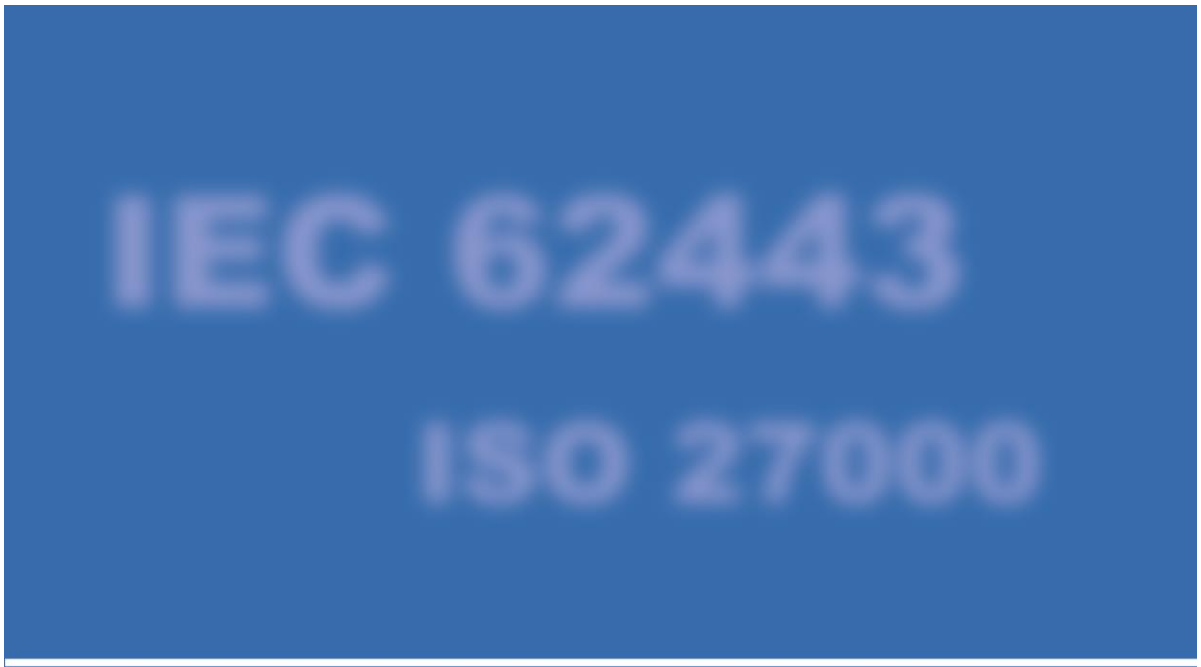
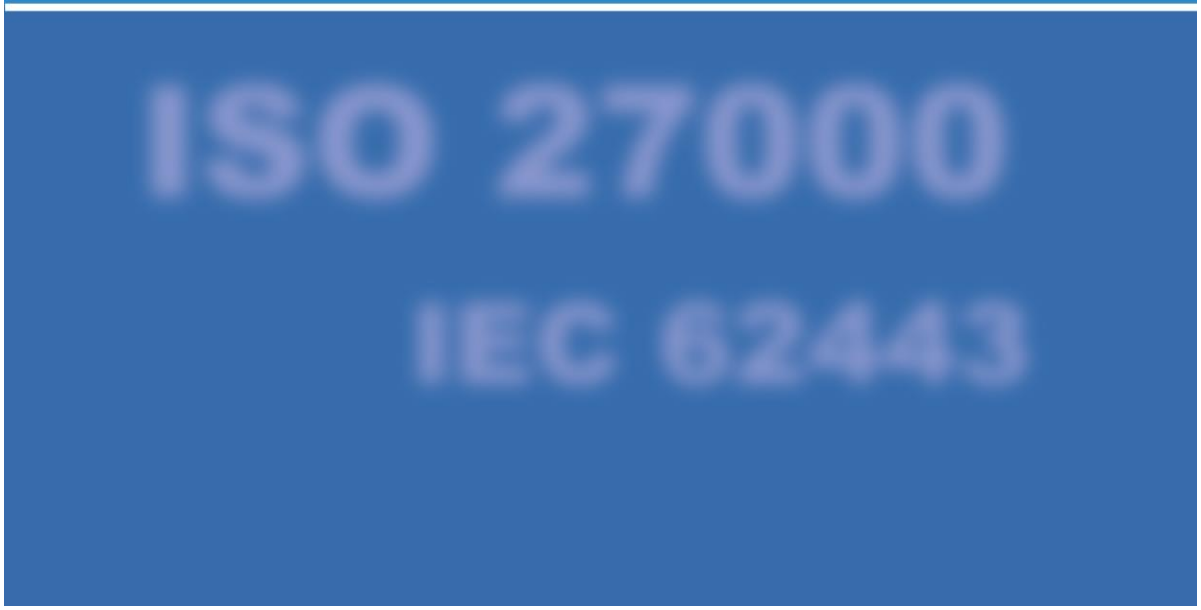


Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443

Eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie

Prof. Dr. Karl-Heinz Niemann - Hannover



Prof. Dr. Karl-Heinz Niemann

Email: Karl-Heinz@Niemann-on-line.de

Dieses Whitepaper ist in Zusammenarbeit mit der
ABB Automation Products GmbH, Heidelberg entstanden.

Inhaltsverzeichnis

1. Einführung

Planer und Betreiber von Produktionsanlagen stehen vor der Frage, welche Normen für die IT-Sicherheitskonzepte und ggf. auch für eine Auditierung dieser Anlagen anzuwenden sind. Da die Verantwortlichkeit in Bezug auf die IT-Sicherheit für die Operational Technology (OT) oft in anderen Händen liegt, als die für Information Technology (IT), gibt es hier gelegentlich abweichende Auffassungen darüber welche Normen zu Grunde zu legen sind.

Personen aus dem IT-Umfeld fokussieren in der Regel auf die Normreihe ISO 27001, während Personen aus dem OT-Umfeld eher die Normreihe IEC 62443 favorisieren. Dieser Beitrag beschreibt die Grundlagen und Ausrichtung der beiden Normreihen und gibt Anregungen, in welchem Kontext welche die Normen sinnvoll und ggf. auch kombiniert nutzbar sind.

Das Dokument schließt mit einer Empfehlung für ein Vorgehen im Bereich von Produktionsanlagen für die Fertigungs- und Prozessindustrie (OT-Security). Abschließend wird im Anhang noch am Beispiel einer Abwasserbehandlungsanlage die Anwendbarkeit der Normen diskutiert.

2. Überblick IT-Sicherheitsnormen und Standards

Im Bereich der IT-Sicherheit stehen Unternehmen eine Reihe von Normen bzw. Normreihen aber auch Empfehlungen von Herstellervereinigungen und Behörden zur Verfügung. Die Normen definieren den Stand der Technik und ermöglichen so eine standardisierte Vorgehensweise in Bezug auf Auslegung, Implementierung, Betrieb und Zertifizierung von IT-Sicherheitssystemen.

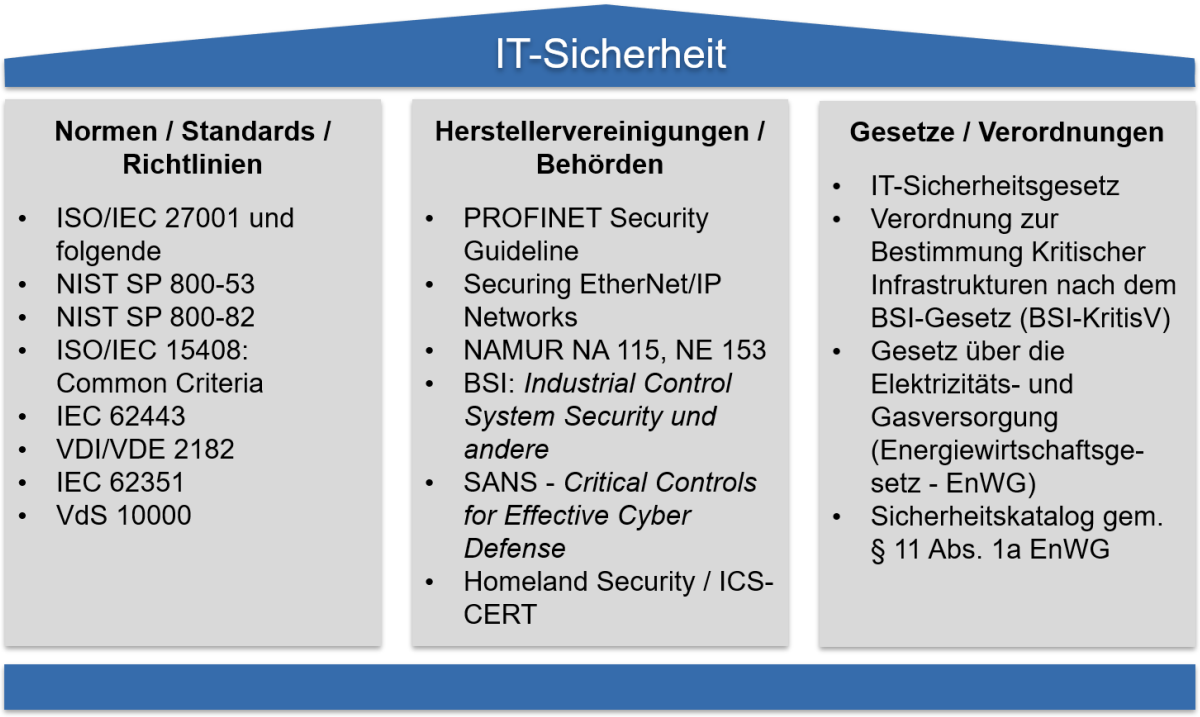


Abbildung 1: Übersicht über Normen und Standards zur IT-Sicherheit

Abbildung 1 gibt einen Überblick über Normen und Standards zur IT-Sicherheit. Neben allgemeinen Normen (ISO 27000-Reihe, IEC 15408, BSI-Grundschutzkatalog) sind auch Normen aufgeführt, die speziell den Produktionsbereich (IEC 62443, IEC 62351, VDI/VDE 2182) adressieren. Die Aufstellung wird ergänzt um eine Reihe von Standards von Hersteller-/Anwendervereinigungen (PROFINET, EtherNet/IP, NAMUR) und Behörden (BSI, Homeland Security).

Die folgenden Abschnitte fokussieren im Wesentlichen auf die Normreihen ISO 27000 und IEC 62443. Es ist zu beachten, dass beide Normreihen noch in der Weiterentwicklung befinden. Einen Überblick über die laufenden und künftig geplanten Arbeiten bietet die Normungs-Roadmap IT-Sicherheit der deutschen elektrotechnischen Kommission [DKE2017]. Eine Beschreibung der in Abbildung 1 genannten weiteren Normen und Standards findet sich in [NIE2017].

2.1. Die Normreihe ISO 27000

Die Normreihe ISO 27000 ist eine aus sechzig Teilnormen bestehende Normreihe zum Thema Informationssicherheitsmanagementsysteme, im Weiteren ISMS genannt. Eine Einführung und Übersicht über die einzelnen Teilnormen einschließlich einer kurzen Beschreibung findet sich in [DIN_EN_ISO_27000] oder online unter [ISE2020]. Die folgenden Abschnitte beschreiben die wesentlichen Teile der Normreihe.

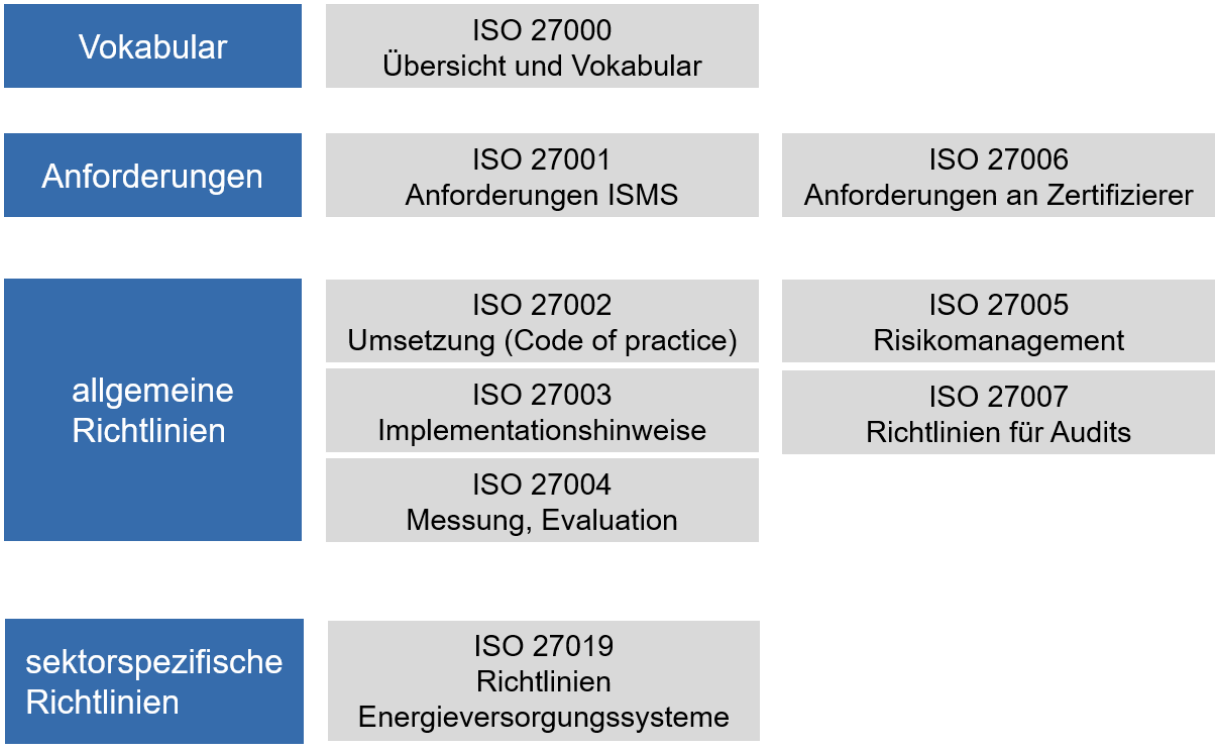


Abbildung 2: Auszug aus der Struktur der ISO 27000 Normreihe in Anlehnung an [KRO2017]

Abbildung 2 gibt einen Überblick über die wesentlichen Teile der ISO 27000 Normreihe. Die Normreihe teilt sich in vier Hauptteile: Vokabular und Übersicht, Anforderungen, allgemeine Richtlinien und sektorspezifische Richtlinien. Die in Abbildung 2 genannten Normteile geben jedoch nur einen Auszug und damit die wichtigsten Teile der Normreihe wieder.

2.1.1. Vokabular und Übersicht

Die **[DIN_EN_ISO_27000]** erläutert zunächst die verwendeten Fachbegriffe und gibt danach einen Überblick über die in der Normreihe enthaltenen weiteren Normen. Die Normreihe befasst sich mit dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Dieses ist nach [DIN_EN_ISO_27000] wie folgt definiert:

> *„Ein Informationssicherheitsmanagementsystem (ISMS) umfasst Politik, Verfahren, Richtlinien und damit verbundene Ressourcen und Tätigkeiten, die alle von einer Organisation gesteuert werden, um ihre Informationswerte zu schützen. Ein ISMS ist ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung,*

> *die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen. Es basiert auf einer Risikobeurteilung und dem Risikoakzeptanzniveau der Organisation und dient dazu, die Risiken wirksam zu behandeln und zu handhaben. Eine Anforderungsanalyse für den Schutz von Informationswerten und die Anwendung angemessener Maßnahmen, um den Schutz dieser Informationswerte bedarfsgerecht sicherzustellen, trägt zur erfolgreichen Umsetzung eines ISMS bei."*

Die Norm fokussiert auf die Informationssicherheit, um Vertraulichkeit, Verfügbarkeit und Integrität von Information sicherzustellen. Dabei wird ein prozessorientierter Ansatz verfolgt, um die erforderlichen Prozesse im Unternehmen zu identifizieren und zu lenken. Die Normreihe verfolgt einen risikobasierten Ansatz in dem Informationssicherheitsrisiken beschrieben, bewertet und behandelt werden. Die Aufrechterhaltung und Verbesserung des ISMS wird in ein einem kontinuierlichen Verbesserungsprozess überwacht, gesteuert und fortlaufend verbessert.

2.1.2. Anforderungen

Die **[DIN_EN_ISO_27001]** definiert Anforderungen an ISMS. Es legt die Anforderungen an die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Aufrechterhaltung und Verbesserung von formalisierten Informationssicherheitsmanagementsystemen (ISMS) im Zusammenhang mit den übergreifenden Unternehmensrisiken einer Organisation fest. Zu den Inhalten gehören u. a.:

- Kontext der Organisation
- Führung und Verpflichtung des Managements
- Sicherheitspolitik des Unternehmens
- Rollen, Verantwortlichkeiten und Befugnisse der Organisation
- Maßnahmen zum Umgang mit Risiken und Chancen
- Unterstützung, Kommunikation, Dokumentation
- Betrieb
- Bewertung der Leistung
- Verbesserungsprozess

Die **[ISO_27006]** spezifiziert Anforderungen und bietet Anleitungen für Stellen, die Audits und Zertifizierungen eines Informationssicherheits-Managementsystems (ISMS) durchführen. Sie ist in erster Linie dazu gedacht, die Akkreditierung von Zertifizierungsstellen zu unterstützen, die ISMS-Zertifizierungen anbieten.

Die enthaltenen Anforderungen müssen in Bezug auf Kompetenz und Zuverlässigkeit von jeder Stelle nachgewiesen werden, die eine ISMS-Zertifizierung anbietet, und der in dieser Internationalen Norm enthaltene Leitfaden bietet eine zusätzliche Interpretation dieser Anforderungen für jede Stelle, die eine ISMS-Zertifizierung anbietet. Diese Norm kann als Kriterienkatalog für Audits verwendet werden.

2.1.3. Allgemeine Richtlinien

Der Teil der allgemeinen Richtlinien zur ISO 27000-Reihe besteht aus mehreren Normen, die im Folgenden kurz beschreiben werden sollen.

Die **[DIN_EN_ISO_IEC_27002]** ist eine Anleitung für die Umsetzung von Informationssicherheitsmaßnahmen. Insbesondere Abschnitt 5 bis Abschnitt 18 geben spezifische Ratschläge und Anleitung für bewährte Praktiken zur Umsetzung der Maßnahmen, die in [DIN_EN_ISO_27001], A.5 bis A.18, festgelegt sind. Hierzu gehören beispielsweise:

- Vergabe von Zugangsrechten, Benutzerverwaltung, Zugangsverwaltung, Verwaltung von Kennwörtern.
- Datenträgerentsorgung
- Zugang zu Netzwerken und Netzwerkdiensten
- Schlüsselverwaltung
- Physischer Sicherheitsperimeter
- Sichern von Räumen und Einrichtungen
- Betriebsabläufe und Verantwortlichkeiten
- Schutz vor Schadsoftware
- Datensicherung
- Netzwerksicherheitsmanagement, Trennung von Netzwerken
- Lieferantenbeziehungen
- u.v.m.

Die obige Liste gibt keinen vollständigen Auszug aus der Norm, sondern soll lediglich als exemplarische Aufzählung dienen.

Die **[ISO_27003]** bietet einen Leitfaden zu den Anforderungen an ein Informationssicherheits-Managementsystem (ISMS), wie sie in ISO/IEC 27001 spezifiziert sind, und gibt Empfehlungen in Bezug auf diese. Die Abschnitte 4 bis 10 dieses Dokuments spiegeln die Struktur der [DIN_EN_ISO_27001] wider. Die [ISO_27003] definiert keine neuen Anforderungen, sondern liefert Erläuterungen und Umsetzungsempfehlungen zum besseren Verständnis. Daher besteht auch keine Verpflichtung, die Anleitungen in diesem Dokument zu beachten.

Die **[ISO_27004]** gibt Hilfestellung um Organisationen zu unterstützen die Informationssicherheitsleistung und Wirksamkeit des ISMS zu evaluieren um die Anforderungen aus ISO/IEC [DIN_EN_ISO_27001] Abschnitt 9.1, zu erfüllen. Es adressiert dabei:

- die Überwachung und Messung der Informationssicherheitsleistung;
- die Überwachung und Messung der Wirksamkeit eines Informationssicherheitsmanagementsystems einschließlich seiner Prozesse und Maßnahmen;
- die Analyse und Evaluation der Ergebnisse der Überwachung und Messung.

Die [ISO_27004] liefert somit ein Rahmenwerk, das es ermöglicht, die Wirksamkeit von ISMS gemäß [DIN_EN_ISO_27001] zu messen und zu bewerten. Hierbei werden auch Sicherheitskennzahlen und deren Ermittlung beschrieben.

Die **[ISO_27005]** enthält Richtlinien für das Risikomanagement der Informationssicherheit. Es unterstützt die in [DIN_EN_ISO_27001] spezifizierten allgemeinen Konzepte und soll die Umsetzung der Informationssicherheit auf der Grundlage eines Risikomanagementansatzes unterstützen. Die Kenntnis der in [DIN_EN_ISO_27001] und [DIN_EN_ISO_IEC_27002] beschriebenen Konzepte, Modelle, Prozesse und Terminologien ist für das vollständige Verständnis wichtig. Dieses Dokument ist auf alle Arten von Organisationen anwendbar (z. B. Wirtschaftsunternehmen, Behörden, gemeinnützige Organisationen), die beabsichtigen, Risiken zu managen, die die Informationssicherheit der Organisation gefährden können.

Die **[ISO_27007]** stellt eine Anleitung für Organisationen zur Verfügung, die interne oder externe Audits eines ISMS durchführen oder ein ISMS-Auditprogramm nach den in ISO/IEC 27001 festgelegten Anforderungen handhaben müssen.

Ein Audit des Informationssicherheits-Managementsystems (ISMS) kann anhand einer Reihe von Auditkriterien durchgeführt werden, z. B.:

- Anforderungen, die in [DIN_EN_ISO_27001] definiert sind;
- Richtlinien und Anforderungen, die von relevanten interessierten Parteien festgelegt wurden;
- gesetzliche und regulatorische Anforderungen;
- ISMS-Prozesse und Kontrollen, die von der Organisation oder anderen Parteien definiert wurden;
- Managementsystemplan(e), der/die sich auf die Bereitstellung spezifischer Ergebnisse eines ISMS bezieht/beziehen (z. B. Pläne zum Umgang mit Risiken und Chancen bei der Einrichtung des ISMS, Pläne zum Erreichen von Informationssicherheitszielen, Risikobehandlungspläne, Projektpläne).

Die Norm bietet einen Leitfaden für alle Größen und Arten von Organisationen und ISMS-Audits unterschiedlicher Größenordnung. Das Dokument konzentriert sich auf interne ISMS-Audits (first party) und ISMS-Audits, die von Organisationen bei ihren externen Dienstleistern durchgeführt werden (second party).

2.1.4. Sektorspezifische Richtlinien

Die ISO-27000-Reihe stellt einige sektorspezifische Richtlinien zur Verfügung, z. B. für Cloud-Computing oder die Telekommunikation. Im Kontext der Automatisierungstechnik ist die sektorspezifische Richtlinie **[ISO_27019]** von Interesse. Diese bietet einen Leitfaden, der auf [DIN_EN_ISO_IEC_27002] basiert und auf Prozessleitsysteme angewandt wird, die von der Energieversorgungsbranche zur Steuerung und Überwachung der Produktion oder Erzeugung, Übertragung, Speicherung und Verteilung von elektrischer Energie, Gas, Öl und Wärme sowie zur Steuerung der zugehörigen unterstützenden Prozesse verwendet werden. Dies umfasst insbesondere Folgendes:

- Zentrale und dezentrale Prozesssteuerungs-, -überwachungs- und -automatisierungstechnik sowie zu deren Betrieb eingesetzte Informationssysteme, wie Programmier- und Parametriergeräte;

- Digitale Steuerungen und Automatisierungskomponenten wie Steuer- und Feldgeräte oder Speicherprogrammierbare Steuerungen (SPS), einschließlich digitaler Sensor- und Aktor-Elemente;
- Alle weiteren unterstützenden Informationssysteme, die im Bereich der Prozesssteuerung eingesetzt werden, z. B. für ergänzende Aufgaben der Datenvisualisierung sowie zur Steuerung, Überwachung, Datenarchivierung, Historienprotokollierung, Berichterstattung und Dokumentation;
- Kommunikationstechnik, die im Bereich der Prozesssteuerung eingesetzt wird, z. B. Netzwerke, Telemetrie, Fernwirkanwendungen und Fernwirktechnik;
- Komponenten der Advanced Metering Infrastructure (AMI), z. B. intelligente Zähler;
- Messgeräte, z. B. für Emissionswerte;
- Digitale Schutz- und Sicherheitssysteme, z. B. Schutzrelais, Sicherheits-SPSen, Notsteuerungsmechanismen
- Energiemanagementsysteme, z. B. von Distributed Energy Resources (DER), elektrischen Ladeinfrastrukturen, in Privathaushalten, Wohngebäuden oder industriellen Kundenanlagen;
- Verteilte Komponenten von Smart-Grid-Umgebungen, z. B. in Energienetzen, in privaten Haushalten, Wohngebäuden oder industriellen Kundenanlagen;
- Alle Software, Firmware und Anwendungen, die auf den oben genannten Systemen installiert sind, z.B. DMS (Distribution Management System) Anwendungen oder OMS (Outage Management System);
- Alle Räumlichkeiten, in denen die oben genannten Geräte und Systeme untergebracht sind;
- Fernwartungssysteme für die oben erwähnten Systeme.

Die [ISO_27019] gilt nicht für die Prozesssteuerungsdomäne von kerntechnischen Anlagen. Diese Domäne wird durch IEC 62645 abgedeckt. Die [ISO_27019] enthält auch die Anforderung, die in [DIN_EN_ISO_27001] beschriebenen Prozesse zur Risikobewertung und -behandlung an den Sektor der Energieversorgungsunternehmen anzupassen.

2.1.5. Weiterführende Literatur zur ISO 27000

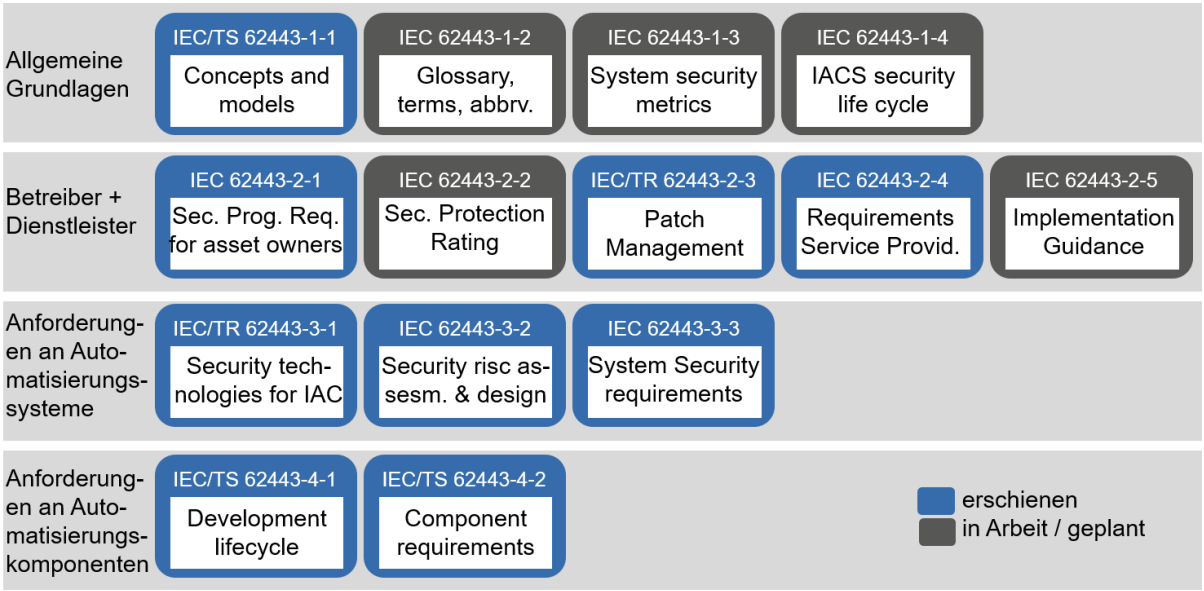
Einsteigern in die Normreihe ISO 27000 wird empfohlen zunächst einen Zugang über ein Lehrbuch und nicht über die Normen direkt zu suchen. Hierzu können z. B. [BRE2020], [KER2020] dienen. Lesern, die einen zusätzlichen Fokus auf dem Thema Risikomanagement haben, sei zusätzlich [KLI2015] empfohlen. Eine online verfügbare Normenübersicht mit Kurzbeschreibungen der Einzelnormen findet sich unter [ISE2020].

2.2. Die Normreihe IEC 62443

Die Normreihe IEC 62443 wird von der Internationalen elektrotechnischen Kommission (IEC) und der International Society of Automation (ISA) entwickelt. Die ersten Arbeiten an der Norm wurden in der Arbeitsgruppe ISA SP99 gestartet und werden zurzeit in einer Kooperation aus IEC und ISA fortgeführt. Daher finden sich in vielen Dokumenten noch Referenzen auf Arbeitsgruppen und Dokumente der ISA.

Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443

Basierend auf den Modellen und Anforderungen der ISO 27000 Normreihe werden in der IEC 62443 Normreihe die speziellen Anforderungen der IT-Sicherheit im Produktionsbereich berücksichtigt. Abbildung 3 zeigt die Struktur der Normreihe.



Quelle: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung

Abbildung 3: Teile der IEC 62443, in Anlehnung an [DKE2020]

Die Norm-Reihe IEC 62443 besteht aus vier Hauptbereichen, die in den folgenden Kapiteln einschließlich der zugeordneten Normen vorgestellt werden.

2.2.1. Allgemeine Grundlagen

Abbildung 4 zeigt die IEC 62443-Normen des Teils „Allgemeine Grundlagen. Die grau hinterlegten Teile sind zurzeit noch in Bearbeitung und nicht veröffentlicht.

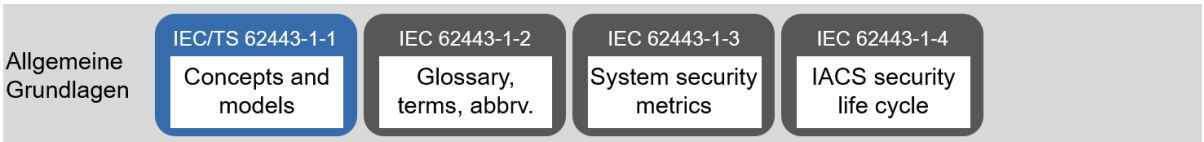


Abbildung 4: IEC 62443 – Teil 1 Allgemeine Grundlagen in Anlehnung an [DKE2020]

Die [IEC_62443-1-1] ist eine technische Spezifikation, die die Terminologie, Konzepte und Modelle für die Sicherheit von industriellen Automatisierungs- und Steuerungssystemen (IACS) definiert. Sie bildet die Grundlage für die übrigen Normen der Reihe IEC 62443. Bestandteile dieser Norm sind u. a.:

- Risk Assessment
- Reifegrad des Security Programms
- Polices

Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443

- Zonen und Conduits
- Modelle
- Referenzarchitektur

Der Teil [IEC_62443-1-2] definiert alle Begriffe, die in den Normen verwendet werden. Der Teil [IEC_62443-1-3] definiert Metriken für die Bewertung der IT-Sicherheit, im Teil [IEC_62443-1-4] werden der Sicherheitslebenszyklus und Anwendungsfälle beschrieben. Alle drei Teile sind noch nicht veröffentlicht und stehen nur im Entwurf für Arbeitskreismitarbeiter zur Verfügung.

2.2.2. Betreiber und Dienstleister

Abbildung 5 zeigt den Teil „Betreiber und Dienstleister" der Normreihe IEC 62443.

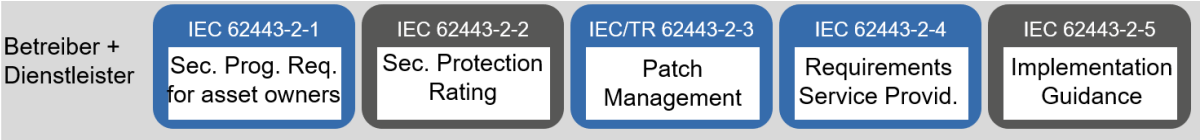


Abbildung 5: IEC 62443 - Teil 2 Betreiber und Dienstleister in Anlehnung an [DKE2020]

Dieser Teil beschreibt das IT-Sicherheits-Management-System und definiert damit die Organisation der IT-Sicherheit, gefolgt von Implementierungshilfen.

Der Teil **[IEC_62443-2-1]** beschreibt Anforderungen an ein IT-Sicherheits-Managementsystem, z. B die

- Definition von Security Prozeduren
- Risiko-Management
- Definition von Trainingsanforderungen
- Pläne zur Business Continuity
- Zugangskontrolle
- Verbesserungsprozess
- usw.

Der Teil **[ISA_62443-2-2]** gibt Hinweise, wie und in welchen Bereichen diese Prozeduren zu implementieren sind. Er spezifiziert ein Rahmenwerk für die Evaluation des Schutzes eines I-ACS. Es beinhaltet ein Verfahren zur Kombination der Evaluation von sowohl organisatorischen als auch von technischen Sicherheitsmaßnahmen in Zahlenwerten, den sogenannten „Protection Level". Das Rahmenwerk bildet die Struktur für die Evaluation der Defense-in-Depth-Strategie des IACS im Betrieb auf der Grundlage der technischen und organisatorischen Anforderungen, die in anderen Dokumenten der IEC-Normenreihe 62443 spezifiziert sind. [DKE2020]. Dieser Teil liegt zurzeit nur im Entwurf vor.

Das Aktualisieren der Software von Automatisierungssystemen, das Patchen, ist von besonderer Bedeutung, weil es bei unsachgemäßem Vorgehen zu Betriebsstörungen kommen kann. Daher widmet die Normreihe dem Patch-Management einen eigenen Teil **[IEC_62443-2-3]**.

Der Teil **[DIN_EN_IEC_62443-2-4]** befasst sich mit dem Einsatz von Dienstleistern für Inbetriebnahme und Service aus Sicht der IT-Sicherheit. „Sie legt Anforderungen zu IT-Sicherheitsleitlinien, Vorgehensweisen und Praktiken fest, die auf die Lieferanten von industriellen Automatisierungssystemen während des Lebensweges ihrer Produkte anwendbar sind sowie auf Instandhaltungsdienstleister. Im Besonderen sind Integratoren angesprochen, die technische Lösungen zu einem Gesamtsystem zusammenführen." [DKE2020] Diese Norm ist in deutscher Sprache verfügbar.

Die **[IEC_62443-2-5]** ist geplant und soll Implementierungshinweise für Betreiber enthalten. Entwürfe zu diesem Normteil liegen dem Autor noch nicht vor.

2.2.3. Anforderungen an Automatisierungssysteme

Abbildung 6 zeigt die Teile der Norm, welche die Anforderungen an Automatisierungssysteme beschreiben.

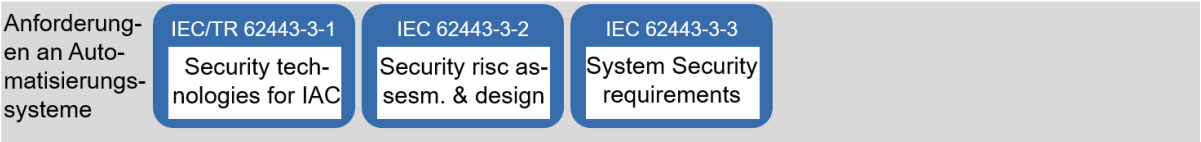


Abbildung 6: IEC 62443 - Teil 3 Anforderungen an Automatisierungssysteme in Anlehnung an [DKE2020]

Der Teil [IEC_62443_3_1] beschreibt zunächst die zu Grunde liegenden Technologien wie z. B. Authentifizierung, Verschlüsselung, Filterung und Logging. Der Teil [IEC_62443_3_2] beschreibt den gesamten Ablauf der Sicherheitsanalyse und darauf aufbauend die Strukturierung einer Anlage in Zonen (abgeschottete Bereiche) und Conduits (gesicherte Verbindungen zwischen den Bereichen). Damit soll eine automatisierungstechnische Anlage in Teilbereiche unterteilt werden, die wiederum gegeneinander abgeschottet sind. Der Teil [IEC_62443_3_3] beschreibt konkrete Anforderungen an Automatisierungssysteme in Form von grundlegenden Anforderungen (Foundational Requirements). Diese Foundational Requirements (FR) legen die IT-Sicherheitseckpunkte des Systems fest.

- Identifizierungs-/Authentifizierungs- Kontrolle (AC)
  - Erfassung aller Benutzer (Mensch, Software, Komponente)
- Benutzerverwaltung (UC)
  - Durchsetzen der Zugangsberechtigungen von Benutzern
- Systemintegrität (DI)
  - Verhindern von Manipulation der IACS
- Vertraulichkeit von Daten (DC)
  - Absichern von Daten in Kommunikationskanälen und Speichern
- Einschränkung des Datenflusses (RDF)
  - Zonenaufteilung und geschützte Kommunikationskanäle
- Zeitnahe Reaktion auf Ereignisse (TRE)
  - Schnelle Benachrichtigung von Entitäten über IT-Sicherheitsvorfälle
- Verfügbarkeit von Ressourcen (RA)

- Sicherstellung der Verfügbarkeit von Ressourcen

Dieser Teil der Norm liefert konkrete Hinweise für Planer und Betreiber von Automatisierungssystemen in Bezug auf konkrete technische Maßnahmen.

Diese Maßnahmen werden so genannten Security Leveln (SL) zugeordnet.

Tabelle 1: Security Level nach [DIN_EN_IEC_62443-4-1]

SL	Beschreibung
1	Verhindern der nicht autorisierten Offenlegung von Informationen durch Abhören oder zufälliges Aufdecken.
2	Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit einfachen Mitteln bei geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation suchende Einheit.
3	Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit raffinierten Mitteln und moderatem Aufwand, IACS-spezifischen Fertigkeiten und mittlerer Motivation suchende Einheit.
4	Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit raffinierten Mitteln und erheblichem Aufwand, IACS-spezifischen Fertigkeiten und hoher Motivation suchende Einheit.

Die Norm nennt die Level SL1 (geringe Anforderungen) bis SL4 hohe Anforderungen. Abhängig von Schutzbedarf der Anlage können die Anforderungen gemäß dem gewünschten Security Level ausgewählt werden.

2.2.4. Anforderungen an Automatisierungskomponenten

Abbildung 7 zeigt die Normteile, welche die Anforderungen an den Entwicklungsprozess und die Komponenten des Automatisierungssystems definieren. Diese Teile richten sich an die Hersteller von Automatisierungssystemen.

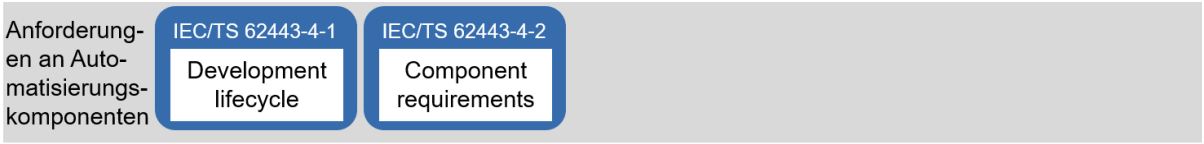


Abbildung 7: IEC 62443 – Teil 4 Anforderungen an Komponenten von Automatisierungssystemen in Anlehnung an [DKE2020]

Der Teil [DIN_EN_IEC_62443-4-1] definiert den Entwicklungsprozess, der bei der Entwicklung von Komponenten für die Automatisierungstechnik zu beachten ist.

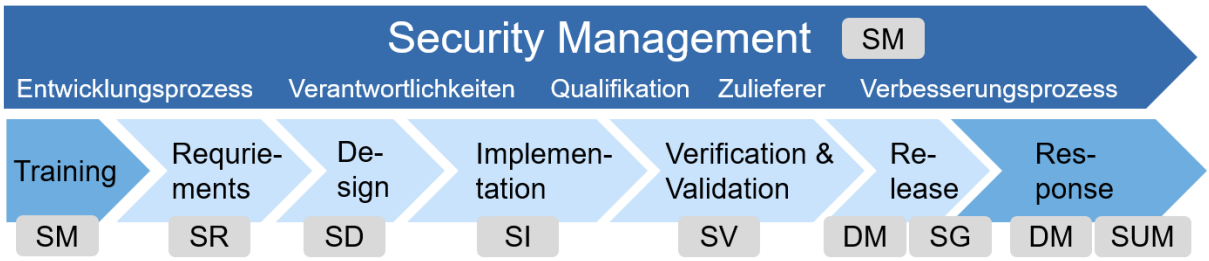


Abbildung 8: Sicherer Entwicklungslebenszyklus, in Anlehnung an [WAL2020]

Abbildung 8 zeigt den in der Norm beschriebenen sicheren Entwicklungslebenszyklus. Es ist zu erkennen, dass sich dieser über alle Phasen des Entwicklungsprozesses erstreckt. Hersteller von Automatisierungskomponenten können über die Implementierung dieser Norm den Produktentwicklungslebenszyklus gemäße dem Security-by-Design-Ansatz aufbauen und so die Basis für die Zertifizierung von Komponenten legen. Die Kurzbezeichner in den grauen Boxen entsprechen den Anforderungsklassen aus den jeweiligen Teilen der Norm. Für eine derart aufgebaute Organisation werden die Reifegrade (Maturity Level) von 1 bis 4 vergeben.

Der Teil [DIN_EN_IEC_62443-4-2] beschreibt die technischen Anforderungen für die Komponenten von Automatisierungssystemen, Applikation und Funktionen. Die Struktur der Anforderungen folgt der [DIN_IEC_62443-3-3], jedoch werden hier die Anforderungen beschrieben, welche die Komponenten erfüllen müssen. Hierbei wird nach Komponentenanforderungen (CR= Component requirement) und weitergehenden Anforderungen (RE = Requirement enhancements) unterschieden. Diesen Anforderungen leiten sich ab aus dem Systemanforderungen (SR = System requirement).

Die in diesem Dokument festgelegten Arten von Komponenten eines IACS sind

- Softwareanwendungen,
- Host-Geräte,
- eingebettete Geräte und
- Netzwerkkomponenten.

Die Mehrheit der CR und RE gilt für alle vier Komponentenarten und wird zu einer einzigen Komponentenanforderung (CR) zusammengefasst. Einige CR und RE gelten nur für einen bestimmten Komponententyp. Der ZVEI gibt mit [ZVE2017] Herstellern von Automatisierungskomponenten einen Einstieg in das Thema.

2.2.5. Zuordnung der IEC 62443-Normteile zu den Akteuren im Sicherheitsprozess

Abbildung 9 gibt einen Überblick über die Akteure im IT-Sicherheitsprozess und die Zuordnung der IEC 62443-Normteile zu diesen Akteuren.

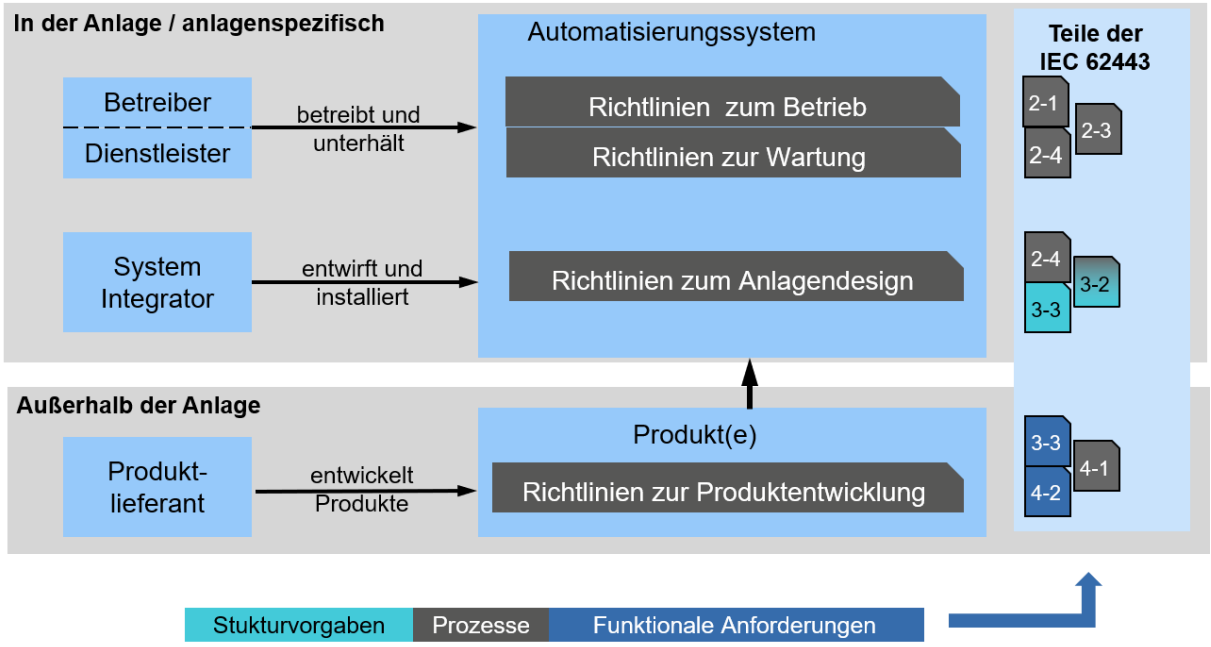


Abbildung 9: Zuordnung der ICE 62443-Normteile zu den Akteuren im Sicherheitsprozess (in Anlehnung an [ISA_62443-2-2])

Die Rolle Betreiber Dienstleister ist verantwortlich für den Betrieb und die Unterhaltung einer Produktionsanlage. Für diese Akteure sind im Wesentlichen die Richtlinien zum Betrieb und zur Wartung relevant. Hier sind die Normteile relevant, die Aufbau und Betrieb des ISMS [IEC_62443-2-1] und die Einbindung von Dienstleistern [IEC_62443-2-4] regeln. Weiterhin ist für die Betreiber der Teil [IEC_62443-2-3] relevant, der die Aktualisierung der Leitsystemsoftware (Patch Management) regelt.

Die Rolle des Systemintegrators entwirft und installiert das Automatisierungssystem. Hier ist der Normteil [DIN_IEC_62443-3-3] relevant, der Vorgaben bzgl. des Aufbaus und der Strukturierung der Anlage macht. Der Teil [DIN_EN_62443-3-2] kann zusätzlich zur Sicherheitsrisikobeurteilung und zur Systemgestaltung herangezogen werden. Sofern der Planungsprozess durch einen Dienstleister durchgeführt wird, ist noch der Teil [IEC_62443-2-4] zu beachten, der Anforderungen an Dienstleiser (Service Provider) beschreibt. Führt der Anlagenbetreiber die Planungsarbeiten selber durch, gelten die in diesem Abschnitt genannten Normen sinngemäß auch für den Betreiber in seiner Rolle als Anlagenplaner.

Die dritte Rolle ist die der Produktlieferanten. Für diese Lieferanten gilt zunächst die [DIN_EN_IEC_62443-4-1], welche die Anforderungen an einen sicheren Entwicklungsprozess (Security by design) spezifiziert. Die Anforderungen an die Produkte, die der Produktlieferant entwickelt, beschreibt der Teil [DIN_EN_IEC_62443-4-2]. Da sich die Anforderungen in dieser

Norm aus Systemanforderungen ableiten, sollte der Produktlieferant auch diese Systemanforderungen [DIN_IEC_62443-3-3] kennen und berücksichtigen.

2.2.6. Weiterführende Literatur zur IEC 62443

Die Normen der Reihe IEC 62443 sind bisher nur zum Teil veröffentlicht. Der überwiegende Teil der Normreihe liegt jedoch zumindest als Entwurf vor. Der aktuelle Stand der Arbeiten und der Freigabestatus der Normteile kann unter [ISA2020] eingesehen werden. Der Stand der deutschen Übersetzungen ist in [DKE2020] abrufbar.

In [KOB2021] wird ein Überblick über die Normreihe IEC 62443 gegeben und die Zusammenhänge zwischen den Normteilen werden erläutert. Dieses Buch gibt einen kompakten und schnellen Einstieg in die Norm. [GUN2018] gibt in seinem Buch ausführliche Hinweise zu Einführung der IEC 62443.

Die Branchenverbände ZVEI [ZVE2017] und VDMA [VDM2016] stellen Leitfäden für die Umsetzung der IEC 62443 zur Verfügung. Der ZVEI aus Herstellersicht, der VDMA aus Betreibersicht.

3. Abgrenzung der IT-Sicherheitsnormen

Nachdem in den vorangehenden Kapiteln die beiden Normreihen IEC 62443 und ISO 27000 im Detail beschrieben wurden, soll nun eine Abgrenzung der beiden Normen in Bezug auf Ihre Anwendbarkeit im Produktionsbereich erfolgen. Hierbei ist zu beachten, dass die IT-Sicherheit ein unternehmensübergreifendes Thema ist und dass somit der Produktionsbereich nicht für sich alleine gesehen werden kann. Dennoch liegen im Produktionsbereich andere Anforderungen in Bezug auf die IT-Sicherheit vor, als im Bürobereich. Daher werden im folgenden Kapitel zunächst diese Anforderungen beschrieben und die Bereich IT (Information Technology) und OT (Operational Technology) gegeneinander abgegrenzt.

3.1. Abgrenzung der Anwendungsdomänen OT und IT

Im Folgenden werden die Anwendungsdomänen IT und OT zunächst gegeneinander abgegrenzt, um daraus im weiteren Verlauf des Kapitels spezifische Anforderungen an das IT-Sicherheitsmanagement abzuleiten. Tabelle 2 definiert die Begriffe IT und OT und zeigt Anwendungsbeispiele.

Tabelle 2: Abgrenzung der Domänen IT und OT

Domäne	Definition nach Gartner Group [GAR2021]	Anwendungsbeispiele
IT	"IT" ist der gängige Begriff für das gesamte Spektrum an Technologien zur Informationsverarbeitung, einschließlich Software, Hardware, Kommunikationstechnologien und zugehörige Dienstleistungen. Im Allgemeinen umfasst die IT keine eingebetteten Technologien, so lange diese keine Daten für den Unternehmensgebrauch erzeugen.	• Client-Systeme des Personals • Laptops • Webserver • Mail-Server • SAP-Systeme • File Server • Netzwerke
OT	Operationelle Technologie (OT) ist Hard- und Software, die durch die direkte Überwachung und/oder Steuerung von industriellen Geräten, Anlagen, Prozessen und Ereignissen eine Veränderung feststellt oder bewirkt.	• Speicherprogrammierbare Steuerungen • Anzeigesysteme (Touch Panels) • Server für die Produktionssteuerung • Industrieroboter • Remote IO-Systeme • Echtzeit-Netzwerke

Nach dieser Definition der beiden Anwendungsdomänen sollen nun die Anforderungen in Bezug auf die IT-Sicherheit betrachtet werden. Dabei ist zunächst zu berücksichtigen, dass innerhalb der beiden Domänen unterschiedlichen Begriffe zum Einsatz kommen. Abbildung 10 zeigt die Abgrenzung der Begriffe.

Schutz der IT im Bürobereich	Schutz der IT im Produktionsbereich	Schutz personen-bezogener Daten
IT-Security IT-Sicherheit Informationssicherheit Information Security	Cyber-Security OT-Security AT-Security ICS-Security	Datenschutz Datensicherheit

Abbildung 10: Abgrenzung der Begriffe IT / OT Security

Es ist zu erkennen, dass beim Schutz der IT im Bürobereich u. a. der Begriff „Informationssicherheit“ IT-Sicherheit oder IT-Security verwendet wird. Bei dem Begriff Informationssicherheit kann es sich zunächst um den Schutz von Informationen allgemein. Hierzu gehört z. B. auch geistiges Eigentum. Die [ISO_27000] verwendet den Begriff der „Informationssicherheit“ und definiert diesen mit der Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Der Begriff IT-Sicherheit oder IT-Security ist ein Teilaspekt der Informationssicherheit. Hierbei handelt es sich um den Schutz von technischen Systemen. Bei Produktionsanlagen kommt oft der Begriff „Cyber-Security“ oder „ICS-Security“ [BSI_2014] zum Einsatz. Diese fokussiert auf die Sicherheit von Produktionsanlagen (OT). Der Begriff Datenschutz wird hier nur der Vollständigkeit halber erwähnt, hat hier aber keine Relevanz. Bezogen auf den unterschiedlichen Anwendungsbereich der IT und der OT leiten sich daraus auch unterschiedliche Anforderungen in Bezug auf die IT- und OT-Security ab. Diese sind in Tabelle 3 dargestellt.

Tabelle 3: Anforderungen IT- und OT Security (in Anlehnung an [FLA2019])

	IT	OT
	Security Eigenschaften	
Priorisierung der Security Anforderungen	Vertraulichkeit, Integrität, Verfügbarkeit, Nichtabstreitbarkeit	Verfügbarkeit, Integrität, Nichtabstreitbarkeit, Vertraulichkeit
Verfügbarkeit	Wichtig, aber nicht kritisch	Kritisch
Integrität	Wichtig	Wichtig
Vertraulichkeit	Kritisch	Nicht kritisch
	Technologie	
Echtzeitverhalten	Erwünscht, aber unkritisch (Quality of Service)	Kritisch für Funktion der Produktionsanlage
Eingesetzte Technologie	Homogen	Sehr heterogen, verschiedene Protokolle, eingebettete Systeme.
	Betrieb	
Nutzungsdauer	3 … 5 Jahre	Teilweise mehr als 20 Jahre
Software Update	Automatisch	Kritisch: Teilweise nur bei Anlagenstillständen, Vorab-Test der Updates erforderlich, Freigabe der Updates durch Leitsystemhersteller erforderlich.
Outsourcing	Üblich	Für Planung, Errichtung und Wartung üblich, nicht für den Betrieb.
	Security Management	
Risikoanalysen	Global, unternehmensweit	Anlagenbezogen
Nutzer-Authentisierung und Zugriffsrechte	Personenbasiert, zentral verwaltet	Oft rollenbasiert, Schichtzugänge für Nutzergruppen
Security Awareness	Hoch	Wenig ausgeprägt
Einsatz von Anti-Virus-Software	Üblich	Problematisch, oft nicht aktuell

Die Angaben in Tabelle 3 zeigen, dass für den IT- und den OT-Bereich unterschiedliche Anforderungen in Bezug auf die IT-Sicherheit bestehen. Dies hat dazu geführt, dass für die IT-Sicherheit von Produktionsanlagen, zusätzlich zur ISO 2700-Reihe die Normenreihe IEC 62443 entstanden ist, die diese besonderen Anforderungen adressiert.

3.2. Unterschiede und Ähnlichkeiten ISO 27000 und IEC 62443

Nachdem im vorangehenden Kapitel die unterschiedlichen Anforderungen der IT und der OT beschrieben wurden, sollen nun die Unterschiede und Ähnlichkeiten betrachtet und auf die beiden Normreihen ISO 27000 und IEC 62443 abgebildet werden.

Die **ISO 27000 Reihe** beschreibt den Aufbau und Betrieb eines IT-Sicherheitsmanagement-Systems (ISMS). Die Normreihe adressiert allgemein die Informationssicherheit und unterscheidet dabei nicht, ob es sich um Daten in IT-Systemen oder auch um geistiges Eigentum handelt. Die Norm [DIN_EN_ISO_27001] ist dabei als Grundnorm anzusehen, in der wesentliche Anforderungen an die Organisation der IT-Sicherheit, wie z. B. Planung, Verantwortlichkeiten, Risikobeurteilung, Kommunikation, Ressourcen, internes Audit) definiert. Man kann also festhalten, dass die organisations- und ablaufbezogenen Aspekte der IT-Sicherheit im Vordergrund stehen. Die [DIN_EN_ISO_IEC_27002] definiert konkrete Anforderungen an die IT-Sicherheit, wie z. B. Zugangssteuerung, Netzwerksicherheit, Trennung von Netzwerken, etc. Ein Fokus der Normreihe liegt auf der Überwachung und Evaluation des ISMS [ISO_27004] und der Zertifizierung [ISO_27007]. Die Norm ist generisch und ist grundsätzlich für Anwendungen in der IT genauso zu verwenden wie für die OT. Allerdings nimmt die Norm keinen speziellen Bezug zu den Anforderungen der OT, wie sie z. B. in Tabelle 3 beschrieben sind. Eine Ausnahme macht allerdings der Teil [DIN_IEC_27019], der speziell auf Energieversorgungssysteme fokussiert.

Die **IEC 62443 Reihe** fokussiert auf den Schutz industrieller Automatisierungssysteme und ist damit dem Bereich der Operational Technology (OT) zuzuordnen. Besonderheiten der OT finden Berücksichtigung. So werden z. B. Anforderungen in Bezug auf Dienstleister [DIN_EN_IEC_62443-2-4] genauso berücksichtig, wie z. B. das Patchmanagement in Produktionsanlagen Teil [IEC_62443-2-3]. Auch der Aspekt des Aufbaus und Betriebs eines ISMS ist in der Normreihe enthalten [IEC_62443-2-1], im Fokus stehen aber konkrete technische Anforderungen an Automatisierungssysteme [IEC_62443_3_3] und die Komponenten von Automatisierungssystemen [DIN_EN_IEC_62443-4-2], wobei sich letztere an die Hersteller von Automatisierungskomponenten richtet.

Beide Normreihen weisen Gemeinsamkeiten auf. Es ist zu erkennen, dass sich die grundlegenden Konzepte und Technologien in beiden Normreihen wiederfinden. Es bleibt jedoch festzuhalten, dass die Normreihe IEC 62443 einen klaren Fokus auf die Automatisierungstechnik aufweist, währen die ISO 27000 Reihe eher prozessorientiert und generisch ist. Siehe hierzu auch [KOH2018].

Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443

Fokus Organisation	1. Management Commitment. 2. Organisation der Zuständigkeiten und Prozesse. 3. Leitlinie/ Richtlinie. 4. Personal. 5. Wissen.
Fokus Technik	6. Identifizieren, Bewerten und Schützen der Assets: 1. Automatisierungssysteme. 2. Netzwerke. 7. Externer Zugriff.
Fokus Organisation	8. Datensicherung. 9. Störungen und Ausfälle. 10. IT-Sicherheitsvorfälle.

Abbildung 11: Aspekte der IT-Sicherheit in Produktionsanlagen

Abbildung 11 zeigt die verschiedenen Aspekte der IT-Sicherheit in Produktionsanlagen. Es ist zu erkennen, dass dabei zum einen der Fokus auf organisatorischen und zum anderen auf technischen Aspekten liegt. Für die Aufgabenpunkte mit Fokus Technik ist die Anwendung der IEC 62443-Normreihe sinnvoll, weil hier eine klare Ausrichtung auf die Anforderungen der Automatisierungstechnik besteht. Für die Aufgaben im Produktionsbereich mit Fokus Organisation kann wahlweise die [IEC_62443-2-1] aber auch die Normreihe ISO 27000 herangezogen werden. Sofern für die IT schon ein ISMS nach ISO 27000 existiert, macht es Sinn, die organisatorischen Aspekte in der OT auch danach zu behandeln. Die Erfahrungen aus einer solch kombinierten Nutzung beider Normenteile bei einem Energieverteilnetzbetreiber werden in [MON2019] beschrieben.

Ein vergleichbarer Ansatz wird in [FRI2019] beschrieben. Auch dieses Dokument beschreibt die gemeinsame Nutzung beider Normenreihen im Bereich der Energieverteilung.

Weitere Informationen zur Organisation der IT-Sicherheit findet sich auch in [NIE2018]. Bei der Betrachtung dieser Normen kommt immer wieder die Fragen einer Zertifizierung von ISMS oder Produkten auf. Die Zertifizierung, z. B. von Automatisierungskomponenten nach der [DIN_EN_IEC_62443-4-2] ist eine Grundlage für die Sicherstellung der IT-Sicherheit einer Produktionsanlage nach der [DIN_IEC_62443-3-3].

3.3. Überlappungen der Anforderungen der IEC 62443 und der ISO 27000

Die vorangehenden Kapitel haben gezeigt, dass die beiden betrachteten Normreihe IEC 62443 und ISO 27000 Überlappungen aufweisen. Eine Abbildung der Anforderungen beider Normreihen (Mapping) ist über verschiedene Quellen verfügbar. Siehe hierzu

- [ÖST2020] Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices
- [BSI2013] ICS-Security-Kompendium
- [ENI2017] ENISA Mapping of OES Security Requirements to Specific Sectors.

4. Zusammenfassung und Empfehlung

Aus den vorangehenden Kapiteln lassen sich folgende Empfehlungen ableiten:

1.) Sofern das Unternehmen bereits über ein ISMS nach ISO 27000 verfügt, sollten die organisatorischen Prozesse im Produktionsbereich diesen Konzepten folgen, um zu einer einheitlichen Prozesslandschaft zu gelangen.
2.) Sofern kein ISMS existiert und nur der Produktionsbereich betrachtet werden soll, kann das ISMS nach [IEC_62443-2-1] realisiert werden.
3.) Kleine und mittlere Unternehmen, für die ein ISMS nach ISO 27000 möglichweise zu aufwändig ist, sollten die Anwendung eines vereinfachten ISMS, z. B. nach BSI Grundschutz [BSI_200-1] oder [VDS_10000] und [VDS_10020] in Betracht ziehen.
4.) Die spezifischen technischen Aspekte der IT-Sicherheit im Produktionsbereich sollten bevorzugt nach der [DIN_IEC_62443-3-3] erarbeitet werden.
5.) Für die betrieblichen Aspekte der IT-Sicherheit im Produktionsbereich können zusätzlich die [IEC_62443-2-3] und die [DIN_EN_IEC_62443-2-4] herangezogen werden.
6.) Anlagen, die der kritischen Infrastruktur gemäß IT-Sicherheitsgesetz [ITSichG2015] sind gesondert zu betrachten, da hier eine wiederkehrende Zertifizierung erforderlich ist, die in der Regel ein ISMS nach ISO 27000 voraussetzt.

5. Anhang: Anwendung auf eine Abwasseranlage

Dieser Anhang zeigt exemplarisch die konkrete Anwendung der bisherigen Betrachtungen auf eine Anlage der Abwassertechnik. Hierbei wird zunächst definiert, ob eine Anlage zu einer kritischen Infrastruktur gehört, oder nicht. Anschließend beschreibt das Dokument die in Deutschland anwendbaren Branchenstandards für den Wasser- und Abwasserbereich. Das Kapitel schließt mit einem Vorschlag für das Vorgehen bei der Bewertung einer Abwasseranlage.

5.1. Risikobetrachtung für Abwasseranlagen

In Bezug auf die Bedrohung der IT-Sicherheit von Abwasseranlagen existieren bereits Veröffentlichungen, welche bekannte Vorfälle beschreiben:

- Bereits im Jahr 2000 wird in Australien ein Angriff auf eine Abwasseranlage dokumentiert [SLA2008]. Hier hat ein externer Consultant die ihm bekannten Zugangscodes zu drahtlosen Übertragungssystemen zu Kompromittierung der Anlage missbraucht.
- Im Jahr 2018 beschreiben Sicherheitsforscher, dass sie einen uneingeschränkten Online-Zugang zu Klärwerken mit Administrator-Rechten erlangen konnten [TRE2018].
- Die KRITIS-Sektorstudie des BSI [BSI2015] Vorfälle auf bei den Stadtwerken Lübeck im Jahr 2014, einen Angriff auf die Wasserversorgung der Stadt Haifa in 2013.
- In einem Bericht aus dem Jahr 2020 stellt das Beratungsunternehmen Alpha Strikes Bereich Abwasser und bei der Informationstechnik der Berliner Wasserbetriebe mehr als 30 Schwachstellen fest [JAN2020].
- In [NEU2020] wird festgehalten, dass ein Großteil der Versorgungsunternehmen nur unzureichend geschützt ist.

Zusammenfassend lässt sich festhalten, dass Abwasseranlagen und die zugehörigen Leitzentralen einem Risiko in Bezug auf die IT-Sicherheit ausgesetzt sind. Dies gilt insbesondere dann, wenn Remote-Zugänge für einen externen Zugriff verwendet werden.

Bei den Angriffen auf Abwasseranlagen ist von zwei wesentlichen Angriffsvektoren auszugehen:

- Angriffe von außen:
    - Gezielte Angriffe von außen, z. B. mit dem Ziel die Datenkommunikation zu stören oder in das Netz einzudringen.
    - Zufällige Angriffe von außen, z. B. durch das Scannen von Adressbereichen zum Auffinden von bestimmten Komponenten.
    - Angriff auf Fernwirksysteme.
    - Angriff über Systeme zur Fernwartung oder Fernbedienung der Anlage.
    - Einbruch in die Anlage.

- Angriffe von innen:
    - Öffnen von kompromittierten Anhängen von Mails, Ausbreitung der Schadsoftware ins Automatisierungsnetzwerk.
    - Unaufmerksamkeit oder mangelndes Knowhow von Personal, z. B. beim Einspielen von SW-Updates.
    - Verbinden von Laptops / USB-Sticks von externem Personal mit Komponenten der Anlage.
    - Innentäter, die absichtlich eine Kompromittierung der Anlage herbeiführen möchten.

Beide Angriffsvektoren sind bei einer Risikobetrachtung zu berücksichtigen.

5.2. Kritische Infrastruktur oder nicht?

Das BSI definiert in seinem Glossar eine kritische Dienstleistung wie folgt:

„Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten." [BSI2021a].

Die Erbringung dieser kritischen Dienstleistungen erfolgt über bestimmte Anlagen, wie z. B. Kraftwerke, Wasserwerke, Hafenanlagen oder Flughäfen. Diese Anlagen werden allgemein als kritische Infrastruktur bezeichnet. Das BSI definiert kritische Infrastrukturen wie folgt:

„Kritische Infrastrukturen sind 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 einträten. In Deutschland werden folgende Sektoren (und Branchen) den Kritischen Infrastrukturen zugeordnet:

- *Transport und Verkehr (Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)*
- *Energie (Elektrizität, Mineralöl, Gas)*
- *Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnik)*
- *Finanz- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen)*
- *Staat und Verwaltung (Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall- und Rettungswesen einschließlich Katastrophenschutz)*
- *Ernährung (Ernährungswirtschaft, Lebensmittelhandel)*
- *Wasser (Öffentliche Wasserversorgung, **öffentliche Abwasserbeseitigung**)*
- *Gesundheit (Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore)*
- *Medien und Kultur (Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke)"* [BSI2021a]

Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443

Die BSI KRITIS-Verordnung [BSI-KritisV_2016] definiert die Anlagengröße, ab der eine öffentliche Abwasserbehandlungsanlage zur kritischen Infrastruktur zählt. Dabei wird von folgenden Zahlen ausgegangen:

- Anfallendes Abwasser: 44 m^3 pro versorgte Person pro Jahr und
- Regelschwellenwert: 500.000 versorgten Personen

Daraus ergibt sich

- 44 m^3/Jahr · 500.000 = 22 Mio. m^3/Jahr

Das bedeutet, dass alle Kläranlagen mit einem Durchsatz von 22 Mio. m^3/Jahr oder mehr zur kritischen Infrastruktur zugeordnet werden. Weitere Details zur Berechnung und zur Bewertung zusammenhängender Anlagen finden sich in [BSI-KritisV_2016]. Diese Verordnung wurde im Jahr 2017 aktualisiert [BSI-KritisV_2017]. Die Aktualisierung hat jedoch keinen Einfluss auf die o.g. Grenzwerte. Mit der Verabschiedung des IT-Sicherheitsgesetzes 2.0 [IT-SIG_2.0] ist mit einer Aktualisierung der KRITIS-Verordnung ist mein einer Reduzierung der Schwellenwerte zu rechnen.

Das statistische Bundesamt erfasst in [STA2016] Kläranlagen nach Größe. Allerdings nur bis zu einer Jahresabwassermenge von 6 Mio. m^3/Jahr. Von 9.105 Kläranlagen in Deutschland weisen 276 eine Jahresabwassermenge von 6 Mio. m^3/Jahr und mehr aus. Das entspricht ca. 3% der Anlagen. Hieraus lässt sich ableiten, dass die Anzahl der Kläranlagen, die zur kritischen Infrastruktur zählen noch darunter liegen wird, da der Grenzwert hierfür ja bei 22 Mio. m^3/Jahr liegt. Diese Einschätzung deckt sich mit Zahlen aus der Wasserversorgung. Dort sind zählen lediglich 0,82% der Anlagen zur kritischen Infrastruktur [NEU2020].

Gemäß der [BSI-KritisV_2016], [ITSichG2015] und [BSIG_2020] müssen betroffene kommunale Abwasserentsorger die folgenden Vorgaben erfüllen:

- Der KRITIS-Betreiber hat eine Kontaktstelle einzurichten, über die er jederzeit durch das BSI erreicht werden kann.
- Erhebliche IT-Sicherheitsvorfälle, die zu einem Ausfall oder einer Beeinträchtigung der Beseitigung des Abwassers führen können oder geführt haben, sind an das BSI zu melden. Hierfür unterhält das BSI eine Meldestelle.
- Der KRITIS-Betreiber muss seine IT nach dem Stand der Technik abgesichert haben.
- Der KRITIS-Bertreiber muss dem BSI die Erfüllung des IT Sicherheitsniveaus durch Sicherheitsaudits, Prüfungen oder Zertifizierungen mindestens alle zwei Jahre nachweisen.

Weitere Informationen mit Fragen und Antworten für Betreiber kritischer Infrastrukturen finden sich in [VKU2016] sowie in [BSI2017].

5.3. Anwendbare Normen und Standards für die Wasser- / Abwassertechnik

In diesem Kapitel soll nun die Anwendbarkeit der Normreihen ISO 27000 und IEC 62443 auf Anlagen der Abwasserwirtschaft geprüft werden. Darüber hinaus wird noch ein branchenspezifischer Standard für die Wasser-/Abwasserwirtschaft betrachtet.

5.3.1. Anwendung der Normreihe ISO 27000 auf Abwasseranlagen

Die Normreihe ISO 27000 kann für die Absicherung abwassertechnischer Anlagen herangezogen werden. Hierbei ist insbesondere der Aufbau eines Information-Security-Management-Systems nach [DIN_EN_ISO_27001] zu beachten. Die technischen Anforderungen an die IT-Sicherheit können nach [DIN_EN_ISO_IEC_27002] realisiert werden. Hierbei ist jedoch zu beachten, dass es sich hierbei um generische Anforderungen handelt, die nicht direkt auf Automatisierungssysteme zielen. Die einzige Norm mit einem Bezug zu Automatisierungssystemen ist die [ISO_27019]. Diese Norm zielt auf Energieerzeugungs- und verteilanlagen, kann aber sinngemäß auch für Abwasseranlage herangezogen werden.

Das Whitepaper des BDEW [BDE2018] liefert eine Abbildung der Anforderungen aus der [DIN_EN_ISO_IEC_27002] auf die Komponenten einer Kläranlage.

Betreiber kritischer Infrastrukturen müssen in regelmäßigen Abständen über ein Audit dokumentieren, dass der Stand der Technik in Bezug auf die IT-Sicherheit gegeben ist. Hier kommt in der Regel die Normreihe ISO 27000 oder der in Kapitel 5.3.3 beschriebene branchenspezifische Sicherheitsstandard zum Einsatz.

Für Betreiber kleiner Abwasseranlagen, die nicht zur kritischen Infrastruktur gehören, ist die Anwendung der ISO 27000-Normreihe herausfordernd, da es sich um ein sehr umfassendes Normenwerk handelt.

5.3.2. Anwendung der Normreihe IEC 62443 auf Abwasseranlagen

Die Normreihe IEC 62443 fokussiert auf automatisierungstechnische Systeme. Der Teil [IEC_62443-2-1] beschreibt Anforderungen an ein IT-Sicherheits-Managementsystem. Der Teil [IEC_62443-2-3] betrachtet das Patch-Management, der Teil [DIN_EN_IEC_62443-2-4] befasst sich mit dem Einsatz von Dienstleistern für Inbetriebnahme und Service aus Sicht der IT-Sicherheit. Es ist zu erkennen, dass diese Normreihe stärker auf die Gegebenheiten in einem Produktionsumfeld, wie z. B. einem ununterbrochenen Betrieb, fokussiert.

Der Teil [IEC_62443_3_3] beschreibt konkrete Anforderungen an Automatisierungssysteme in Form von grundlegenden Anforderungen (Foundational Requirements). Diese Foundational Requirements (FR) legen die IT-Sicherheitseckpunkte des Systems fest. Die Teile [DIN_EN_IEC_62443-4-1] und [DIN_EN_IEC_62443-4-2] definieren Anforderungen an die Lieferanten der automatisierungstechnischen Komponenten.

Es lässt sich zusammenfassend feststellen, dass die Normreihe IEC 62443 alle erforderlichen Bestandteile (ISMS, Risikoermittlung, technische Anforderungen and Systeme und Kompo-

nenten) bereitstellt. Betreiber, die im Wesentlichen die Automatisierungsanlage im Fokus haben, können hier zielgerichtet vorgehen, ohne die Komplexität der ISO 27000 Reihe bewältigen zu müssen. Erfahrungsberichte zur Absicherung von Kläranlagen in Verbindung mit der IEC 62443 finden sich z. B. in [CHR2019] und [TEB2020]. Es bleibt allerdings festzuhalten, dass in jedem Fall ein ISMS einzuplanen ist.

5.3.3. Anwendung branchenspezifischer Sicherheitsstandard Wasser/Abwasser (B3S WA)

Das IT-Sicherheitsgesetz [ITSichG2015] definiert in §8a(2):

„Betreiber kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderung nach Absatz 1 zu gewährleisten."

Auf Basis dieser Festlegung entstand der branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA). Er besteht aus den folgenden Teilen:

- Merkblatt IT-Sicherheit Branchenstandard Wasser / Abwasser [DWA-M_1060]
- IT-Sicherheitsleitfaden - Web-Applikation zum Merkblatt DWA-M 1060 [DWA2020]
- Orientierungshilfe zum Nachweisverfahren [DWA2018]

Das Merkblatt [DWA-M_1060] definiert zunächst den Anwendungsbereich und die wesentlichen Begriffe. Danach folgt die Definition der angestrebten Schutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit. Im Einzelnen bedeutet dies laut Merkblatt:

- Ausfälle/Ausfallzeiten der informationstechnischen Systeme, Komponenten oder Prozesse werden vermieden und ein Zugriff auf die relevanten Daten ist jederzeit möglich.
- Die unautorisierte Modifikation der informationstechnischen Systeme, Komponenten oder Prozesse und ihrer Daten wird verhindert.
- Die korrekte Funktion der Systeme und Unversehrtheit der Daten, die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit der Daten und ihrer Herkunft ist gewährleistet.
- Die Informationen sind vor unbefugter Preisgabe geschützt.

In einem nächsten Schritt beschreibt das Merkblatt die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) und die Anforderungen an ein betriebliches Kontinuitätsmanagement. Danach folgt die Beschreibung der Risikoabschätzung mit den Einzelschritten: Risikoidentifikation, Risikoanalyse, Risikobewertung und Verantwortlichkeiten des Betreibers. Der folgende Teil des Merkblattes beschreibt dann die Maßnahmen zur Risikominimierung.

Im das Merkblatt ergänzenden IT-Sicherheitsleitfaden werden anhand von Anwendungsfällen sowohl die Gefährdungen in Bezug auf die IT-Sicherheit als auch die entsprechend zu ergreifenden Maßnahmen für alle betroffenen Anlagentypen laut [BSI-KritisV_2016] im Sektor Was-

ser beschrieben. Die Anwendungsfälle beschreiben die möglichen IT-Systeme/ IT-Konfigurationen und sonstigen Gegebenheiten in Bezug auf die IT-Ausstattung der Anlagen. [DWA-M_1060]. Basis für diese Fälle ist das BSI-Grundschutzkompendium [BSI2021b].

Der branchenspezifische Standard ist sowohl auf Abwasseranlagen der kritischen Infrastruktur als auch auf herkömmliche Abwasseranlage anwendbar. Erfahrungsberichte in der Anwendung des Standards finden sich in [FIE2020] und [TEN2018].

Das BSI hat einen Leitfaden zur Anwendung des Standards [BSI2018] herausgegeben. In diesem Dokument wird insbesondere auf die parallele Nutzung der ISO 27001 und des Branchenstandards eingegangen. Das BSI gibt am Ende des Dokuments eine ausführliche Referenztabelle zum Vergleich der Alternativen.

6. Verzeichnisse

6.1. Abbildungsverzeichnis

6.2. Tabellenverzeichnis

6.3. Literaturverzeichnis

[BDE2018] BDEWBDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf.

[BRE2020] Brenner, Michael; gentschen Felde, Nils; Hommel, Wolfgang Praxisbuch ISO/IEC 27001. Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Carl Hanser Verlag GmbH & Co. KG, München, 2020.

[BSI_200-1] Bundesamt für Sicherheit in der Informationstechnik (BSI) BSI-Standard 200-1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2.

[BSI_2014] Bundesamt für Sicherheit in der Informationstechnik ICS-Security-Kompendium. Testempfehlungen und Anforderungen für Hersteller von Komponenten. Stand 19.11.2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf;jsessionid=DB019AA1A22E666BE17192033909CB6D.2_cid359?__blob=publicationFile, 26.10.2014.

[BSI2013] Bundesamt für Sicherheit in der Informationstechnik ICS-Security-Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile, 05.06.2014.

[BSI2015] Bundesamt für Sicherheit in der Informationstechnik (BSI) KRITIS-Sektorstudie Ernährung und Wasser. https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_Ernaehrung_Wasser.pdf?__blob=publicationFile.

[BSI2017] Bundesamt für Sicherheit in der Informationstechnik (BSI) Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf;jsessionid=E0CD6CAD7BAE814DD7140BE30ED859D5.internet081?__blob=publicationFile&v=1.

[BSI2018] Bundesamt für Sicherheit in der Informationstechnik (BSI) Nutzung des branchenspezifischen Sicherheitsstandards Wasser/Abwasser (B3S WA) in Verbundunternehmen. Ausgangssituation – Analyse – Empfehlungen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/B3S_WA_Analyse_Empfehlungen_pdf.pdf?__blob=publicationFile&v=3.

[BSI2021a] Bundesamt für Sicherheit in der Informationstechnik (BSI) Schutz Kritischer Infrastrukturen. Glossar. https://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/glossar_node.html;jsessionid=CA30D56F33392F5444A3F945140B4B85.1_cid345.

[BSI2021b] Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6.

[BSIG_2020] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik. BSI-Gesetz-BSIG, 2020.

[BSI-KritisV_2016] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung). BSI-KritisV, 2016.

[BSI-KritisV_2017] Erste Verordnung zur Änderung der BSI-Kritisverordnung. BSI Kritis Vo, 2017.

[CHR2019] Christ, Jochen Cybersecurity für die Wasserwirtschaft: Schützen, was wichtig ist. In Automation Blue, 2, 2019; S. 56–59.

[DIN_EN_62443-3-2] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V, DIN EN 62443-3-2 (VDE 0802-3-2) Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 65/690/CDV:2018); Deutsche und Englische Fassung prEN 62443-3-2:2018. Beuth Verlag, 2018.

[DIN_EN_IEC_62443-2-4] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-2-4 (VDE 0802-2-4):2020-07 Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2015 + Cor.:2015 + A1:2017); Deutsche Fassung EN IEC 62443-2-4:2019 + A1:2019.

[DIN_EN_IEC_62443-4-1] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V, DIN EN IEC 62443-4-1 (VDE 0802-4-1) IT -Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1 2018); Deutsche Fassung EN IEC 62443-4-1 2018. Beuth Verlag, Berlin, 2018.

[DIN_EN_IEC_62443-4-2] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN EN IEC 62443-4-2 IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS) (IEC 62443-4-2:2019); Deutsche Fassung EN IEC 62443-4-2:2019, 2019.

[DIN_EN_ISO_27000] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN EN ISO/IEC 27000:2020 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020, 2020.

[DIN_EN_ISO_27001] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN ISO/IEC 27001:2017 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013

einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017, 2017.

[DIN_EN_ISO_IEC_27002] DIN Deutsches Institut für Normung e. V, DIN ISO/IEC 27002:2017 Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017, 2017.

[DIN_IEC_27019] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN ISO/IEC TR 27019 DIN SPEC 27019 Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014). Beuth Verlag, Berlin, 2015.

[DKE2017] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE Deutsche Normungsroadmap IT-Sicherheit. Version 3. https://www.din.de/resource/blob/238492/39d3f201a42007061c8013c0b76cf530/deutsche-normungs-roadmap-it-sicherheit-version-3-0-data.pdf.

[DKE2020] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE EC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung. https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung.

[DIN_IEC_62443-3-3] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN IEC 62443-3-3 (VDE 0802-3-3) Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme- Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + Cor.:2014). Beuth Verlag, 2015.

[DWA2018] DWA Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. Branchenspezifischer Sicherheitsstandard Wasser/Abwasser (B3S WA) – Hinweise zum Nachweisverfahren gemäß § 8a (3) BSIG. https://de.dwa.de/files/_media/content/05_PUBLIKATIONEN/DWA-Regelwerk/Arbeitshilfen%20aus%20dem%20DWA-Regelwerk/Branchenspezifischer_Sicherheitsstandard_Wasser_Abwasser.pdf.

[DWA2020] DWA Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. IT-Sicherheitsleitfaden (Version 2.0 - 2020) Web-Applikation zum Merkblatt DWA-M 1060. https://de.dwa.de/de/it-sicherheitsleitfaden.html.

[DWA-M_1060] DWA Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V., DWA-M 1060 Merkblatt IT-Sicherheit Branchenstandard Wasser / Abwasser, 2017.

[ENI2017] ENISA European Union Agency for Network and Information Security Mapping of OES Security Requirements to Specific Sectors. https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/.

[FIE2020] Fiene, Hans-Jürgen Fachbericht: Umsetzung des B3S-Sicherheitsstandards im Klärwerk Langwiese. In Automation Blue, 4, 2020.

[FLA2019] Flaus, Jean-Marie Cybersecurity of industrial systems. ISTE Ltd, London, UK, 2019.

[FRI2019] Fries, Steffen Cybersecurity in Industrial Environments -From requirements to solutions on the example of Digital Grid. http://www.iaria.org/conferences2019/filesSECURWARE19/SteffenFries_Tutorial_SECURWARE.pdf.

[GAR2021] Gartner Inc. Gartner Glossary Information Technology. https://www.gartner.com/en/information-technology/glossary.

[GUN2018] Gunter, David G.; Medoff, Michael D.; O'Brien, Patrick C. Implementing IEC 62443. A pragmatic approach to cybersecurity. Exida, Sellersville, PA, 2018.

[IEC_62443-1-1] IEC- International Electrotechnical Commission, IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.

[IEC_62443-1-2] IEC- International Electrotechnical Commission, ISA-TR62443-1-2 Security for industrial automation and control systems - Master Glossary.

[IEC_62443-1-3] IEC- International Electrotechnical Commission, IEC/TS 62443-1-3 Security for industrial process measurement and control – Network and system security – Part 1-3: System security compliance metrics, 2014.

[IEC_62443-1-4] IEC- International Electrotechnical Commission, ISA-62443-1-4 Security for industrial automation and control systems Life Cycle and Use Cases, 2013.

[IEC_62443-2-1] IEC- International Electrotechnical Commission, IEC 62443-2-1-2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, 2010.

[IEC_62443-2-3] IEC- International Electrotechnical Commission, IEC TR 62443-2-3:2015 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment, 2015.

[IEC_62443-2-4] IEC- International Electrotechnical Commission, IEC 62443-2-4 Security for industrial automation and control systems – Network and system security – Part 2-4: Requirements for IACS solution suppliers., 2014.

[IEC_62443-2-5] IEC- International Electrotechnical Commission, IEC 62443-2-5 Implementation guidedance for IACS asset owners, not released.

[ISA_62443-2-2] ISA - The International Society of Automation, ISA-62443-2-2 Security for industrial automation and control systems - Part 2-2: IACS security program rating, 2020.

[ISA2020] ISA - The International Society of Automation ISA99, Industrial Automation and Control Systems Security. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99.

[ISE2020] IsecT Ltd Overwiew on ISO 27000 standard series. https://www.iso27001security.com/html/iso27000.html.

[ISO_27000] ISO - International Standardization Organization, ISO/IEC 27000:2018(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018.

[ISO_27003] ISO - International Standardization Organization, ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance, 2017.

[ISO_27004] ISO - International Standardization Organization, ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation, 2016.

[ISO_27005] ISO - International Standardization Organization, ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018.

[ISO_27006] ISO - International Standardization Organization, ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems, 2015.

[ISO_27007] ISO - International Standardization Organization, ISO/IEC 27007:2020 nformation security, cybersecurity and privacy protection — Guidelines for information security management systems auditing, 2020.

[ISO_27019] ISO - International Standardization Organization, ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry, 2017.

[ITSichG2015] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015.

[IT-SIG_2.0] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). IT-SiG 2.0: Bundesgesetzblatt, 2021; S. 1122–1138.

[JAN2020] Jansen, Frank; Fiedler, Maria Wasserbetriebe gegen Hackerangriffe mangelhaft geschützt. https://www.tagesspiegel.de/politik/gutachten-warnt-vor-zusammenbruch-wasserbetriebe-gegen-hackerangriffe-mangelhaft-geschuetzt/26045264.html.

[KER2020] Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Springer Fachmedien Wiesbaden, Wiesbaden, 2020.

[KLI2015] Klipper, Sebastian Information Security Risk Management. Risikomanagement mit ISO/IEC 27001, 27005 und 31010. Springer Vieweg, Wiesbaden, 2015.

[KOB2021] Kobes, Pierre Leitfaden Industrial Security. IEC 62443 einfach erklärt. VDE Verlag, Berlin, 2021.

[KOH2018] Kohl, Andreas; Bisale, Chaitanya Effektive und effiziente Security auf Basis internationaler Standards. In np, 9, 2018; S. 12–14.

[KRO2017] Kroeselberg, Dirk, Buchi, Frederic; Meulenbroek, Hans Cyber Security Tutorial Energy Automation and IEC 62443. https://www.pcic-library.com/sites/default/files/final/EUR17_63.pdf.

[MON2019] Montes Protela, Carlos; Hoeve, Maarten; Tan, Fook Hwa; Slootweg, Han Implementing an ISA/IEC-62443 and ISO/IEC-27001 OT Cyber Security Managment System at Dutsch DSO Enexis: 25th International Conference on Electricity Distribution. Madrid, 3-6 June 2019. [CIRED], [Liège, Belgium], 2019; S. 1–5.

[NEU2020] Neuerer, Dietmar Cyberattacken: Großteil der Wasserversorger nur unzureichend geschützt. https://www.handelsblatt.com/politik/deutschland/sicherheit-der-wasserversorgung-cyberattacken-grossteil-der-wasserversorger-nur-unzureichend-geschuetzt/26219428.html?ticket=ST-1111967-HqtoAWo6kfuH5auW4Xb5-ap6.

[NIE2017] Niemann, Karl-Heinz IT-Sicherheit in Produktionsanlagen. Eine Einführung für kleine und mittlere Unternehmen. https://doi.org/10.25968/opus-1135.

[NIE2018] Niemann, Karl-Heinz Organisation der IT Sicherheit in der Produktion. In zehn Schritten zur sicheren Produktionsanlage. In atp Magazin, 11-12, 2018; S. 80–89.

[SLA2008] Slay, Jill; Miller, Michael Lessons Learned from the Maroochy Water Breach. In (Goetz, E.; Shenoi, Sujeet Hrsg.): Critical infrastructure protection. Springer, New York, NY, 2008; S. 73–82.

[STA2016] Statistisches Bundesamt Öffentliche Wasserversorgung und öffentliche Abwasserentsorgung - Öffentliche Abwasserbehandlung und -entsorgung -. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Umwelt/Wasserwirtschaft/Publikationen/Downloads-Wasserwirtschaft/abwasser-oeffentlich-2190212169004.pdf?__blob=publicationFile.

[TEB2020] Tebbe, Christopher Mit IT-Sicherheitsanalysen immer auf dem aktuellen Stand!: Digitalisierung erfolgreich umgesetzt. Schriftenreihe des Mittelstand 4.0-Kompetenzzentrums Hannover, Hannover, 2020; S. 14–22.

[TEN2018] Tenhart, Ludger B3S WA: Eignung festgestellt, in der Praxis angekommen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_2018/B3S_WA_Eignung_feststellen_in_der_Praxis_angekommen.pdf?__blob=publicationFile&v=1.

[TRE2018] Tremmel, Moritz Per Weblogin ins Klärwerk. https://www.golem.de/news/schwachstellen-aufgedeckt-per-weblogin-ins-klaerwerk-1812-138363.html.

[VDM2016] VDMA - Verband der Maschinen und Anlagenbauer e. V. Leitfaden Security für den Maschinen- und Anlagenbau Der Weg durch die IEC 62443. http://pks.vdma.org/documents/105969/15311113/1479910314521_INS%20Security-Leitfaden%20VDMA_v1.0_WEB.pdf/b615dd92-3b84-4e93-afb6-23f54fead723.

[VDS_10000] VdS Schadenverhütung GmbH, VdS 10000:2018-12(02) Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), 2018.

[VDS_10020] VdS Schadenverhütung GmbH, VdS 10020:2018-01(01) Cyber Security für kleine und mittlere Unternehmen (KMU) - Leitfaden zur Interpretation und Umsetzung der VdS 3473 für Industrielle Automatisierungssysteme, Köln, 2018.

[VKU2016] Verband kommunaler Unternehmen e. V. Fragen und Antworten zur IT-Sicherheitsgesetzgebung Wasser / Abwasser. https://digital.vku.de/fileadmin/user_upload/vku_faq_it-sicherheit_wasser_abwasser.pdf.

[WAL2020] Waldeck, Boris Zertifizierter Entwicklungsprozess nach 62443-4-1 – Security by design, Online Seminar, Lemgo, 2020.

[ZVE2017] ZVEI - Zentralverband Elektrotechnik und Elektronikindustrie e. V. Orientierungsleitfaden für Hersteller zur IEC 62443. https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Orientierungsleitfaden_fuer_Hersteller_IEC_62443/Orientierungsleitfaden_fuer_Hersteller_IEC_62443.pdf.