01 *Blatt 1: Informationssicherheit in der industriellen Automatisierung: Allgemeines Vorgehensmodell*

[VDI2182-2.1] VDI/VDE 2182:2013-02 *Blatt 2.1: Informationssicherheit in der industriellen Automatisierung: Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller (Speicherprogrammierbare Steuerung (SPS))*

[VDI2182-3.1] VDI/VDE 2182:2013-09 *Blatt 3.1: Informationssicherheit in der industriellen Automatisierung: Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller (Prozessleitsystem einer LDPE-Anlage)*

[VDI2182-3.2] VDI/VDE 2182:2013-05 *Blatt 3.2: Informationssicherheit in der industriellen Automatisierung: Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren (LDPE-Reaktor)*

[Verdi15] Vereinte Dienstleistungsgewerkschaft (ver.di): *ver.di-Branchenanalyse Wasserwirtschaft 2015.* 2015.
URL ver-und-entsorgung.verdi.de/branchen/wasserwirtschaft_1/++co++598a98d8-2976-11e6-831e-52540077a3af
Überprüfungsdatum 2017-02-21

[WHG09] *Gesetz zur Ordnung des Wasserhaushalts (Wasserhaushaltsgesetz - WHG)* (2009-07-31).
URL www.gesetze-im-internet.de/bundesrecht/whg_2009/gesamt.pdf
Überprüfungsdatum 2017-02-22

[Wil94] WILLIAMS, Theodore J.: *The Purdue enterprise reference architecture.* In: *Computers in Industry* 24 (1994), 2-3, S. 141–158

[WRRL00] *Richtlinie 2000/60/EG zur Schaffung eines Ordnungsrahmens für Maßnahmen der Gemeinschaft im Bereich der Wasserpolitik.* In: *Amtsblatt der Europäischen Gemeinschaften* (2000-10-23).
URL eur-lex.europa.eu/resource.html?uri=cellar:5c835afb-2ec6-4577-bdf8-756d3d694eeb.0003.02/DOC_1&format=PDF
Überprüfungsdatum 2017-02-22

[WT16] WAGNER, Kirsten ; TERHART, Ludger: *IT-Sicherheit in der Wasserversorgung : Branchenstandard IT-Sicherheit Wasser/Abwasser.* In: *Energie- / Wasser-Praxis* (2016), Nr. 12, S. 134–136

[WZ11] WELLENREUTHER, Günter ; ZASTROW, Dieter: *Automatisieren mit SPS - Theorie und Praxis : Programmierung: DIN EN 61131-3, STEP 7, CoDeSys, Entwurfsverfahren, Bausteinbibliotheken ; Applikationen: Steuerungen, Regelungen, Antriebe, Safety ; Kommunikation: AS-i-Bus, PROFIBUS, Ethernet-TCP/IP, PROFINET, Web-Technologien, OPC, WLAN ; mit 108 Steuerungsbeispielen und 8 Projektierungen.* 5., korrigierte und erw. Aufl. Wiesbaden : Vieweg + Teubner, 2011 (Studium)

[Zet14] ZETTER, Kim: *Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon.* 1. Aufl. New York : Crown, 2014

[ZVEI10] Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI): *Manufacturing Execution System (MES): Branchenspezifische Anforderungen und herstellerneutrale Beschreibung von Lösungen.* 2010. URL www.zvei.org/Publikationen/MES-Doppelseiten.pdf Überprüfungsdatum 2017-01-02

10 Glossar und Abkürzungsverzeichnis

AV	Antivirensoftware
AWWA	American Water Works Association
B3S	Branchenspezifischer Sicherheitsstandard
B3S WA	Branchenspezifischer Sicherheitsstandard Wasser / Abwasser Vor dem Hintergrund des IT-Sicherheitsgesetzes von DWA und DVGW entworfener Informationssicherheitsstandard für die Wasserwirtschaft.
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz Deutsches Gesetz, das festlegt, welche Anlagenbetreiber innerhalb der KRITIS-Branchen unter das IT-Sicherheitsgesetz fallen.
CIA	Grundwerte der Informationssicherheit: Vertraulichkeit (Confidentiality, C), Integrität (Integrity, I) und Verfügbarkeit (Availability, A)
DCS	Distributed Control System
DHS	Department of Homeland Security US-amerikanisches Ministerium für Innere Sicherheit
DVGW	Deutscher Verein des Gas- und Wasserfachs
DWA	Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall
ERP	Enterprise Resource Planning Software, die Funktionen der Unternehmensleitebene der Automatisierungspyramide erfüllt. Dazu gehören beispielsweise Controlling und Optimierung der Wertschöpfungskette.
EWS	Engineering-Workstation Rechner für die Erstellung und Kompilation der Programme für die Steuergeräte (SPSen). Dedizierte Rechner für diesen Zweck werden auch als Programmiergerät (PG) bezeichnet. Die kompilierten Programme werden anschließend auf die SPSen überspielt.
FW	Firewall. Software (ggf. auf dediziertem Gerät), die anhand von Regeln den Datenverkehr im Netz filtert.
Geltungsbereich	Der Geltungsbereich eines IT-Grundschutz-Profils definiert die Zielgruppe, an die sich das Profil wendet, und ihre Rahmenbedingungen.

Historian	Datenbank für die Archivierung von Prozessdaten
HMI	Human-Machine-Interface Bedienschnittstelle einer automatisierten Anlage. Das HMI ermöglicht sowohl die Überwachung als auch den manuellen Eingriff in den automatisierten Prozess, etwa durch das Setzen von Sollwerten und das Bedienen von Aktoren.
HP	Hauptprofil
HW	Hardware
IACS	Industrial Automation and Control Systems, siehe ICS
ICS	Industrial Control System: Systeme zur Fertigungs- und Prozessautomatisierung im industriellen Umfeld. Unter den Begriff fallen in dieser Arbeit alle technischen Systeme, die für die automatisierte Steuerung eines Prozesses und die menschliche Überwachung dieser automatisierten Steuerung zuständig sind.
ICS-Security	IT-Sicherheit für ICS: Befasst sich mit auf ICS-Geräten elektronisch gespeicherten Informationen. Das Ziel der ICS-Sicherheit ist jedoch nicht nur der Schutz der Informationen, sondern insbesondere auch des Prozesses und der Anlagen, die diese Informationen steuern. Wird in dieser Arbeit mit dem englischen Begriff *Security* verwendet, um sie von der *Safety* abzugrenzen, die in ICS-Netzen ebenfalls eine hohe Rolle spielt (siehe Safety).
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission Internationale Normungsorganisation für Elektrotechnik und Elektronik
Informationssicherheit	Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein [BSI08a]
Informationsverbund	Der Informationsverbund definiert, welche Geschäftsprozesse im Rahmen eines IT-Grundschutz-Profils betrachtet werden und die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die für die Ausführung der Geschäftsprozesse nötig sind.
Institution	Oberbegriff für Unternehmen und Behörden
IP	Internet Protocol: Protokoll auf Schicht 3 des ISO/OSI-Referenzmodells, das für die Internet-Kommunikation verwendet wird.

IPS	Intrusion Prevention System
ISA	International Society of Automation Gemeinnützige Organisation, die Standards für die Automatisierungstechnik entwickelt.
ISO	International Organization for Standardization Internationale Normungsorganisation
IT	Information Technology bzw. Informationstechnik. Oberbegriff für Informations- und Datenverarbeitung durch technische Geräte, Dienste und Funktionen.
IT-Sicherheit	Schutz elektronisch gespeicherter Informationen und deren Verarbeitung [BSI08a]
IT-SiG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, kurz: IT-Sicherheitsgesetz [IT-SiG15] Seit Juli 2015 geltendes deutsches Gesetz, das KRITIS-Betreiber dazu verpflichtet, ihre kritischen Dienstleistungen nach dem Stand der Technik angemessen abzusichern und dies mindestens alle zwei Jahre überprüfen zu lassen. Auch die Meldung von IT-Sicherheitsvorfällen schreibt das Gesetz vor.
KMU	Kleine und mittlere Unternehmen: In dieser Arbeit werden KMU als Institution mit weniger als 500 Mitarbeitern definiert. Diese Definition orientiert sich an der des Instituts für Mittelstandsforschung Bonn (<500 Mitarbeiter, ≤ 50 Mio. € Jahresumsatz) und weicht von der EU-Definition (<250 Mitarbeiter, ≤ 50 Mio. € Jahresumsatz) ab.
Konzentrierte Anlage	Automatisierungstechnische Anlage mit konzentrierter ICS-Netzstruktur
Konzentrierte ICS-Netzstruktur	In dieser Arbeit bedeutet eine konzentrierte ICS-Netzstruktur, dass die ICS-Steuerungskomponenten lokal innerhalb eines Gebäudekomplexes liegen. Auch der lokale Leitstand der Anlage liegt innerhalb des Gebäudekomplexes und kommuniziert mit den Steuerungskomponenten mittels LAN-Technik.
KRITIS	Kritische Infrastruktur nach IT-Sicherheitsgesetz bzw. BSI-Kritis-Verordnung [IT-SiG15; KritisV16].
LAN	Local Area Network: Rechner- oder Kommunikationsnetz, das sich in etwa über einen Gebäudekomplex ausdehnt.

Leitstand	In dieser Arbeit bezeichnet der Leitstand die Räumlichkeit bzw. Funktionseinheit, in der mindestens Funktionen eines HMI, möglicherweise aber weitere zur Prozessleitebene der Automatisierungspyramide gehörigen Funktionalitäten verortet sind (Engineering-Workstation, Control Server, …)
MES	Manufacturing Execution System Software, die Funktionen der Betriebsleitebene der Automatisierungspyramide erfüllt. Dazu gehören beispielsweise Produktionsplanung, Ressourcenplanung und Wartung.
Modellierung	Im IT-Grundschutz die Zuordnung von mindestens einem IT-Grundschutz-Baustein zu jedem Zielobjekt. Da Bausteine Anforderungen enthalten, impliziert die Modellierung eine Auswahl von Anforderungen für die Zielobjekte eines Informationsverbunds.
NERC	North American Electrical Reliability Cooperation Gemeinnützige Organisation, die für die Zuverlässigkeit des Stromerzeugungs- und -übertragungssystems im nordamerikanischen Raum zuständig ist.
NIST	National Institute of Standards and Technology US-Bundesbehörde für Standardisierung, dem US-Handelsministerium unterstellt
Office-IT	Oberbegriffe für Hard- und Software, die üblicherweise im Büro-Umfeld verwendet wird – etwa PCs, Laptops, Server und Drucker.
OS	Betriebssystem (Operating System)
OT	Operational Technology: Oberbegriff für ICS und weitere Automationslösungen, die nicht im industriellen Umfeld verortet sind, z.B. Gebäudeleittechnik oder Internet-of-Things-Geräte. Er wird vor allem zur Abgrenzung von der IT (Information Technology) verwendet
PCS	Process Control System (deutsch: Prozessleitsystem, PLS)
PLC	Programmable Logic Controller (deutsch: Speicherprogrammierbare Steuerung, SPS) In dieser Arbeit als Oberbegriff für automatische Steuergeräte auf der Steuerungsebene der Automatisierungspyramide verwendet.
PLS	Prozessleitsystem (englisch: Process Control System, PCS)
Referenzarchitektur	Eine typische Architektur des Informationsverbunds einer Referenzinstitution. Eine Referenzarchitektur besteht aus Zielobjekten und einem oder mehreren Netzplänen.

Referenzinstitution	Eine typische Institution der Branche oder Anwendergruppe, an die ein IT-Grundschutz-Profil sich wendet.
Remote-I/O	Remote-Input/Output Gerät, dass die Ein- und Ausgaben von Feldgeräten verarbeitet und die Schnittstelle zu den Steuergeräten darstellt. Remote-I/Os können auch Ein- und Ausgaben für mehrere Sensoren und Aktoren zusammenfassen und wenn nötig vorverarbeiten. Außerdem werden sie für Feldgeräte verwendet, die weit entfernt von den Steuergeräten sind oder in besonders anspruchsvollen Umgebungen wie explosionsgefährdeten Bereichen arbeiten.
Safety	In der Automatisierungstechnik steht Safety meist für funktionaler Sicherheit und hat zum Ziel, dass Maschinen oder Geräte funktionieren, ohne für ihre Umwelt gefährliche Zustände einzunehmen. Um dies sicherzustellen, sind spezielle Steuereinheiten aktiv, die gefährliche Maschinenzustände verhindern sollen [IEC15].
SCADA	Supervisory Control and Data Acquisition
Security	siehe IT-Sicherheit
SIS	Safety Instrumented System Automatisierungssystem, das safety-relevante Funktionen steuert; beispielsweise die Abschaltung einer Anlage in Notfällen. Technisch gesehen ist ein SIS ein gewöhnliches Automatisierungssystem, bestehend aus Steuergeräten, Sensoren und Aktoren, jedoch ist es unabhängig vom restlichen System. Der Begriff SIS stammt aus [IEC61511].
SPS	Speicherprogrammierbare Steuerung (englisch: Programmable Logic Controller, PLC) In dieser Arbeit als Oberbegriff für automatische Steuergeräte auf der Steuerungsebene der Automatisierungspyramide verwendet.
SW	Software
UP	Unterprofil
Verteilte Anlage	Automatisierungstechnische Anlage mit verteilter ICS-Netzstruktur
Verteilte ICS-Netzstruktur	In dieser Arbeit bedeutet eine verteilte ICS-Netzstruktur, dass die ICS-Steuerungskomponenten über einen größeren Bereich als den eines Gebäudekomplexes verteilt sind. Die Anlage hat einen zentralen Leitstand, der mit den Steuerungskomponenten mittels WAN-Technik kommuniziert.
VDI	Verein Deutscher Ingenieure

VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VPN	Virtual Private Network: Logisches privates Netz auf Basis einer öffentlichen Netzinfrastruktur, das zusätzliche Authentisierungs- und Verschlüsselungstechnik, z.B. IPsec, verwendet.
WAN	Wide Area Network: Rechner- oder Kommunikationsnetz, dessen Ausdehnung über einen Gebäudekomplex hinausgeht. WANs können sich über die gesamte Welt ausdehnen. Ein Beispiel ist das Internet. In der Wasserwirtschaft wird für die Kommunikation über ein WAN häufig der Begriff Fernwirktechnik verwendet.
Wasserwirtschaft	In dieser Arbeit der Oberbegriff für Institutionen, die Dienstleistung innerhalb der Wasserversorgung und der Abwasserbeseitigung erbringen.
WS	Workstation, zum Beispiel in „Engineering-WS“
Zielobjekt	Zielobjekte sind im IT-Grundschutz die IT-Systeme, Infrastruktur, Anwendungen und Netzkomponenten, die den Informationsverbund ausmachen und im Rahmen einer Sicherheitskonzeption abgesichert werden sollen.