OT-Security für Produktionsanlagen mit PROFINET

Eine Einordnung der IEC 62443 für Betreiber, Integratoren und Hersteller

Whitepaper

für PROFINET

Version 0.20 – Date Februar 2022

Order No.: 7.341

File name : IEC_62443_ Einführung_7341_V020_Feb22

Prepared by the PROFIBUS Working Group PG10 “Security” in the Technical Committee CB.

In this specification the following key words (in **bold** text) will be used:

may:	indicates flexibility of choice with no implied preference.
should:	indicates flexibility of choice with a strongly preferred implementation.
shall:	indicates a mandatory requirement. Designers **shall** implement such mandatory requirements to ensure interoperability and to claim conformance with this specification.

Publisher:
PROFIBUS Nutzerorganisation e.V.
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany
Phone : +49 721 986197 0
Fax: +49 721 986197 11
E-mail: info@profibus.com
Web site: www.profibus.com

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Versionshistorie

Version	Autor	Datum	Änderungshistorie
0.6	Niemann	13.09.2021	Erste Version mit Content
0.7	Niemann	15.09.2021	Weiterer Content ergänzt
0.9	Niemann	08.10.2021	Kommentare X. Schmidt bearbeitet und Inhalt vervollständigt
0.11	Niemann	10.10.2021	Glossar und Index erstellt
0.13	Niemann	12.10.2021	Version für WG Review
0.14	Niemann	01.11.2021	Kommentare E+H integriert und bearbeitet, Zuordnung Security Level bearbeitet. Review Kommentare Siemens bearbeitet
0.15	Niemann	12.12.2021	Review Kommentare Siemens bearbeitet, Safety-Teil gestrichen
0.16	Niemann	16.12.2021	Nach WG Review. Alle Änderungen eingearbeitet. WG-Review abgeschlossen.
0.17	Niemann	06.01.2022	Angleichung von de und en Version
0.18	Niemann	18.02.2022	Einarbeiten von Kommentaren aus WG-Review
0.19	Niemann	24.02.2022	Review Kommentare WG Sitzung eingearbeitet
0.20	Niemann	24.02.2022	Finalisierung. Version für Beiratsreview

1 Management Summary – Scope des Dokumentes

Die Sicherstellung der OT-Security in Produktionsanlagen erfordert das Zusammenspiel verschiedener Akteure im OT-Sicherheitsprozess. PROFIBUS & PROFINET International (PI) ist einer dieser Akteure. PI definiert z. B. Eigenschaften des PROFINET-Protokolls und gibt Vorgaben in Bezug auf die Planung und Errichtung von PROFINET-Systemen. In einem zunehmenden Maße fragen Anwender nach einer Einordnung des PROFINET-Systems in den OT-Security-Prozess und nach einer Einordnung von PROFINET in die Anforderungen einschlägiger OT-Security-Normen, wie z. B. der Normreihe IEC 62443.

Dieses Whitepaper gibt zunächst einen Überblick über die verschiedenen Teile der Normreihe IEC 62443 und beschreibt kurz deren Inhalte. Danach folgt eine Zuordnung der Normteile zu den Akteuren im OT-Security-Prozess. Im Bereich der Operational Technology (OT) sind dies die Betreiber, die Systemintegratoren und die Produktlieferanten.

Aufbauend auf diesen Vorbetrachtungen folgt eine Einordnung von PROFINET. Dargestellt wird die Rolle, die PROFIBUS & PROFINET International (PI) und die Hersteller von PROFINET-Produkten im OT-Security-Prozess spielen. Darüber hinaus wird beschrieben, wie Betreiber durch die Bereitstellung von Informationen im OT-Security-Prozess unterstützt werden.

2 Verwandte Dokumente und Referenzen

Das folgende Kapitel 2.1 listet zunächst PI-Dokumente, die in Bezug zu diesem Dokument stehen und die weiterreichende Information liefern können, auf. Das Kapitel 2.2 gibt die zitierten Normen und sonstige Quellen wieder.

2.1 Verwandte Dokumente

PROFIBUS Nutzerorganisation e. V. PROFINET IO Security Level 1 (Netload). Guideline for PROFINET. https://www.profibus.com/download/profinet-security-level-1-netload/. Order Nr. 7.302, 2017.

PROFIBUS Nutzerorganisation e.V. PROFINET Security Richtlinie. Richtlinie für PROFINET. http://www.profibus.com/nc/download/specifications-standards/downloads/profinet-security-guideline/display/. Order Nr. 7.001, 2014.

PROFIBUS Nutzerorganisation e.V. Security Class 1 for PROFINET-Security. Guideline for PROFINET. https://www.profibus.com/download/profinet-security-guideline. Order Nr. 7.312, 2020.

PROFIBUS Nutzerorganisation e.V. Security Erweiterungen für PROFINET - PI White Paper für PROFINET. https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/. Ohne Order Nr., 2019.

2.2 Referenzen / Normen

[AKE2009] Akerberg, Johan; Björkman, Mats: Exploring Network Security in PROFIsafe. In (Buth, B.; Rabe, G.; Seyfarth, T. Hrsg.): Computer Safety, Reliability, and Security: 28th International Conference, SAFECOMP 2009, Hamburg, Germany, September 15-18, 2009. Proceedings. Springer, 2009; S. 67–80.

[BSI2021] Bundesamt für Sicherheit in der Informationstechnik (BSI): Glossar der Cyber-Sicherheit. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/glossar-der-cyber-sicherheit_node.html.

[CYB2020] US-CERT: Cybersecurity & Infrastructure Security Agency Ransomware Impacting Pipeline Operations Alert (AA20-049A). https://www.us-cert.gov/ncas/alerts/aa20-049a.

[DHS2016] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[DIN_EN_IEC_62443-3-2] VDE 0802-3-2:2021-12. IT-Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung, 2021. (IEC 62443-3-2:2020); Deutsche Fassung EN IEC 62443-3-2:2020.

[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_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.

[DKE2020] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE: IEC 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 EN IEC 62443-3-3:2020-01 VDE 0802-3-3:2020-01 Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + COR1:2014); Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019.

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

[HOR2019] Horch, Alexander, Hannen, Heinrich-Theodor, Ditting, Stefan, Schween, Heiko: Verschlüsselung sicherer Kommunikation- Ein Widerspruch. In atp Magazin, 6-7, 2019; S. 93–99.

[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_62443-2-5] IEC- International Electrotechnical Commission: IEC 62443-2-5 Implementation guidedance for IACS asset owners, not released.

[IEC_62443-3-1] IEC- International Electrotechnical Commission: ISA 62443-3-1 Technical Report Security Technologies for Industrial Automation and Control Systems, Rev. 2, 2007.

[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.

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

[NIE2021] Niemann, Karl-Heinz: Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443 - Eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie. Hochschule Hannover, Hannover, 2021.

[PNO2010] PROFIBUS Nutzerorganisation e.V.: Overview and guidance for PROFINET specifications. Technical Specification for PROFINET. Order No. 2.702. https://de.profibus.com/downloads/profinet-specification/.

[PNO2013] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Richtlinie. Order No. 7.001. 2013. https://de.profibus.com/downloads/profinet-security-guideline.

[PNO2017a] Profibus Nutzerorganisation e. V.: PROFINET IO Security Level 1 (Netload). Guideline for PROFINET. Order No.: 7.302. 2017. https://www.profibus.com/download/profinet-security-level-1-netload/.

[PNO2017b] Profibus Nutzerorganisation e. V.: Test Specification PROFINET IO Security Level 1. Technical Specification for PROFINET. https://www.profibus.com/download/profinet-security-level-1-netload/.

[PNO2018] PROFIBUS Nutzerorganisation e.V.: Security Extensions for PROFINET - PI White Paper for PROFINET. https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/.

[PNO2020] PROFIBUS Nutzerorganisation e.V.: Security Class 1 for PROFINET-Security. Guideline for PROFINET. Order No.: 7.312. 2020. https://www.profibus.com/download/profinet-security-guideline.

[PNO2021a] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO Version 2.4 MU3 – Oct 2021. Order No.: 2.722. https://www.profibus.com/download/profinet-specification. (Dient als Draft für nächste Release der IEC 61158-6-10)

[PNO2021b] PROFIBUS Nutzerorganisation e.V. Application Layer services for decentralized periphery. Technical Specification for PROFINET. Version 2.4 MU3 – Order No.: 2.712, Oct. 2021. https://www.profibus.com/download/profinet-specification. (Dient als Draft für nächste Release der IEC 61158-5-10)

[SAN2020] SANS Institute Glossary of Security Terms. https://www.sans.org/security-resources/glossary-of-terms/.

[VDI_2182_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA): VDI/VDE 2182 Blatt 1 Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Beuth Verlag, Berlin, 2020.

[VDI_2182_4] VDI/VDE Gesellschaft Mess- und Automatisierungstechnik, VDI/VDE 2182 Blatt 4: Informationssicherheit in der industriellen Automatisierung Empfehlungen zur Umsetzung von Security-Eigenschaften für Komponenten, Systeme und Anlagen, 2018.

[VDM2021] VDMA - Verband der Maschinen und Anlagenbauer e. V.: Leitfaden IEC 62443 für den Maschinen- und Anlagenbau. Überarbeite Ausgabe 2021. https://www.vdmashop.de/Informatik-und-Technik/Leitfaden-IEC-62443-fuer-den-Maschinen--und-Anlagenbau---Ueberarbeitete-Ausgabe-2021---PDF-Download.html

[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.

2.3 Disclaimer

Die PROFIBUS Nutzerorganisation e.V. (nachfolgend „PNO“) hat in diesem Dokument Informationen mit größtmöglicher Sorgfalt eingebracht und diese zusammengestellt. Dennoch ist dieses Dokument, basierend auf dem jetzigen Kenntnisstand, nur informierend und wird auf Basis eines Haftungsausschlusses zur Verfügung gestellt. Das Dokument kann in der Zukunft Änderungen, Erweiterungen oder Korrekturen unterliegen, ohne dass ausdrücklich darauf hingewiesen wird.

Dieses Dokument hat keinen normativen Charakter. Es kann in bestimmten Einsatzumgebungen, in bestimmten technischen Konstellationen oder beim Einsatz in bestimmten Ländern sinnvoll sein, von den gegebenen Handlungsempfehlungen abzuweichen. Errichter und Betreiber der Anlage sollten in diesem Fall die Vor- und Nachteile der gemachten Empfehlungen in der konkreten Anwendung abwägen und, sofern als sinnvoll erachtet, gegebenenfalls die Umsetzung einer abweichenden Lösung beschließen.

Der Nutzer darf die Informationen zu keiner Zeit an Dritte vertrieben, vermieten oder in sonstiger Weise überlassen.

Eine Haftung der PNO für Sach- und Rechtsmängel der bereitgestellten Informationen, insbesondere für deren Richtigkeit, Fehlerfreiheit, Freiheit von Schutz- und Urheberrechten Dritter, Vollständigkeit und/oder Verwendbarkeit – außer bei Vorsatz, grober Fahrlässigkeit oder Arglist

– ausgeschlossen. Im Übrigen ist jegliche Haftung der PNO ausgeschlossen, soweit nicht z. B. wegen Verletzung des Lebens, des Körpers oder Gesundheit, wegen Vorsatzes oder grober Fahrlässigkeit oder wegen der Verletzung wesentlicher Vertragspflichten zwingend gehaftet wird.

3 Definitionen und Abkürzungen

Die beiden folgenden Kapitel definieren die verwendeten Begriffe und Abkürzungen. Zuvor sollen einige Begriffe im Bereich der Informationssicherheit abgegrenzt werden.

Abbildung 1: Abgrenzung genutzter Begriffe

Grundsätzlich wird allgemein von der Informationssicherheit gesprochen, so wie z. B. in der [DIN_EN_ISO_27001], wenn es allgemein um den Schutz von Informationen geht. Die Norm spricht hier z. B. von einem „Informationssicherheitsmanagementsystem“. Neben dieser allgemeinen Beschreibung haben sich in der Literatur alternative Begriffe, wie z. B. IT-Security und IT-Sicherheit etabliert. Die Verwendung dieser Begriffe impliziert, dass hier Anwendungen in einem herkömmlichen IT-Umfeld und keine Produktionsanlagen betrachtet werden. Abbildung 1 zeigt die gängigsten Begriffe, die im Bereich der Informationssicherheit verwendet werden. Die Informationssicherheit im Bereich von Produktionsanlagen oder vergleichbaren Systemen stellt zusätzliche Anforderungen, z. B. in Bezug auf die Verfügbarkeit der Automatisierungssysteme. Um dieses Anwendungsumfeld mit seinen zusätzlichen Anforderungen zu kennzeichnen, werden hierfür Begriffe die OT-Security (OT=Operational Technology) oder ICS-Security (ICS=Industrial Control System) verwendet. Der Begriff Cyber-Security wird oft generell verwendet und findet sich sowohl im IT- als auch im OT-Bereich. Der Schutz von personenbezogenen Daten, (Datenschutz) wird nicht näher beleuchtet.

Dieses Whitepaper fokussiert auf Produktionsanlagen. Daher wird im Folgenden der Begriff OT-Security verwendet, wenn die Informationssicherheit von Produktionsanlagen gemeint ist. Die Informationssicherheit von Office-Systemen wird mit dem Begriff IT-Security bezeichnet.

3.1 Definitionen

Tabelle 1 zeigt eine Liste der verwendeten Fachbegriffe. Die Begriffsdefinitionen wurden zum Teil aus [SAN2020] und [IEC_62443-1-1] übernommen.

Tabelle 1: Liste der verwendeten Begriffe

Begriff	Beschreibung
Angriff	Anschlag auf ein System, der auf eine intelligente Bedrohung zurückgeht
Authentizität	Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die

Begriff	Beschreibung
	Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen. [BSI2021]
Authentifizierung	Unter Authentifizierung versteht man den Prozess der Bestätigung der Richtigkeit der behaupteten Identität. Ein Authentifizierungsprozess kann sowohl Menschen als auch Geräte betreffen.
Automatisierungssystem	System zur Überwachung, Steuerung und/oder Regelung eines technischen Prozesses.
Betreiber	Besitzer der Assets einer Produktionsanlage, der in der Regel auch diese Produktionsanlage betreibt.
Conduit	Logische Gruppierung von Kommunikationskanälen zur Verbindung von zwei oder mehr Zonen, die gemeinsame Sicherheitsanforderungen haben. -> Siehe Zone
Cyber Security	Allgemeiner Begriff für die Informationssicherheit. Wird häufig sowohl im OT- als auch im IT-Bereich verwendet.
Datenschutz	Schutz personenbezogener Daten.
Datensicherheit	Siehe Datenschutz.
Firewall	Eine logische oder physische Unterbrechung in einem Netzwerk, um den unbefugten Zugriff auf Daten oder Ressourcen zu verhindern.
ICS-Security	Siehe OT-Security.
Informationssicherheit	Informationssicherheit hat den Schutz von Informationen als Ziel. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein. [BSI2021]
Information Security	Siehe Informationssicherheit
Information Technology (IT)	Beschreibt in diesem Dokument informationsverarbeitende Systeme, die in der Regel nicht zur Steuerung technischer Prozesse verwendet werden. Der Begriff wird in Abgrenzung zur Operational Technology (OT) genutzt, um z. B. Anwendungen im Bürobereich zu kennzeichnen. -> Siehe auch Operational Technology.
Innentäter	Angreifer, der zu der Organisation gehört, die er angreift.
Integrität	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass

Begriff	Beschreibung
	diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. [BSI2021]
Intrusion Detection System	Ein Sicherheitsmanagementsystem für Computer und Netzwerke. Ein IDS sammelt und analysiert Informationen aus verschiedenen Bereichen eines Computers oder eines Netzwerks, um mögliche Sicherheitsverletzungen zu erkennen, zu denen sowohl Eindringlinge (Angriffe von außerhalb des Unternehmens) als auch Missbrauch (Angriffe innerhalb des Unternehmens) gehören.
IT	Siehe Information Technology.
IT-Sicherheit	Siehe IT-Security.
IT-Security	In diesem Dokument verwendeter Begriff um die Informationssicherheit für IT-Systeme zu beschreiben. Hierbei stehen Anforderungen einer Büroumgebung im Vordergrund. Der Begriff wird in Abgrenzung zur OT-Security verwendet.-> Siehe OT-Security. Bei der OT-Security werden Anforderungen der Informationssicherheit für Produktionsanlagen betrachtet. Da eine Produktionsumgebung höhere Anforderungen stellt, wird daher zwischen IT-Security und OT-Security unterschieden.
Komponentenhersteller	In diesem Dokument der Hersteller einer Komponente eines Automatisierungssystems (z. B. Frequenzumrichter), jedoch ohne die Rolle ein ganzes Automatisierungssystem herzustellen. Abgrenzung zum Begriff Systemhersteller. -> Siehe Systemhersteller.
Kritische Infrastruktur	Anlagen oder Systeme, die für die Versorgung der Bevölkerung eine wichtige Rolle spielen. Typische Vertreter sind z. B. Wasserwerke, Kraftwerke, Kläranlagen ab einer bestimmten Größe.
Maturity Level	Reifegrad einer Organisation in Bezug auf die Erfüllung von Anforderungen.
Office-System	Siehe Information-Technology.
Operational Technology (OT), **Operationelle Technologie**	Technologie, die zum Überwachen, Steuern und/oder Regeln von technischen Prozessen verwendet wird. Der Begriff wird in Abgrenzung zur Information-Technology verwendet. -> Siehe IT
OT	Siehe Operational Technology.
OT-Security	In diesem Dokument verwendeter Begriff, um die Informationssicherheit für technische Systeme, wie z. B. Automatisierungssysteme zu beschreiben. Der Begriff wird in Abgrenzung zur IT-Security verwendet. -> Siehe IT-Security. Hierbei stehen Anforderungen einer Produktionsumgebung im Vordergrund. Da eine Produktionsumgebung höhere Anforderungen stellt, wird zwischen IT-Security und OT-Security unterschieden.
OT-Security-Norm(en)	Normen, die sich auf die Informationssicherheit technischer Systeme beziehen. Hier ist die IEC 62443 Normreihe relevant.

Begriff	Beschreibung
OT-Security-Prozess	Sicherheitsprozess für technische Systeme, wie z. B. Automatisierungssysteme.
Patch	Softwarepaket zur Korrektur eines oder mehrerer Fehler in einer Software.
Produktlieferant	Siehe Komponentenhersteller.
Produktionsanlage	Anlage zur Herstellung von Gütern.
PROFINET-System	Kommunikationssystem auf Basis des PROFINET Protokolls.
Risikobewertung	Prozess, der systematisch potenzielle Schwachstellen in Bezug auf überprüfbare Systemressourcen und Bedrohungen für diese Ressourcen identifiziert, Schadensrisiken und Konsequenzen auf der Grundlage der Eintrittswahrscheinlichkeit quantifiziert und (optional) empfiehlt, wie Ressourcen für Gegenmaßnahmen zugewiesen werden können, um die Risiken zu minimieren.
Safety-System	Bezeichnung für ein System, welches Anforderungen in Bezug auf die funktionale Sicherheit erfüllt.
Security by Design	Entwicklungsprozess bei dem der Aspekt der Informationssicherheit im Entwicklungsprozess verankert ist.
Security Level	Definition nach [DIN_IEC_62443-3-3]. Ein Maß an Vertrauen, dass das Automatisierungssystem oder eine Komponente davon frei von Schwachstellen ist und in der vorgesehenen Weise funktioniert.
Systemhersteller	In diesem Dokument: Hersteller, der ein komplettes Automatisierungssystem liefern kann. Dieses besteht z. B. aus Steuerungen, Remote IO, Switches, Engineering-Station, Bedien- und Beobachtungsstation, etc.
Systemintegrator	Person oder Unternehmen, welches im Auftrag des Betreibers Produktionsanlagen oder Teile davon plant und in Betrieb nimmt.
Technologielieferant	Person oder Unternehmen, welches Hardware- oder Software-Komponenten an Produkt- und Systemlieferanten liefert, die diese dann in ihre Produkte oder Systeme integrieren. Beispiel für einen Technologielieferanten wäre z. B. der Hersteller eines Protokollstacks für PROFINET.
Verschlüsselung	Kryptografisches Verfahren, das einen Klartext in einen Chipher-Text mit dem Ziel übersetzt, den Original-Inhalt für Außenstehende unzugänglich zu machen.
Zellenschutzkonzept	Konzept zum Schutz, das eine Segmentierung und gegenseitige Abschottung von Kommunikationssystemen vorsieht.
Zone	Sammlung von Einheiten, die eine Partitionierung eines Systems unter Berücksichtigung ihrer funktionalen, logischen und physischen Beziehung darstellen.

3.2 Abkürzungen

Tabelle 2 beschreibt die im Dokument verwendeten Abkürzungen.

Tabelle 2: Liste der Abkürzungen

Abkürzung	Beschreibung
IT	Beschreibt in diesem Dokument informationsverarbeitende Systeme, die in der Regel nicht zur Steuerung technischer Prozesse verwendet werden. Der Begriff wird in Abgrenzung zur Operational Technology (OT) verwendet.
OT	Technologie, die zum Überwachen, Steuern und/oder Regeln von technischen Prozessen verwendet wird. Dies geschieht in Abgrenzung zur Information-Technology, die eher Büroanwendungen zugeordnet wird.

4 Einführung in die OT-Security für Produktionsanlagen

Die Betreiber von Produktionsanlagen sind zunehmend gefordert, die OT-Security ihrer Produktionsanlagen sicherzustellen. Spektakuläre Angriffe auf kritische Infrastrukturen, z. B. auf eine Ölpipeline in den U.S.A. [CYB2020] belegen eindrucksvoll, dass die Automatisierungstechnik, die sogenannte Operational Technology (OT), wachsenden Bedrohungen ausgesetzt ist. PROFIBUS & PROFINET International (PI) hat diesem Aspekt bereits im Jahr 2013 durch Herausgabe einer Richtlinie zum sicheren Betrieb von PROFINET-Netzwerken [PNO2013] Rechnung getragen. Diese Richtlinie beschreibt die Segmentierung und den Zellenschutz von PROFINET-Netzwerken, um einen sicheren Betrieb und einen Schutz gegen Angriffe von außen zu gewährleisten. Das in der Richtlinie realisierte Zellenschutzkonzept liefert jedoch keinen Schutz gegen Innentäter. Man geht davon aus, dass diese den Perimeter-Schutz überwinden können und so Zugang zum abgeschotteten Netzwerkbereich erlangen. Um zusätzlich einen Schutz gegen Innentäter realisieren zu können, arbeitet PROFIBUS & PROFINET International (PI) an einem weiterreichenden Konzept, welches einen Schutz der Kommunikation durch kryptografische Prüfsummen (kryptografische Hashes) vorsieht, ggf. durch eine Verschlüsselung ergänzt. Dieses weiterreichende Konzept ist in [PNO2018] beschrieben. Eine Abbildung auf die PROFINET Spezifikation liegt in [PNO2021a] und [PNO2021b] ebenfalls vor.

Betreiber von Produktionsanlagen sollten den Schutzbedarf ihrer Anlage ermitteln und auf diesen Schutzbedarf angepasste Maßnahmen vornehmen. Hierbei ist festzulegen, ob das Zellenschutzkonzept oder ein erweiterter Schutz durch kryptografisch abgesicherte Protokolle benötigt wird.

Die Informationssicherheit ist in einem Unternehmen ganzheitlich zu beurteilen. Hierbei sind sowohl die Systeme der kommerziellen Datenverarbeitung (IT), als auch die Systeme aus dem Produktionsbereich (OT) zu betrachten. IT und OT sind, wie in Tabelle 3 dargestellt, zu unterscheiden. PROFIBUS & PROFINET International ist mit seinen Aktivitäten in der Hauptsache der OT zuzuordnen.

Tabelle 3: Abgrenzung IT und OT

Domäne	Definition nach Gartner Group [GAR2021]	Anwendungsbeispiele
IT	Information Technology (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.	• Arbeitsplatzrechner • Laptops • Webserver • Mail-Server • SAP-Systeme • File Server • Netzwerke
OT	Operational Technology (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

Obwohl die grundlegenden Anforderungen von IT und OT in Bezug auf die Informationssicherheit ähnlich sind, erfordern beide Anwendungsdomänen differenzierte Herangehensweisen, da z. B. in der OT dem Aspekt der Verfügbarkeit eine hohe Wichtigkeit zugeordnet wird. Abbildung 2 zeigt die unterschiedliche Priorisierung der Schutzziele für IT und OT

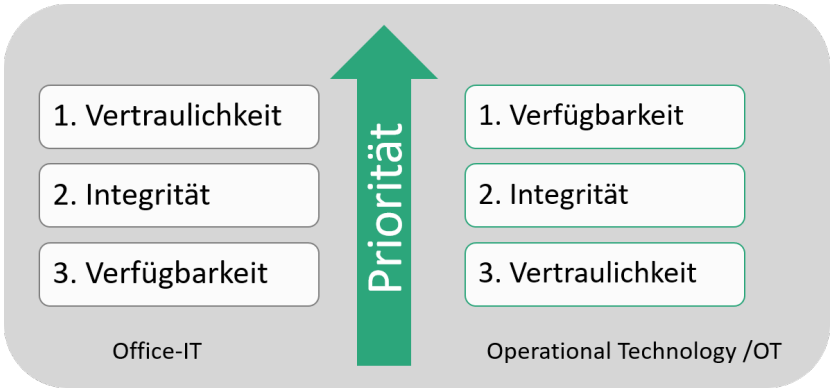

Abbildung 2: Schutzziele IT und OT

Aus diesem Grund sind die Normreihen ISO 27000 für den IT-Bereich und die IEC 62443 für den OT Bereich entstanden. Unterschiede und Gemeinsamkeiten dieser beiden Normreihen werden in [NIE2021] ausführlich diskutiert.

5 Die Norm IEC 62443

Die Normreihe IEC 62443 wurde mit Fokus auf die industrielle Automatisierungstechnik entwickelt. Die Norm richtet sich an Betreiber, Integratoren sowie System- und Komponentenhersteller von Automatisierungsanlagen. Die in der Norm definierten Konzepte und Vorgehensweisen basieren in vielen Aspekten auf der Normreihe ISO 27000. Abbildung 3 zeigt die Teile der IEC 62443-Normreihe.

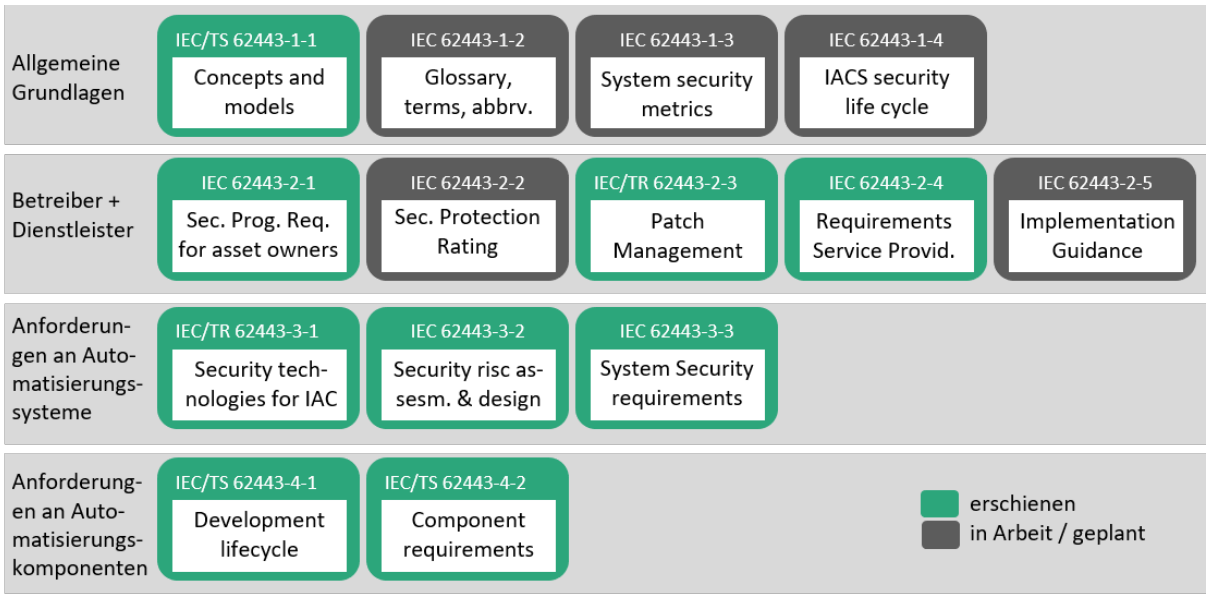

Abbildung 3: Struktur der Normreihe IEC 62443, in Anlehnung an [DKE2020]

Wie in Abbildung 3 zu erkennen ist, gliedert sich die Norm in vier Hauptbereiche, die im Folgenden näher beschrieben werden. Die grün hinterlegten Teile sind bereits veröffentlicht. Die grau hinterlegten Teile stehen nur als Entwurf für Diskussions- und Review-Zwecke eingeschränkt zur Verfügung.

5.1 IEC 62443 – Teil 1: Allgemeine Grundlagen

Abbildung 4 zeigt die Normteile, die den allgemeinen Grundlagen zuzuordnen sind.

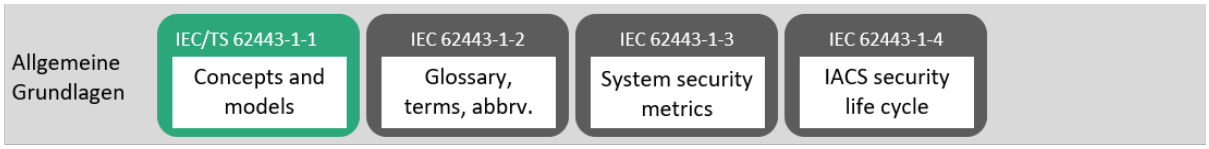

Abbildung 4: IEC 62443 - Teil 1: Allgemeine Grundlagen, in Anlehnung an [DKE2020]

Die Norm [IEC_62443-1-1] beschreibt die grundlegenden Konzepte und definiert die Begriffe und Security-Modelle für Automatisierungssysteme. Die Norm weist u.a. die folgenden Bestandteile auf:

- Risikoanalyse
- Reifegrad des Security Programms
- Vorgehensmodelle
- Zonen und Conduits

- Security Modelle
- Referenzarchitektur

Die [IEC_62443-1-2] definiert die in der Norm verwendeten Begriffe. Der Teil [IEC_62443-1-3] beschreibt Bewertungskriterien (Metriken) zur Bewertung der OT-Security. Der gesamte Sicherheitslebenszyklus und die zugehörigen Anwendungsfälle beschreibt der Teil [IEC_62443-1-4]. Die drei letztgenannten Teile liegen zurzeit lediglich im Entwurf vor, sie sind noch nicht allgemein zugänglich.

5.2 IEC 62443 – Teil 2: Betreiber und Dienstleister

Abbildung 5 zeigt die Teile der Norm IEC 62443, die sich an Betreiber und Dienstleister richten. Der Fokus liegt dabei auf dem Sicherheitsmanagement-System für Anlagebetreiber und den Anforderungen für Service-Anbieter.

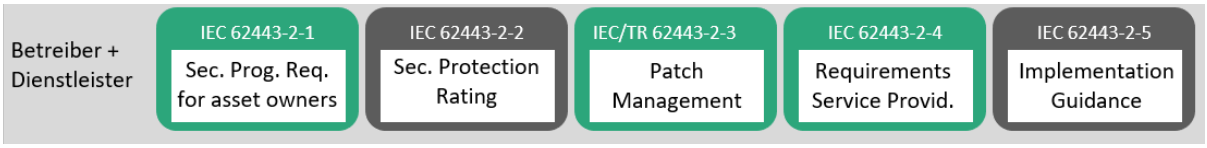

Abbildung 5: IEC 62443 - Teil 2: Betreiber und Dienstleister, in Anlehnung an [DKE2020]

Der Normteil [IEC_62443-2-1] definiert das Sicherheits-Management-System für Produktionsanlagen und beschreibt die entsprechenden Anforderungen. Dazu gehören z. B.:

- Definition von Security Prozessen
- Risiko-Management
- Definition von Anforderungen an das Training von Personal
- Pläne zur Kontinuität des Geschäftsbetriebes
- Zugangskontrolle
- Kontinuierlicher Verbesserungsprozess
- usw.

Der Teil [ISA_62443-2-2] beschreibt zunächst die Rollen und Verantwortlichkeiten im Security Prozess, um die Evaluation des Schutzes eines Automatisierungssystems über ein umfassendes (engl. holistic) Schutzschema zu realisieren. Durch die Kombination von technischen und organisatorischen Maßnahmen wird der Schutz der Automatisierungsanlage gewährleistet. Im Dokument wird ein entsprechendes Bewertungsschema vorgestellt, welches eine quantitative Bewertung des Anlagenschutzes über so genannte Protection-Level ermöglicht. Der Reifegrad der Organisation wird über Maturity-Level erfasst und nimmt darüber hinaus eine ganzheitliche Bewertung der technischen und organisatorischen Anforderungen vor.

Die Aktualisierung der Software von Automatisierungssystemen ist ein kritischer Prozess, da durch ein fehlgeschlagenes Software-Update ein Automatisierungssystem potentiell ausfallen kann. Aus diesem Grund finden sich in der [IEC_62443-2-3] umfassende Beschreibungen für die Durchführung von Software-Updates. Es wird insbesondere auf das Testen und das Ausrollen der Patches fokussiert.

Der Einsatz von Dienstleistern (Service-Providern) ist in vielen Produktionsanlagen geübte Praxis, z. B. für Inbetriebnahme und Service. Die Anforderungen an externes Personal definiert der Normteil [DIN_EN_IEC_62443-2-4], der bereits in deutscher Sprache vorliegt. Die Norm spezifiziert Vorgehensweisen für externes Personal, wobei sowohl Instandhaltungsdienstleister als auch Systemintegratoren berücksichtigt werden.

Der Normteil [IEC_62443-2-5] wird Implementierungshinweise für Betreiber enthalten. Dieser Normteil liegt noch nicht vor.

5.3 IEC 62443 – Teil 3: Anforderungen an Automatisierungssystem

Abbildung 6 listet die Normteile, welche die Anforderungen an ein Automatisierungssystem definieren.

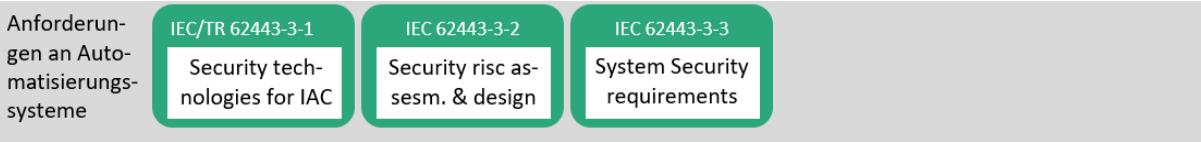

Abbildung 6: IEC 62443 - Teil 3 Anforderungen an Automatisierungssysteme, in Anlehnung an [DKE2020]

Der Teil [IEC_62443-3-1] beschreibt grundlegende Sicherheitstechnologien, wie z. B. Authentifizierungsverfahren, Firewalls, virtuelle Netzwerke, Intrusion-Detection-Systeme u.v.m. Dabei werden auch deren Anwendbarkeit für Automatisierungssysteme und evtl. vorhandene Schwächen beschrieben.

Der Normteil [DIN_EN_IEC_62443-3-2] befasst sich mit dem Sicherheitsprozess und insbesondere der Sicherheitsanalyse einer Produktionsanlage. Daraus wird dann ein Konzept für die Strukturierung der Anlage in Zonen (abgeschottete Bereiche) und Conduits (gesicherte Verbindungen zwischen den Bereichen) abgeleitet. Das Dokument führt dann durch den Prozess der Risikobewertung bei dem die vorhandenen Schwachstellen, die Eintrittswahrscheinlichkeit eines Schadens und das Schadensausmaß erfasst, evaluiert und dokumentiert werden. Auf Basis dieser Risikobetrachtung werden Schutzmaßnahmen zur Reduzierung des Risikos definiert.

Der Teil [DIN_IEC_62443-3-3] definiert grundlegende Anforderungen (engl. Foundational Requirements) an Automatisierungssysteme. Diese sind:

- 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-/OT-Sicherheitsvorfälle
- Verfügbarkeit von Ressourcen (RA)
  - Sicherstellung der Verfügbarkeit von Ressourcen

Auf Basis dieser grundlegenden Anforderungen definiert die Norm 99 Detailanforderungen an das Automatisierungssystem für die oben genannten Bereiche. Da die Automatisierungssysteme in unterschiedlichen Einsatzbereichen zu finden sein werden, unterscheidet die Norm die Anforderungen nach sogenannten Security-Leveln (SL) gemäß Tabelle 4.

Tabelle 4: Security Level [DIN_IEC_62443-3-3]

SL	Beschreibung
SL0	Keine besonderen Maßnahmen, kein besonderer Schutz notwendig
SL1	Schutz gegen gelegentlichen oder zufälligen Verstoß
SL2	Schutz gegen einen absichtlichen Verstoß mit einfachen Mitteln und geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation
SL3	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und mittlerem Aufwand, automatisierungstechnischen Fertigkeiten und mittlerer Motivation
SL4	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und erheblichem Aufwand, automatisierungstechnischen Fertigkeiten und hoher Motivation

Nicht alle Anforderungen sind für alle Security Level anzuwenden. Abhängig von dem Security Level sind mehr oder weniger Anforderungen zu erfüllen. Demzufolge kann der Betreiber das für ihn relevante Security Level definieren und dabei unterschiedliche Zonen in der Anlage unterschiedliche Security-Level zuordnen.

5.4 IEC 62443 – Teil 4: Anforderungen an Automatisierungskomponenten

Abbildung 7 zeigt die beiden Normteile, welche Anforderungen an Automatisierungskomponenten und den zugeordneten Entwicklungslebenszyklus beschreiben. Diese beiden Normteile sind für die Hersteller von Automatisierungs- und Netzwerkkomponenten relevant.

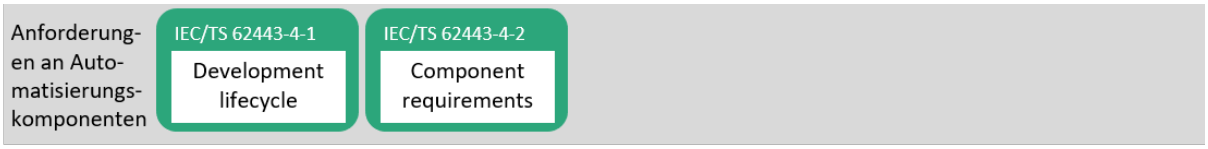

Abbildung 7: IEC 62443 - Teil 4: Anforderungen an Komponenten von Automatisierungssystemen in Anlehnung an [DKE2020]

Der Teil [DIN_EN_IEC_62443-4-1] befasst sich mit dem sicheren Entwicklungsprozess für Komponenten der Automatisierungstechnik, beschreibt alle Stufen der Entwicklung unter Berücksichtigung von OT-Sicherheitsanforderungen. Abbildung 8 zeigt die wesentlichen Schritte des Entwicklungsprozesses und die Kategorien der zugehörigen Anforderungskürzel in den grauen Textfeldern. Ziel des Konzeptes ist ein Security-by-Design-Ansatz. Weitere Informationen zu diesem Ansatz finden sich neben der [IEC_62443-4-2] auch in [VDI_2182_4].

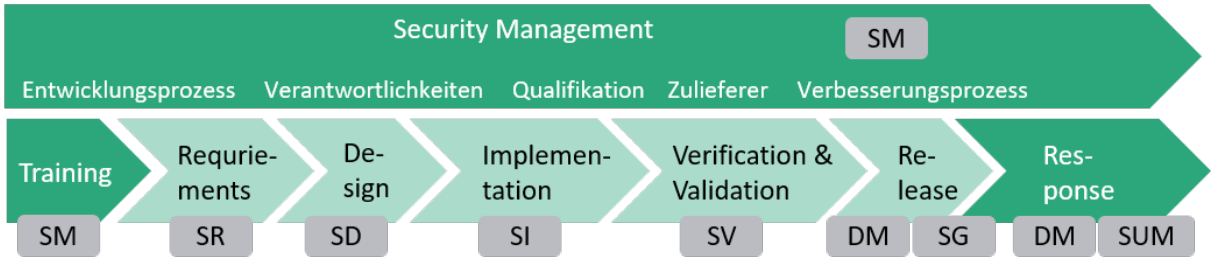

Abbildung 8: Sicherer Entwicklungslebenszyklus, in Anlehnung an [WAL2020]

Der im vorangehenden Kapitel beschriebene Normteil [DIN_IEC_62443-3-3] definiert Anforderungen an ein Automatisierungssystem. Es leuchtet ein, dass die Komponenten, aus denen das Automatisierungssystem besteht, diese Anforderungen ebenfalls erfüllen müssen oder die Erfüllung dieser Anforderungen unterstützen müssen. Daher definiert der Normteil [DIN_EN_IEC_62443-4-2] Anforderungen an Komponenten von Automatisierungssystemen und Netzwerkkomponenten. Diese Anforderungen leiten sich aus den Systemanforderungen ab, sind aber auf die jeweiligen Komponenten abgebildet. Die Norm unterscheidet Komponentenanforderungen (CR = Component Requirement) und weitergehende Anforderungen (RE = Requirement Enhancements). Diese Anforderungen basieren auf den Systemanforderungen (SR = System-Requirements) der [DIN_IEC_62443-3-3].

Die Norm [DIN_EN_IEC_62443-4-2] unterscheidet vier unterschiedliche Komponententypen, für die Anforderungen teilweise unterschiedlich definiert werden.

- Softwareanwendungen
- Host-Geräte
- Eingebettete Systeme (engl. Embedded Systems)
- Netzwerkkomponenten

Der überwiegende Teil der Anforderungen gilt für alle Komponentenarten in gleicher Weise.

5.5 Weiterführende Literatur zur IEC 62443

Die Normen der Reihe IEC 62443 sind zum Teil noch in der Erstellung. Ein Teil der Normreihe liegt erst im Entwurf vor. Das Dokument [ISA2020] liefert einen Überblick über den Stand der Normungsaktivitäten. Die DKE [DKE2020] stellt eine Übersicht über den Stand der deutschen Übersetzungen zur Verfügung.

Weitere Informationen zur Normreihe finden sich in [KOB2021]. Dort wird ein Überblick über die Normreihe IEC 62443 gegeben, ergänzt um die Zusammenhänge zwischen den Normteilen. Dieses Buch gibt einen kompakten und schnellen Einstieg in die Norm. [GUN2018] liefert Beispiele zur Einführung und Nutzung der IEC 62443.

Der ZEVI stellt in [ZVE2017] Komponentenherstellern Informationen zur Umsetzung der IEC 62663 aus Komponenten-Herstellersicht zur Verfügung. Ebenso geht der VDMA [VDM2021] mit dem Leitfaden für Maschinenbauer mit IEC 62443 vor.

i

6 Die Rollen und Verantwortlichkeiten in der IEC 62443

Die Übersicht über die Normteile richtet sich an verschiedene Adressaten wie die Abbildung 9 zeigt.

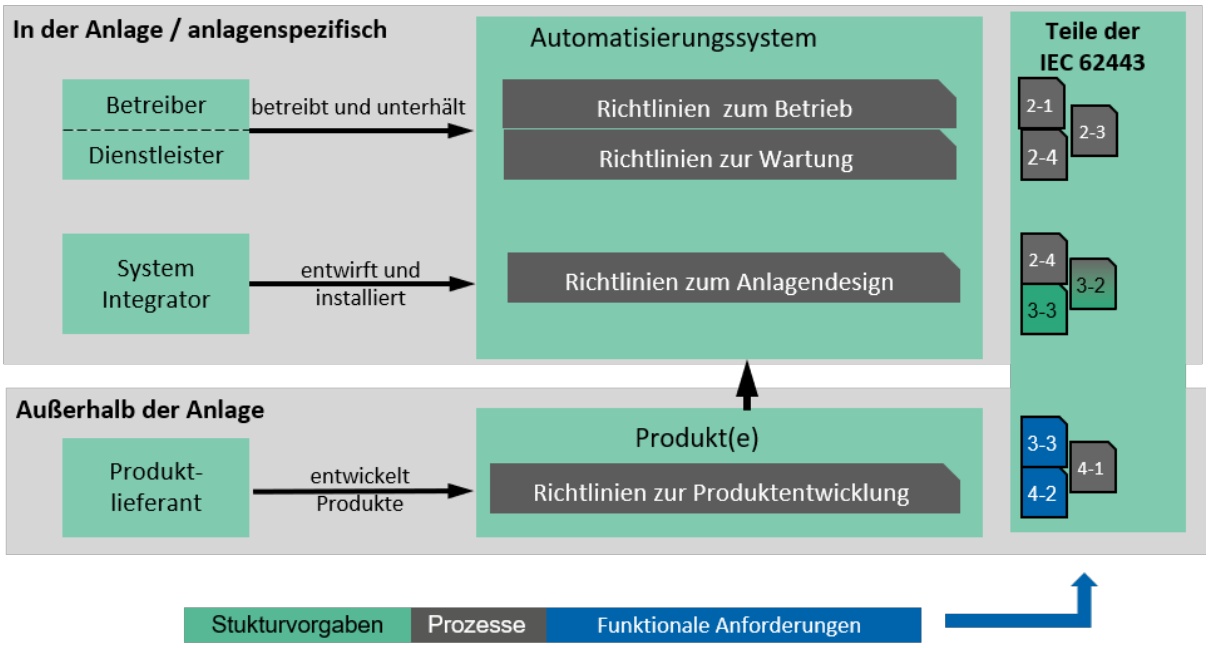

Abbildung 9: Zuordnung der Rollen im Sicherheitsprozess, (in Anlehnung an [ISA_62443-2-2])

Im Wesentlichen werden die Rollen Betreiber, System-Integrator und Produktlieferant unterschieden. Der Betreiber kann zusätzlich auf Dienstleister, z. B. für Service-Arbeiten, zurückgreifen.

6.1 Die Rolle Betreiber in der IEC 62443

Die Rolle Betreiber / Dienstleister ist verantwortlich für den Betrieb und Wartung einer Produktionsanlage. Für diese Rollen sind im Wesentlichen die Richtlinien der IEC 62443 zum Betrieb und zur Wartung relevant. Hier sind die Normteile von Interesse, die Aufbau und Betrieb des Sicherheitsmanagementsystems (engl. Information Security Management System -ISMS) [IEC_62443-2-1] sowie die Rolle von Dienstleistern [DIN_EN_IEC_62443-2-4] definieren. Weiterhin ist für die Betreiber der Teil [IEC_62443-2-3] von Bedeutung, der die Aktualisierung der Leitsystemsoftware (Patch Management) regelt.

6.2 Die Rolle System-Integrator in der IEC 62443

Der Systemintegrator entwirft und installiert das Automatisierungssystem. Für diese Rolle ist der Normteil [DIN_IEC_62443-3-3] relevant, der Vorgaben bzgl. des Aufbaus und der Strukturierung der Anlage, z. B. in Zonen liefert. Der Teil [DIN_EN_IEC_62443-3-2] kann ergänzend zur Sicherheitsrisikobewertung und zur Systemstrukturierung (Zonenkonzept) herangezogen werden. Sofern der Planungsprozess nicht durch den Betreiber, sondern durch einen Dienstleister durchgeführt wird, ist ergänzend der Teil [DIN_EN_IEC_62443-2-4] zu beachten, der Anforderungen an Dienstleister (eng. Service Provider) beschreibt. Führt der Anlagenbetreiber die Planungsarbeiten selbst durch, gelten die in diesem Abschnitt genannten Normen sinngemäß ebenfalls für den Betreiber in seiner Rolle als Anlagenplaner.

6.3 Die Rolle Produktlieferant in der IEC 62443

Die dritte zu betrachtende 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_EN_IEC_62443-4-2] kennen und berücksichtigen.

7 Einordnung von PROFINET in die IEC 62443

PROFIBUS & PROFINET International (PI) unterstützt seine Mitgliedsunternehmen bei der Entwicklung von Produkten und Systemen. Dies geschieht durch die Bereitstellung von Standards und Richtlinien. Diese betreffen sowohl das Protokoll selbst als auch den Einsatz von PROFINET-Produkten in Form von Anwendungsrichtlinien.

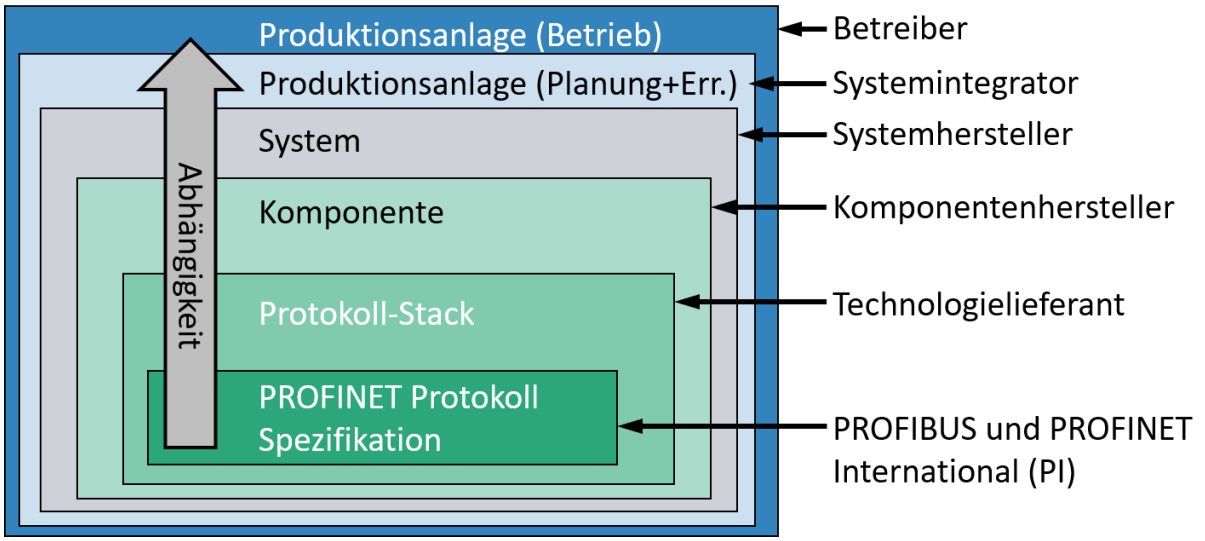

Abbildung 10: Die Rollen im Produktentstehungsprozess

Abbildung 10 zeigt die Rollen im Produktentstehungsprozess. Zunächst stellt PI Protokollspezifikationen, z. B. für PROFINET bereit. Einen Überblick über diese Spezifikationen gibt [PNO2010]. Aufbauend auf diesen Spezifikationen entwickeln dann Technologielieferanten Software-Module, wie z. B. PROFINET-Protokoll-Stacks. Komponentenhersteller bauen unter Nutzung dieser Software-Module PROFINET-Komponenten, wie z. B. Remote-IO-Baugruppen, Frequenzumrichter oder Laserscanner. Diese Komponenten werden mit anderen PROFINET-Komponenten zu Systemen verbaut. Es existieren Systemhersteller, die die Rollen Komponentenhersteller und Technologielieferant zeitgleich ausfüllen. Systemintegratoren passen Systeme und weitere Komponenten zu Produktionsanlagen ein, die anschließend vom Betreiber genutzt werden.

Die Normreihe IEC 62443 definiert den OT-Sicherheitsprozess als ganzheitlichen Prozess: Von der Produktentstehung über den Betrieb bis zur Außerbetriebsetzung. Daher haben viele der genannten Akteure Teilaspekte der IEC 62443-Normreihe in ihren Prozessen zu berücksichtigen. Tabelle 5 beschreibt den Lieferumfang (Deliverables) längs des Produktentstehungs- und Nutzungsprozesses, die jeweiligen Produkte oder Dienstleistungen sowie die Rolle der PI.

Tabelle 5: Deliverables im Produktentstehungsprozess

Deliverables	Zu beachtender IEC 62443-Normteil	Akteur produziert	Unterstützung der PI
PROFINET Protokollspezifikation	[DIN_EN_IEC_62443-4-1] [DIN_EN_IEC_62443-4-2]	PI-Arbeitsgruppe schreibt und evaluiert PROFINET Spezifikation unter Beachtung des sicheren Entwicklungsprozesses. Z. B. mit vorangehender Risikoanalyse und Beachtung der funktionalen Anforderungen des Teils 4-2.	PI Arbeitsgruppen (WGs) erstellen Protokollspezifikationen unter Berücksichtigung der Normanforderungen.
PROFINET Protokollstack	[DIN_EN_IEC_62443-4-1] [DIN_EN_IEC_62443-4-2]	Stack-Lieferant programmiert PROFINET Protokollstack (Software Modul) unter Beachtung des sicheren Entwicklungsprozesses. Z. B. mit vorangehender Verifikation der OT-Sicherheitsanforderungen durch Codereviews und entsprechende Schnittstellen- und Modultests und Beachtung der funktionalen Anforderungen des Teils 4-2.	PI Arbeitsgruppen erstellen. zusätzlich zur Protokollspezifikation Implementierungshinweise als Unterstützung für den Entwicklungsprozess, z. B. [PNO2020].
PROFINET Komponente	[DIN_EN_IEC_62443-4-1] [DIN_EN_IEC_62443-4-2]	Komponentenhersteller produziert PROFINET-Komponente, ggf. unter Nutzung eines Protokollstacks. Bei der Entwicklung der Komponenten sind der sichere Produktentwicklungslebenszyklus nach Teil 4-1 und die funktionalen Anforderungen nach Teil 4-2 zu beachten.	PI Arbeitsgruppen erstellen zusätzlich zur Spezifikation: Implementierungshinweise als Unterstützung für den Entwicklungsprozess, z. B. [PNO2020], Interpretationshilfe für den Teil 4-2 (in Arbeit) und Security-Test-Spezifikation [PNO2017a].
PROFINET System	[DIN_EN_IEC_62443-4-1] [DIN_EN_IEC_62443-4-2] [DIN_IEC_62443-3-3]	Systemhersteller produziert System ggf. unter Nutzung von PROFINET Komponenten oder von PROFINET Protokollstacks. Der sichere Produktentwicklungslebenszyklus nach Teil 4-1, die Komponentenanforderungen nach Teil 4-2 und die Systemanforderungen	PI Arbeitsgruppen erstellen zusätzlich zur Spezifikation: Implementierungshinweise als Unterstützung für den Entwicklungsprozess, z. B. [PNO2020], Interpretationshilfe

		nach Teil 3-3 sind zu beachten.	für den Teil 4-2 (in Arbeit) und Security-Test-Spezifikation [PNO2017a].
Produktionsanlage (Planung + Errichtung)	[DIN_EN_IEC_62443-2-4] [DIN_EN_IEC_62443-3-2] [DIN_IEC_62443-3-3]	Systemintegrator plant und errichtet eine Produktionsanlage im Auftrag des Betreibers. Er führt in Abstimmung mit Betreiber unter Berücksichtigung von Teil 3-2 Risikoanalyse durch und legt erforderlichen Security-Level fest. Er entwirft und strukturiert die Anlage unter Berücksichtigung von Teil 3-3 und beachtet dabei die Anforderungen an Dienstleister aus Teil 2-4	PI liefert Beschreibung von Vorgehensweisen und Standardlösungen für PROFINET-basierte Systeme unter Berücksichtigung des Teils 3-3. Siehe [PNO2013].
Produktionsanlage (Betrieb)	[IEC_62443-2-1] [IEC_62443-2-3] [DIN_EN_IEC_62443-2-4]	Betreiber betreibt Anlage über den Lebenszyklus von der Errichtung bis zur Außerbetriebsetzung. Betreiber etabliert und unterhält OT-Security-Managementprozess und beachtet dabei die Prozessanforderungen nach Teil 2-1. Die Software-Aktualisierungen im Betrieb werden unter Beachtung von Teil 2-3 durchgeführt. Der Einsatz von Dienstleistern berücksichtig den Teil 2-4.	---

Tabelle 5 zeigt, dass die PI für die einzelnen Schritte des Produkt- und Anlagenentstehungsprozesses unterstützende Dokumentation bereitstellen wird. Einige Dokumente sind bereits veröffentlicht. Weitere sind noch in der Entstehung begriffen.

7.1 Das zukünftige OT-Security-Konzept von PROFINET

Derzeit erarbeitet die PI ein Security-Konzept, welches eine Absicherung der Kommunikation mit kryptografischen Mitteln erfolgt. Das grundlegende Konzept ist in [PNO2018] beschreiben. Die Umsetzung in der PROFINET Spezifikation findet sich in [PNO2021a] und [PNO2021b]. Abbildung 11 zeigt in grüner Farbe die Kommunikationsbeziehungen in einer PROFINET-Anlage, die künftig im Rahmen der PROFINET Spezifikation kryptografisch gesichert werden sollen.

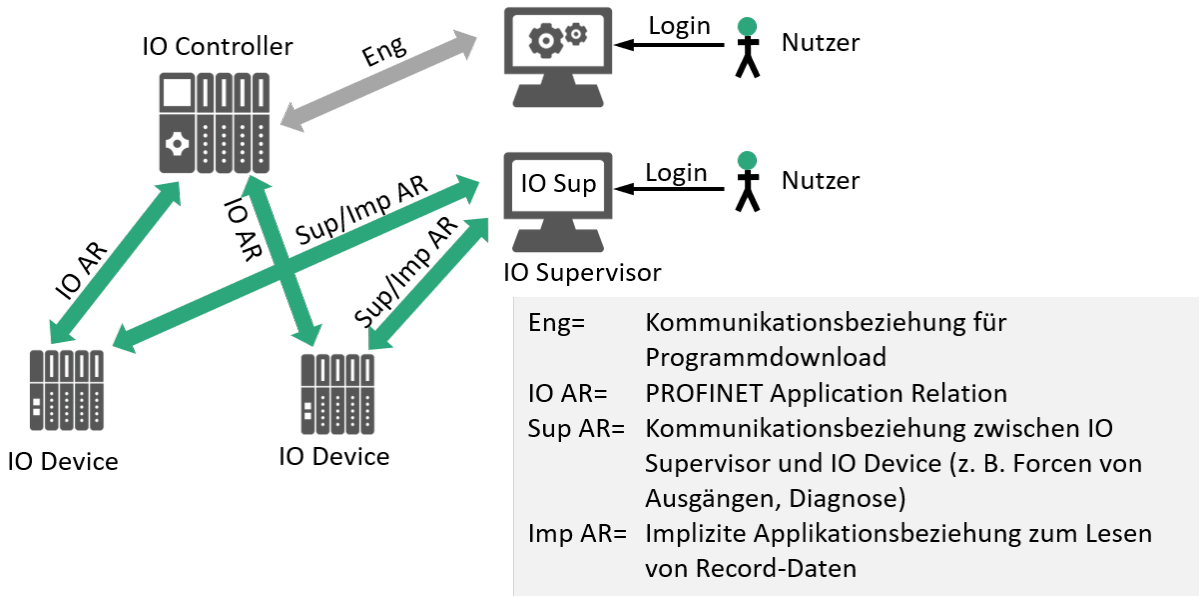

Abbildung 11: Kommunikationsbeziehungen im PROFINET Security Konzept

Die grau dargestellte Anbindung der Engineering-Station ist ebenfalls kryptografisch gesichert. Diese Absicherung ist jedoch herstellerspezifisch und ist somt nicht Bestandteil der PROFINET-Spezifikation. Auch die Nutzerzugriffe auf die Engineering-Station und den IO-Supervisor sind herstellerspezifisch abzusichern und nicht Bestandteil der geplanten Arbeiten.

Das PROFINET-Security-Konzept basiert auf den folgenden Eckpunkten:

- Schutz der Kommunikation durch eine kryptografische Prüfsumme (Hash, Message Authentication Code)
- Je nach Dienst zusätzliche Absicherung durch Verschlüsselung
- Nutzung von Hersteller- und Betreiber-Zertifikaten zur Sicherstellung der Authentizität der Kommunikationsteilnehmer
- Hochlauf des Systems in einem zweistufigen Prozess
    - Start des Verbindungaufbaus unter Nutzung eines asymmetrischen Verfahrens.
    - Danach Übergang auf ein symmetrisches Verfahren (Performance-Gründe)

Wesentliche Aspekte der Security-Maßnahmen sind bereits in der aktuellen PROFINET-Spezifikation [PNO2021a], [PNO2021b] eingearbeitet.

7.2 Abbildung der PROFINET Security Klassen auf die Security Level der IEC 62443

Tabelle 4 definiert die Security-Level, die in der [DIN_IEC_62443-3-3] festgelegt sind. Die Level beschreiben die Fähigkeiten eines Angreifers. Die Level reichen von SL0 (kein Schutz erforderlich) bis SL4 (Schutz gegen Angreifer mit hoher Motivation und hohen Fähigkeiten). Bei der Risikoanalyse muss der Betreiber den für die Anlage erforderlichen Security-Level definieren. Abhängig vom gewünschten Security Level greifen dann schärfere oder weniger scharfe Anforderungen der Norm.

Zur Erfüllung dieser Anforderungen müssen die Komponentenhersteller die Security-Anforderungen der [DIN_EN_IEC_62443-4-2] bei der Entwicklung ihrer Produkte berücksichtigen. Hierbei muss der Hersteller festlegen, welchen Security Level gemäß Tabelle 4 das Produkt erfüllen soll. Abhängig vom zu erreichenden Security-Level sind entsprechende Anforderungen zu erfüllen und auch durch einen entsprechenden Test nachzuweisen. Zusätzlich müssen die Hersteller bei der Entwicklung der Produkte den sicheren Entwicklungslebenszyklus gemäß

[DIN_EN_IEC_62443-4-1] im Unternehmen etabliert haben und dessen Anforderungen bei der Entwicklung der Produkte berücksichtigen. Mit der PROFINET-Spezifikation liefert PI zusätzlich einen Baustein für eine Komponente, welche die Security-Anforderungen der [DIN_EN_IEC_62443-4-2] berücksichtigt.

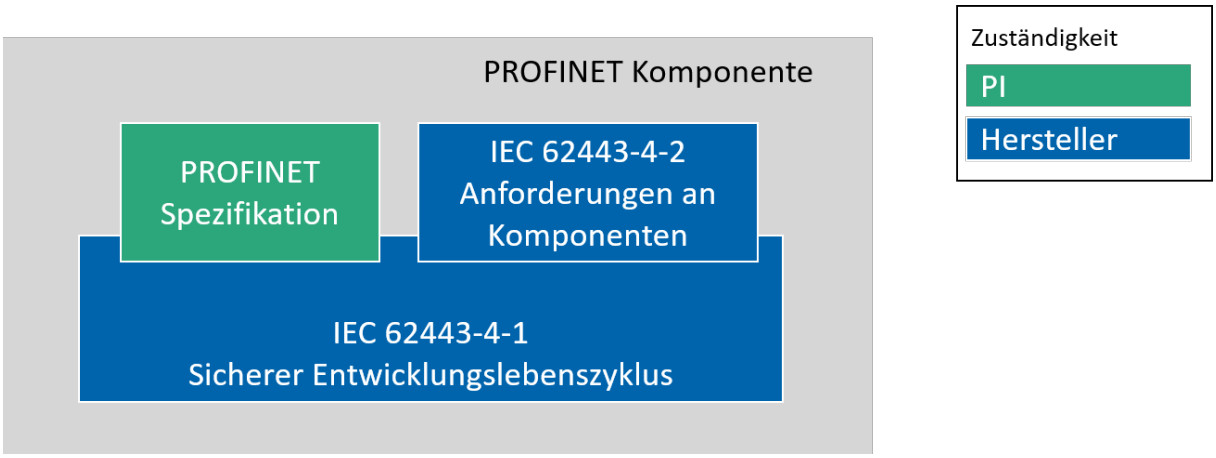

Abbildung 12: Security-Bestandteile einer PROFINET Komponente

Abbildung 12 zeigt das Zusammenspiel der Security-Bestandteile einer PROFINET-Komponente:

- PI stellt mit der PROFINET-Spezifikation die Grundlage für eine sichere Kommunikation der Baugruppe zur Verfügung.
- Der Komponentenhersteller realisiert seine Komponente, wobei der Kommunikationsteil der Komponente sich auf die Vorgaben der PROFINET-Spezifikation abstützen kann.
- Der Komponentenhersteller entwickelt die Komponente unter Beachtung des sicheren Produktentwicklungslebenszyklus.

Man kann also festhalten, dass die PROFINET-Spezifikation eine wichtige Grundlage für eine sichere PROFINET Komponente liefert, dass aber der Hersteller weitere Anforderungen im Produkt und im Produktentwicklungslebenszyklus zu beachten hat.

In [PNO2018] definiert PI die PROFINET-Security Klassen gemäß Tabelle 6.

Tabelle 6: PROFINET Security-Klassen

Security Klasse	Name der PROFINET Security-Klasse	Definition	Typisches Einsatzgebiet
1	Robustness	Heutiger Stand der PN-Security und zusätzlich: SNMP-Default Strings können geändert werden, DCP-Befehle können auf „nur lesen“, gesetzt werden, GSD Dateien werden durch Signierung gegen unbemerkte Veränderung geschützt.	Inkrementelle Verbesserung zum aktuellen Stand der PN-Security.
2	Integrity + Authenticity	Zusätzlich zu den Anforderungen der Security-Klasse 1 werden die Integrität und Authentizität der Assets und der Kommunikationsbeziehungen über kryptografische Funktionen abgesichert. Die Vertraulichkeit der Konfigurationsdaten ist sichergestellt. Die Vertraulichkeit der IO Daten ist nicht erforderlich.	Systeme mit Kommunikationsbeziehungen über Anlagenzonengrenzen hinweg. System kann nicht oder kaum in gegenseitig abgeschottete Zonen unterteilt werden. Zugang zur Anlage kann nicht abgesichert werden (z. B. Anlage im Freien ohne dauerhaft anwesendes Personal). Anwendung stellt keine Anforderungen in Bezug auf Vertraulichkeit der IO-Daten.
3	Confidentiality	Zusätzlich zu den Anforderungen der Security-Klasse 2 wird die Vertraulichkeit aller Kommunikationsbeziehungen gewährleistet.	Anlage gemäß Security-Klasse 2 bei der aus den IO-Daten des Systems auf Firmengeheimnisse geschlossen werden kann.

Es ist zu erkennen, dass diese Security-Klassen Fähigkeiten des PROFINET-Protokolls in Bezug auf Anforderungen der OT-Security beschreiben. Eine direkte Abbildung auf die Security Level aus der [DIN_IEC_62443-3-3] gemäß Tabelle 4 ist allerdings nicht möglich, da das PROFINET Security Konzept gemäß Abbildung 12 nur einen Baustein zur Erfüllung der Security-Anforderungen liefert. Allerdings kann eine Zuordnung erfolgen, welche Komponentenanforderungen der [DIN_EN_IEC_62443-4-2] durch die PROFINET-Security-Klassen gemäß Tabelle 6 erfüllt werden können, sofern die weiteren Anforderungen durch den Hersteller berücksichtigt werden.

Tabelle 7: Zuordnung der PROFINET-Security-Klassen zu den IEC 62443-Security-Leveln

IEC 62443 Security Level (SL)	Erforderliche PROFINET Security Klasse	Kommentar
SL0	beliebig	Keine besonderen Anforderungen.
SL1	PN Security Klasse 2 und die Berücksichtigung der Anforderungen von SL1 bei der Entwicklung der Baugruppe gemäß [DIN_EN_IEC_62443-4-2]	Bei zusätzlichen Anforderungen in Bezug auf Vertraulichkeit der Daten PN Security-klasse 3.
SL2	PN Security Klasse 2 und die Berücksichtigung der Anforderungen von SL2 bei der Entwicklung der Baugruppe gemäß [DIN_EN_IEC_62443-4-2]	Bei Anforderungen in Bezug auf Vertraulichkeit der Daten Klasse 3.
SL3	PN Security Klasse 2 und die Berücksichtigung der Anforderungen von SL3 bei der Entwicklung der Baugruppe gemäß [DIN_EN_IEC_62443-4-2]	Bei Anforderungen in Bezug auf Vertraulichkeit der Daten Klasse 3 und zusätzliche Maßnahmen.
SL4	Zurzeit nicht betrachtet	Zurzeit nicht betrachtet

Tabelle 7 zeigt, dass die IEC-62443-Security-Level SL1, SL2 und SL3 über die PROFINET Security-Klassen 2 und 3 abgedeckt werden können, sofern der Baugruppenhersteller die weiteren Anforderungen des jeweiligen Security Levels bei der Entwicklung des Produktes berücksichtigt. Der Security Level 4 wurden in den bisherigen Analysen von PI nicht betrachtet.

Sofern über das PROFINET Betriebsgeheimnisse über die zyklischen Daten übertragen werden (z. B. Produktionsrezepte), sollte die PROFINET Security-Klasse 3 zum Einsatz kommen.

7.3 Die Rolle von PI und der Hersteller in Bezug auf die OT-Security

In Tabelle 5 wurden bereits die „Deliverables“ der einzelnen Akteure und ebenfalls die Rolle der PI beschrieben. Hieraus lässt sich die Arbeitsteilung zwischen den Herstellern und der PI ableiten, die folgendermaßen aussieht.

PI: Künftig Bereitstellung von:

1. PROFINET-Spezifikation(en), welche die entsprechenden Security-Features von PROFINET spezifizieren.
2. Dokumente zur Interpretation der Spezifikation.
3. Erweiterung der PROFINET-Test-Beschreibung für den Test der Security-Features auf Basis von [PNO2017a], [PNO2017b].
4. Erweiterung des Test-Systems für den automatisierten Test der Security-Funktionen in den Testlaboren
5. Software zur Signierung von GSD(ML)-Dateien auf Basis von [PNO2020]
6. Aktualisierte PROFINET Security-Richtline auf Basis von [PNO2013].

Hersteller:

1. Implementierung eines sicheren Produktentwicklungslebenszyklus gemäß [DIN_EN_IEC_62443-4-1]
2. Beachtung der Anforderungen aus [DIN_EN_IEC_62443-4-2] bei der Integration der PROFINET-Schnittstelle. Hierbei kann die von der PI bereitgestellten Interpretationshilfe (zurzeit noch in Arbeit) zur Unterstützung herangezogen werden. Abhängig vom angestrebten IEC 62443-Security-Levlel ist der Hersteller auch für die Beachtung der Security-Anforderungen des jeweiligen Security-Levels bei Implementierung und Test des Produktes verantwortlich.
3. Abdeckung aller Security-Aspekte, die nicht durch die PROFINET-Spezifikation abgedeckt sind und die Komponente allgemein betreffen, z. B. Nutzerverwaltung in der Engineering-Station oder im Webserver der Komponenten, Absicherung der Kommunikation zwischen Engineering-Station und Automatisierungskomponenten.

Aus der Aufgabenteilung ist zu erkennen, dass die PNO vorgefertigte Bausteine für ein OT-Security-Konzept liefern kann, aber nicht für komplette Produkte oder Systeme. Diese Verantwortung liegt nach wie vor in der Hand der Hersteller.

7.4 Was kann PI nicht leisten?

Mit dem PROFINET-Protokoll und den unterstützenden Dokumenten definiert PI lediglich einen Teil des Automatisierungssystems. Die Sicherstellung der OT-Security des Gesamtsystems, die Beachtung des geschützten Entwicklungslebenszyklus nach [DIN_EN_IEC_62443-4-1] und die Erfüllung der Anforderungen der [DIN_EN_IEC_62443-4-2], die nicht durch PROFINET abgedeckt sind, obliegt dem Hersteller der Komponente / des Systems.

7.5 Empfehlung für Betreiber in Bezug auf die IEC 62443

Betreiber von Produktionsanlagen sollten sich in Bezug auf die OT-Security Ihrer Produktionsanlagen wie folgt positionieren:

1. Der Betreiber ist für die Errichtung und die Aufrechterhaltung eines Information-Security-Management-System (ISMS) verantwortlich. Dies kann wahlweise nach der [IEC_62443-2-1] aber auch nach [DIN_EN_ISO_27001] erfolgen. Zur Abgrenzung zwischen diesen Normen und den Vor- und Nachteilen siehe [NIE2021].
2. Bei der Planung einer Anlage sollte der Betreiber oder der beauftrage Systemintegrator eine Risikoanalyse nach [ISA_62443-2-2] durchführen und den erforderlichen Security Level (SL) festlegen. Alternativ ist eine Risikoanalyse nach [VDI_2182_1] möglich.
3. Abhängig vom erforderlichen Security Level, dem Ergebnis der Risikoanalyse und der Leistungsfähigkeit der Geräte (unterstützte PN Security Klassen) sollte die Anlage gemäß [DIN_IEC_62443-3-3] strukturiert und -sofern erforderlich- in Zonen aufgeteilt werden. Dabei sind Vorgaben für die Konfiguration und den Betrieb in Form einer Security Policy festzulegen.
4. Die Verwendung von Komponenten, die unter Berücksichtigung der Anforderungen nach [DIN_EN_IEC_62443-4-2] entwickelt wurden, kann eine sichere Auslegung einer Anlage vereinfachen, ist aber keine zwingende Voraussetzung.
5. In Bezug auf PROFINET-Systeme liefert [PNO2013] Hinweise und Musterkonfigurationen. Eine Aktualisierung dieser Richtlinie ist in Planung.

Das PROFINET-Zonenkonzept stellt mit der Abschottung der Anlage und einer Unterteilung in Zonen eine wesentliche Komponente eines Defense-in-Depth-Konzeptes [DHS2016] dar. Mit den in Arbeit befindlichen Security Erweiterungen wird nun zusätzlich der Schutz innerhalb einer Zone durch eine kryptografische Absicherung des PROFINET-Protokolls erhöht.

8 Zusammenfassung

Das vorliegende Dokument grenzt zunächst die Anwendungsfelder IT (klassische Informationstechnologie) und OT (Operational Technologie – Einsatz in Produktionsanlagen) voneinander ab und definiert die beiden Einsatzfelder. Im Weiteren fokussiert der Beitrag auf das Einsatzfeld OT. Dafür kommt in der Regel die Normreihe IEC 62443 als OT-Security-Norm zum Einsatz. Der Beitrag liefert dem Leser zunächst eine Einführung in die OT-Security-Norm IEC 62443 und beschreibt die einzelnen Bestandteile der Norm und den für die Entwicklung relevanten sicheren Entwicklungslebenszyklus.

Die Norm definiert die Rollen Betreiber, Dienstleister, Systemintegrator und Produktlieferant. Das White-Paper beschreibt, welche Aufgaben und welche Teile der Norm diesen Rollen zuzuordnen sind.

Nach diesen einführenden Teilen erfolgt eine Einordnung von PROFINET in den Kontext der IEC-62443-Normenreihe. Hierbei werden neben den schon genannten Rollen zusätzlich die Rolle von. PROFIBUS & PROFINET International (PI), die Rolle der Technologielieferanten und der Komponenten- und Systemhersteller eingeführt. Anschließend beschreibt das White-Paper die jeweiligen Rollen, die den „Deliverables“ im Produktentstehungsprozess zuzuordnen sind. Nach einer grundlegenden Beschreibung des PROFINET-Security-Konzeptes erfolgt eine Abbildung der PROFINET Security-Klassen auf die Security-Level der IEC 62443. Der Abschnitt schließt mit einer Empfehlung für Betreiber in Bezug auf die Verwendung der IEC-62443-Normreihe.

9 Index

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 986197 0 ● Fax +49 721 986197 11
E-mail info@profibus.com
www.profibus.com ● www.profinet.com