Security Erweiterungen für PROFINET

PI White Paper für PROFINET

Version 1.05 – Datum 12.02.2019

File name : PROFINET_Protocol_Security_Whitepaper_V105_Feb19

Comments to be submitted to WG editior: Karl-Heinz.Niemann@Hs-Hannover.de

Prepared by PI Working Group Security “CB / PG 10”

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 / 96 58 590
Fax: +49 721 / 96 58 589
E-mail: info@profibus.com
Web site: www.profibus.com

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Änderungshistorie

Version	Autor	Datum	Änderungsvermerk
1.00	Karl-Heinz Niemann	15.12.2018	Erste Version nach WG-Freigabe für PI-internes Review
1.03	Karl-Heinz Niemann	06.02.2019	Review während WG Sitzung, Alle Review Kommentare eingearbeitet
1.04	Karl-Heinz Niemann	12.02.2019	Einarbeiten von Änderungen, die sich aus Review-Kommentaren ergeben haben und in der Sitzung nicht eingearbeitet wurden. Löschen der erledigten Review-Kommentare
1.05	Karl-Heinz Niemann	12.02.2019	Bereinigte Version ohne Änderungsverfolgung. Kandidat für Beiratsreview

Abstract

Im Rahmen der weitreichenden Digitalisierung von Produktionsprozessen rückt die IT-Sicherheit von Produktionsanlagen immer stärker in den Vordergrund. Die durchgängige Vernetzung im Unternehmen, die vertikale Integration und die Tendenz zu flacheren Systemhierarchien erfordern durchgängige Ansätze für die IT-Sicherheit in der Produktion. Bisherige Konzepte, die in der Hauptsache auf eine Abschottung der Produktionsanlagen setzen, müssen durch neue Konzepte, die einen Schutz der Komponenten vorsehen, ergänzt werden.

Diese Notwendigkeit hat PROFIBUS & PROFINET International (PI) erkannt und die Arbeitsgruppe CB/WG 10 Security mit der Erarbeitung eines Konzeptes beauftragt. Dieses Dokument gibt einen ersten Einblick in die bisherigen Ergebnisse der Arbeit. Es soll dazu dienen, in eine Diskussion mit Herstellern, Integratoren und Anwendern einzusteigen. Ziel dieser Diskussion ist ein abgestimmtes und tragfähiges Konzept, welches die industrielle Kommunikation mit PROFINET fit für die Anforderungen der Zukunft macht.

Das vorliegende Dokument beschreibt zunächst die Motivation und die Vorgehensweise für die Erarbeitung eines Security-Konzeptes. Danach werden die Security-Anforderungen ermittelt und die Akteure im Security-Prozess werden benannt und gegeneinander abgegrenzt. Im Weiteren befasst sich das Dokument dann mit den notwendigen Ergänzungen am PROFINET Protokoll und den für den Systemhochlauf erforderlichen zusätzlichen Protokollen. Am Ende werden die Stellen beschrieben, an denen Änderungen erforderlich sein werden. Das Dokument schließt mit einer Aufstellung der zu ändernden Spezifikationen und einem Ausblick auf das weitere Vorgehen.

1 Motivation

Die industrielle Kommunikation mit Industrial Ethernet Protokollen, wie z. B. PROFINET, gewinnt, auch im Kontext von Industrie 4.0, zunehmend an Bedeutung. Horizontale und vertikale Vernetzung in Unternehmen werden künftig weiter zunehmen.

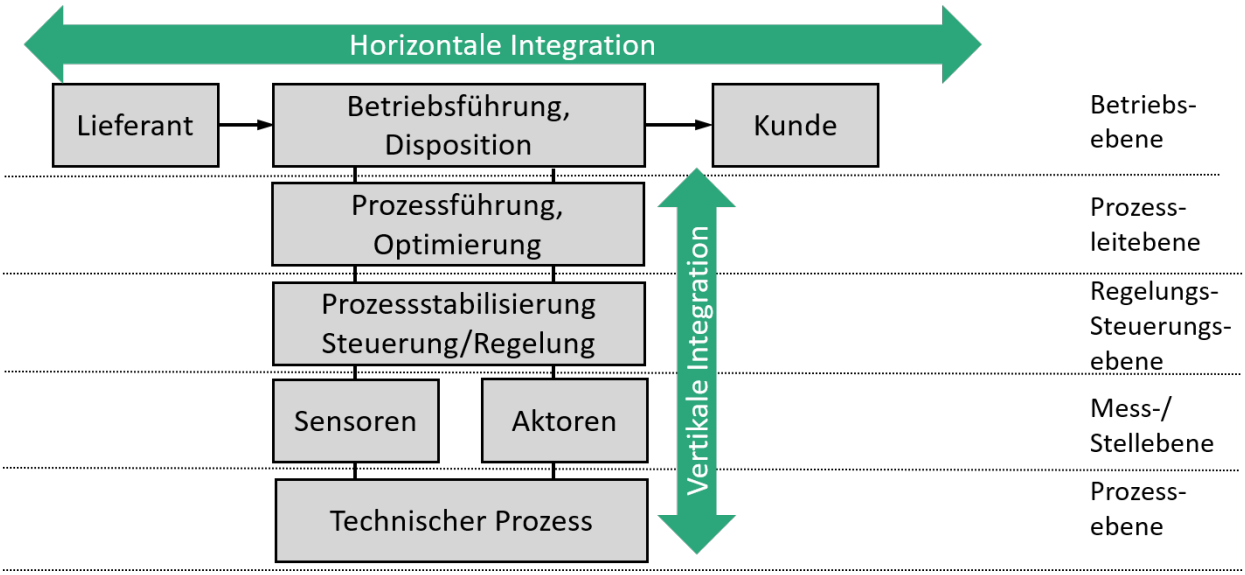

Abbildung 1: Horizontale und vertikale Integration in einem Beispielunternehmen

Abbildung 1 zeigt am Beispiel einer klassischen Automatisierungsstruktur die horizontale und die vertikale Integration in einem Beispielunternehmen. Bei der horizontalen Integration ist das produzierende Unternehmen über seine Unternehmensgrenzen hinweg sowohl mit Lieferanten als auch mit Kunden datentechnisch verbunden. Produktionsdaten werden über Unternehmensgrenzen hinweg ausgetauscht. Bei der vertikalen Integration werden Informationen nicht nur an die überlagerte Ebene, sondern auch über Ebenengrenzen hinweg kommuniziert.

Die Anzahl kommunikationsfähiger Komponenten wird steigen. Dabei wird die Sicherstellung der IT-Sicherheit von Produktionsanlagen als die wesentliche Anforderung an künftige Automatisierungslösungen angesehen [VDE2016]. Dieser Anforderung müssen sich auch industrielle Echtzeitsysteme, wie PROFINET, stellen. Die IT-Sicherheit ist ein wesentlicher Bestandteil der Industrie-4.0-Strategie von PROFIBUS & PROFINET International (PI). Aus diesem Grund befasst sich die PI-Arbeitsgruppe CB/WG 10 Security momentan vorrangig mit diesem Thema.

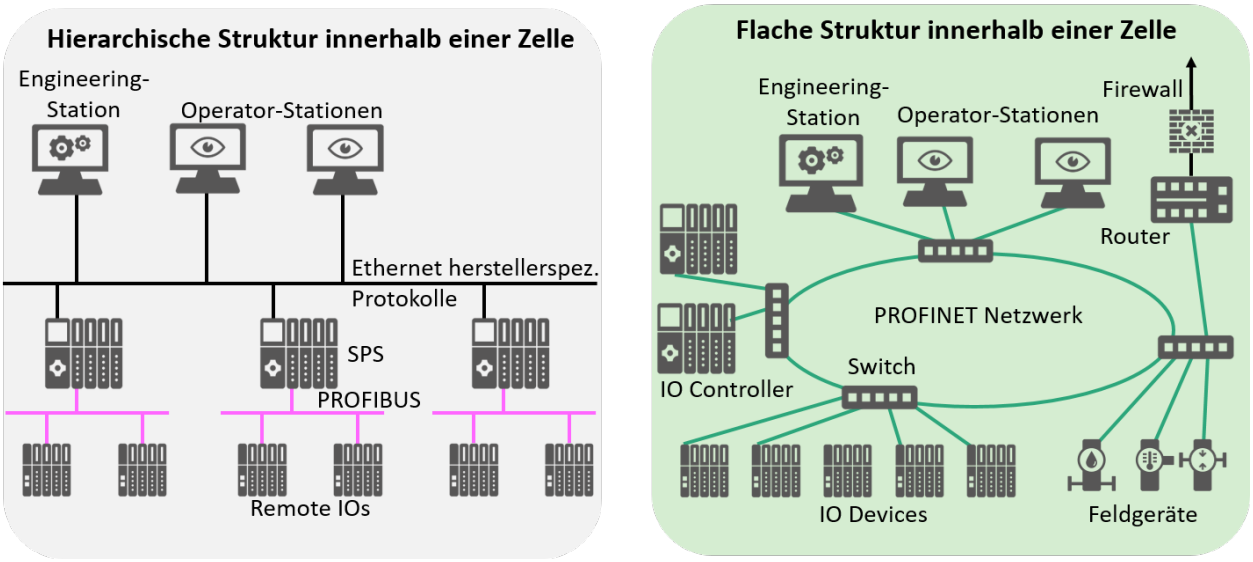

Abbildung 2: Wandel der Systemstrukturen

Abbildung 2 zeigt den Wandel der Systemstrukturen und die Auflösung von Hierarchien im Automatisierungsnetzwerk. Auf der linken Seite ist eine hierarchische Struktur abgebildet, wie man sie z. B. bei PROFIBUS-basierten Automatisierungssystemen findet. Engineering- und Operatorstationen sowie die speicherprogrammierbaren Steuerungen (SPS) kommunizieren über das Automatisierungsnetzwerk, häufig über ein herstellerspezifisches Protokoll. Die speicherprogrammierbaren Steuerungen kommunizieren mit den Remote IOs über PROFIBUS.Es kommen also auf unterschiedlichen Ebenen des Netzwerks unterschiedliche Protokolle zum Einsatz. Die rechte Seite des Bildes zeigt eine Struktur mit einem einheitlichen Protokoll innerhalb einer Produktionszelle, wie Sie für Industrial Ethernet-Systeme, wie z. B. PROFINET, verwendet wird. Alle Komponenten sind an ein Netzwerk angeschlossen und verwenden z. B. das PROFINET-Protokoll. Häufig werden mehrere solcher Zellen, wie in Abbildung 3 dargestellt, an ein überlagertes System angebunden (vertikale Integration).

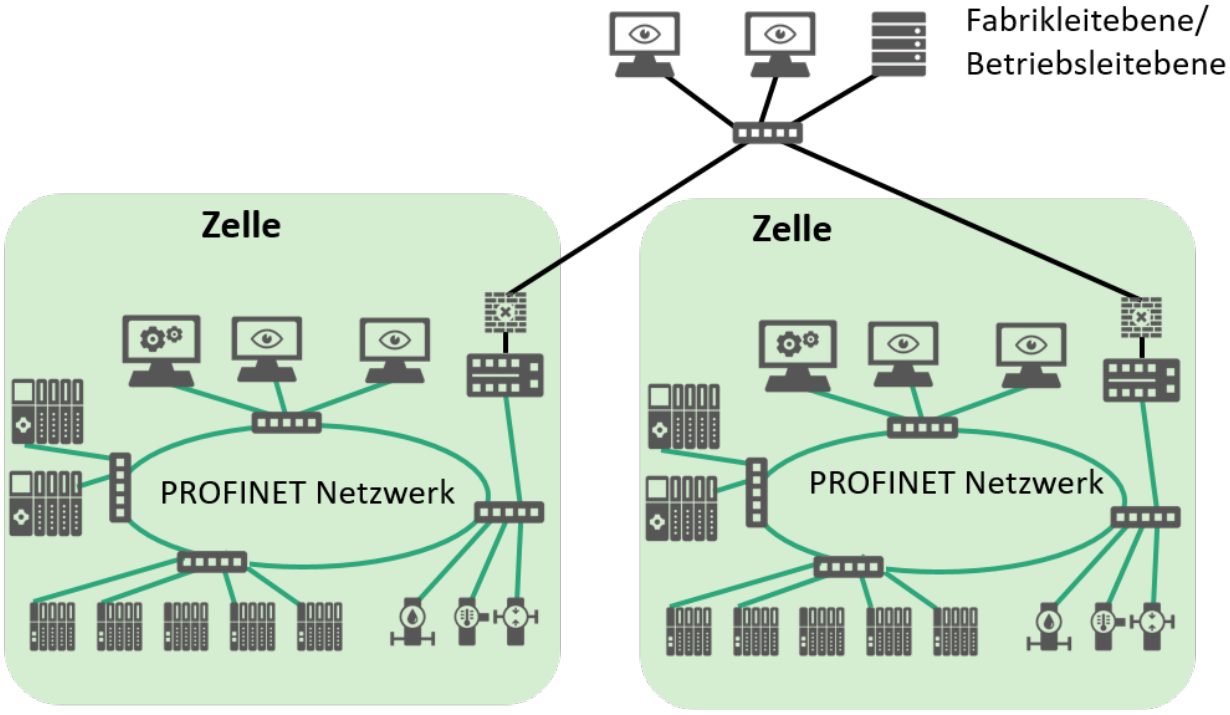

Abbildung 3: Anbindung mehrerer Zellen an ein überlagertes System

Künftig werden auch intelligente Feldgeräte (z, B. Tempertaturmessumformer, Druckmessumformer) direkt über PROFINET und auch mit überlagerten Systemen kommunizieren.

Die Systemstruktur mit einheitlichem Protokoll bietet eine direkte Erreichbarkeit aller Komponenten im System. Das Netzwerk-Management wird vereinfacht. Eine Anbindung an überlagerte Systeme, aber auch der direkte Zugang zu den Komponenten, ist einfach möglich. Allerdings stellt diese homogene Struktur auch Herausforderungen in Bezug auf die IT-Sicherheit. Alle Komponenten, auch IO Devices, aka Remote IOs und intelligente Feldgeräte sind für potentielle Angreifer direkt über das Netzwerk erreichbar. Dies stellt künftig zusätzliche Anforderungen an diese Geräte, für den Fall, dass Angreifer in das Automatisierungsnetzwerk eindringen oder den Fall, dass Innentäter auf das Netzwerk zugreifen.

2 Zweck dieses Dokuments

Dieses Dokument soll Komponentenherstellern, Systemherstellern und Anwendern einen ersten Einblick in die geplanten Protokollerweiterungen geben und die zu Grunde liegenden Überlegungen und Konzepte dokumentieren. Hierbei wird neben einer Absicherung der Kommunikation besonderer Wert auf den Erhalt der Echtzeiteigenschaften von PROFINET, einfache Handhabbarkeit, der Koexistenz mit bestehenden Installationen und die Wartbarkeit gelegt.

In einem zweiten Schritt sollen nach der Veröffentlichung und Diskussion mit Herstellern und Anwendern die entsprechenden Spezifikationsdokumente erstellt, bzw. bestehende Spezifikatio-

nen erweitert werden. Dabei können sich gegenüber diesem Dokument noch Änderungen ergeben. Daher hat dieses Dokument keinen normativen Charakter. Es sind ausschließlich die später freigegebenen Spezifikationsdokumente für eine Implementierung maßgebend.

3 Heutiger Stand PROFINET Security

Das IT-Sicherheitskonzept für PROFINET geht von einem Defense-in-Depth Ansatz aus [DHS2016]. Die Produktionsanlage wird dabei durch einen mehrstufigen Perimeter, u. a. Firewalls, gegen Angriffe, insbesondere von außen, geschützt [PNO2013]. Darüber hinaus ist innerhalb der Anlage eine weitere Absicherung durch Unterteilung in Zonen unter Einsatz von Firewalls möglich. Zusätzlich wird durch einen Security-Komponententest die Festigkeit der PROFINET-Komponenten gegen Überlastung in einem definierten Umfang sichergestellt [PNO2015]. Dieses Konzept wird durch organisatorische Maßnahmen in der Produktionsanlage im Rahmen eines Security Management-Systems [ISO_27001] unterstützt.

Die beschriebenen Schutzmaßnahmen entsprechen heute dem Stand der Technik. Dennoch werden künftig weiterreichende Schutzmaßnahmen erforderlich werden. Zum einen ist festzustellen, dass in zunehmendem Maße auch Innentäter Produktionsanlagen gefährden [BSI2013]. Gegen diesen Täterkreis sind die beschriebenen Schutzmaßnahmen, die im Schwerpunkt auf eine Abschottung setzen, nur eingeschränkt wirksam. Darüber hinaus fordern Anwenderkreise, z. B. aus der Prozessindustrie, einen weitergehenden Schutz [NE_153]. PROFIBUS & PROFINET International (PI) hat sich daher entschlossen, das PROFINET Protokoll künftig durch weitergehende Schutzmaßnahmen auf Protokollebene abzusichern. Security ist grundsätzlich nicht allein durch Maßnahmen in den Komponenten möglich, sondern immer nur durch eine Kombination von Anlagendesign und organisatorischen Maßnahmen möglich. Siehe hierzu auch [IEC_62443-2-1].

4 Vorgehensweise

Dieses Dokument beschreibt die Arbeitsergebnisse der PI-Arbeitsgruppe CB/WG 10 Security. In vorangehenden Arbeitsschritten wurde eine Bedrohungsanalyse für PROFINET-Netzwerke und der darin angebundenen Komponenten im Rahmen einer STRIDE-Analyse [SHO2014] durchgeführt. Daraus wurden Schutzziele abgeleitet und mögliche Schutzmaßnahmen betrachtet. Auf dieser Basis wurden dann technische Lösungsszenarien analysiert und an Hand der definierten Angriffsszenarien verifiziert. Eine Überprüfung aus Anwendersicht und eine Spiegelung an den grundlegenden Anforderungen der IEC 62443 soll nach Veröffentlichung dieses Dokumentes erfolgen. Auf Basis dieser Vorgehensweise wird nun in diesem Dokument das entstandene Konzept vorgestellt.

Noch ein Hinweis zur Benutzung von Begriffen: In Dokumenten, die sich mit der IT-Sicherheit oder Informationssicherheit befassen, werden verschiedene Begriffe verwendet. Die Norm [ISO_27001] spricht von Informationssicherheit, die deutsche Fassung der [DIN_IEC_62443-3-3] spricht von IT-Sicherheit. In anderen Dokumenten finden sich auch Begriffe wie OT-Security oder Cyber-Security. Da sich dieses Dokument im Wesentlichen auf die Normreihe IEC 62443 bezieht, wird der Begriff IT-Sicherheit verwendet.

5 Security Anforderungen an PROFINET

In Kapitel 1 wurde beschrieben, dass über die schon bestehenden Schutzmaßnahmen hinaus, ein weiterreichender Schutz von PROFINET auf Protokollebene erfolgen soll. Darüber hinaus ist aus [DIN_IEC_62443-3-3] bekannt, dass sich Schutzanforderungen in Schutz-Leveln beschreiben lassen, die durch die Kombination aus technischen und organisatorischen Maßnahmen erreichbar sind. Da dieses Dokument auf Protokollerweiterungen zur Erreichung von Schutzzielen fokussiert, ist eine Abgrenzung zwischen technischen und organisatorischen Maßnahmen erforderlich. Daher werden in diesem Kapitel zunächst die Schutzziele allgemein betrachtet. Danach erfolgt eine Abgrenzung, um die für die Protokollerweiterung notwendigen technischen Maßnahmen zu identifizieren. Abschließend fasst das Kapitel die weiteren, nicht-funktionalen Anforderungen zusammen, die sich nicht direkt aus Schutzzielen ableiten lassen.

5.1 Schutzziele / Schutzmaßnahmen

Die Norm [DIN_IEC_62443-3-3] und andere Quellen definieren die in Tabelle 1 genannten Schutzziele

Tabelle 1: Schutzziele der IT-Sicherheit

Schutzziel	Beschreibung	Relevanz für PROFINET
Integrität (engl. Integrity)	Eigenschaft eines Systems zum Schutz vor unerlaubter Datenmanipulation.	Hoch: Nachrichtenpakete dürfen nicht verfälscht werden, da sonst z. B. Aktoren ungewollt aktiviert oder falsche Messwerte erfasst werden.
Vertraulichkeit (engl. confidentiality)	Informationen sind nur für bestimmte Teilnehmer zugänglich und bleiben vor Dritten verborgen.	Gering: Das Schutzziel Vertraulichkeit von IO-Daten wird als gering eingeschätzt, sofern daraus keine Schlüsse auf Firmengeheimnisse (z. B. Rezepturen) gewonnen werden können.
Ressourcen-Verfügbarkeit (engl. availability)	Eigenschaft eines Systems, stets die geforderte Funktion zu erfüllen.	Hoch: Abhängig vom Produktionsprozess bestehen in der Regel hohe bis sehr hohe Verfügbarkeitsanforderungen. Dies gilt insbesondere für kritische Infrastrukturen.
Authentizität (engl. authenticity)	Eindeutige Identifikation einer Systemkomponente und deren Daten.	Hoch: Die Authentizität sichert, dass Daten einer Quelle eindeutig zugeordnet werden können. Die Komponenten müssen sich dafür „ausweisen“ und über eine fälschungssichere digitale Identität verfügen.
Autorisierung (engl. Authorization)	Die einem authentifizierten Nutzer (menschlicher Nutzer, Softwareprozess oder Gerät) zugewiesenen Berechtigungen die es diesem erlauben, die geforderten Aktionen im Automatisierungssystem durchzuführen, durchsetzen sowie die Verwendung dieser Berechtigungen überwachen.	Hoch: Durch die Nutzungskontrolle wird sichergestellt, dass nur autorisierte Nutzer Eingriffe am Automatisierungssystem vornehmen können.
Verbindlichkeit, Nicht-Abstreitbarkeit (engl. non-repudiation)	Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachende Person oder Stelle nachzuweisen.	Mittel: Betrifft Anlagen, bei denen eine Rückverfolgbarkeit von Nutzereingriffen erforderlich ist. Zum Beispiel Pharma-Anlagen, die nach FDA 21 CFR Part 11 [FDA2018] [TEB2015] betrieben werden.

Es ist zu erkennen, dass mit Ausnahme der Schutzziele Vertraulichkeit und Verbindlichkeit (Nicht Abstreitbarkeit), fast alle Schutzziele für PROFINET mit der Relevanz „hoch“ bewertet werden. Um diese Schutzziele zu erreichen, sind Schutzmaßnahmen erforderlich, die an verschiedenen Stellen und von verschiedenen Akteuren zu realisieren sind. Ziel dieses Papiers ist es, die Schutzmaßnahmen zu identifizieren, die durch Änderungen bzw. Ergänzungen am PROFINET Protokoll und möglicherweise auch an der kommunikationsrelevanten Hardware zu bewerkstelli-

gen sind. Andere Schutzmaßnahmen, z. B. organisatorische Schutzmaßnahmen, sollen nicht betrachtet werden, da diese nicht im Verantwortungsbereich der Hersteller bzw. von PI liegen und von diesen nicht beeinflusst werden können. Das folgende Kapitel befasst sich daher mit einer Zuordnung der Anforderungen zu den Akteuren, um die für dieses Papier relevanten Schutzmaßnahmen zu ermitteln.

5.2 Abgrenzung der Anforderungen und der Akteure

Abbildung 4 zeigt die in der Normreihe IEC 62443 beschriebenen Akteure im IT-Sicherheitsprozess und die zugeordneten Teile der Norm.

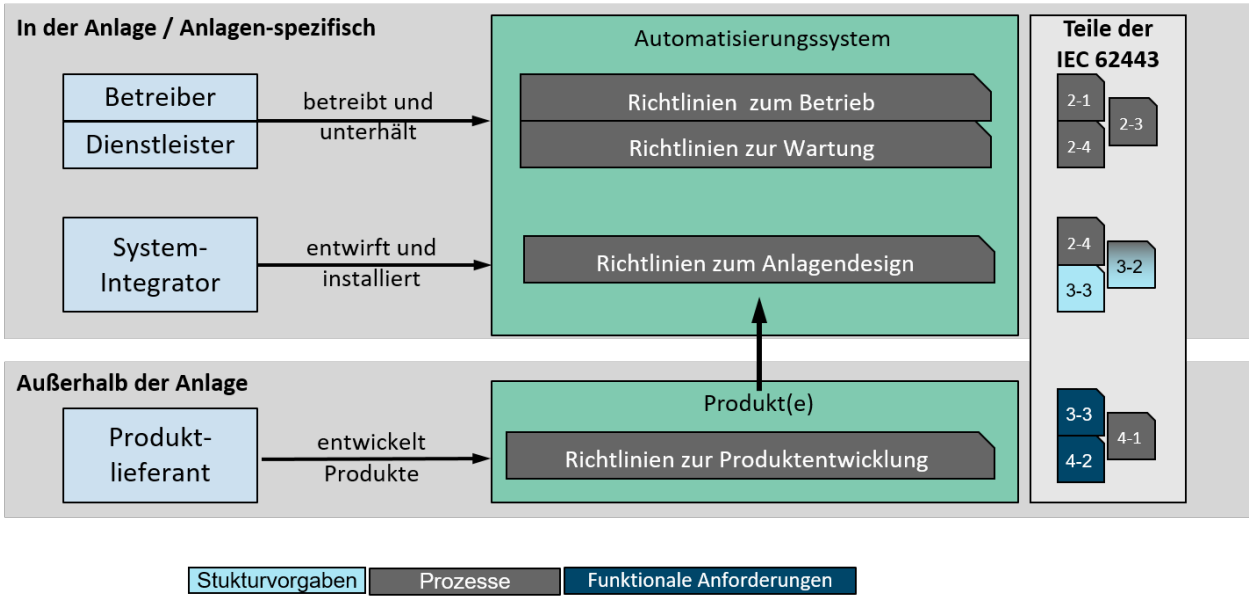

Abbildung 4: Akteure im Sicherheitsprozess und zugeordnete Teile der IEC 62443

Die Akteure sind: Betreiber, Dienstleister (zur Instandhaltung) Systemintegrator und Produktlieferant. Abbildung 4 zeigt diese mit den zugehörigen, wesentlichen Aktivtäten im Sicherheitsprozess dargestellt. Es ist zu erkennen, dass die Sicherstellung der IT-Sicherheit einer Produktionsanlage das koordinierte Zusammenspiel aller drei Akteure notwendig ist, um ein hohes Schutzniveau zu erreichen.

Der Betreiber der Anlage ist gemäß [IEC_62443-2-1] für die Organisation der IT-Sicherheitsprozesse verantwortlich. Hierzu gehört z. B die Schulung des Personals, das Aufstellen von Richtlinien, das Verwalten von Zugangsrechten, das Sicherstellen der physischen und umgebungsbezogenen Sicherheit sowie das Patch-Management gemäß [IEC_62443-2-3]. Eine vollständige Auflistung der Aufgaben findet sich in den zitierten Normen.

Das hier vorliegende Dokument betrachtet die Anforderungen, welche die Produktlieferanten zu erfüllen haben. Aus diesem Grund werden organisatorische und planerische Aspekte nicht weiter beleuchtet. Für diese Punkte sei auf [PNO2013] verwiesen.

Im folgenden Schritt sollen nun die Anforderungen für die Produktlieferanten noch weiter aufgeschlüsselt werden in allgemeine Anforderungen, die der Hersteller zu realisieren hat, und PROFINET protokollbezogene Anforderungen, die herstellerübergreifend gelten und von PI definiert werden.

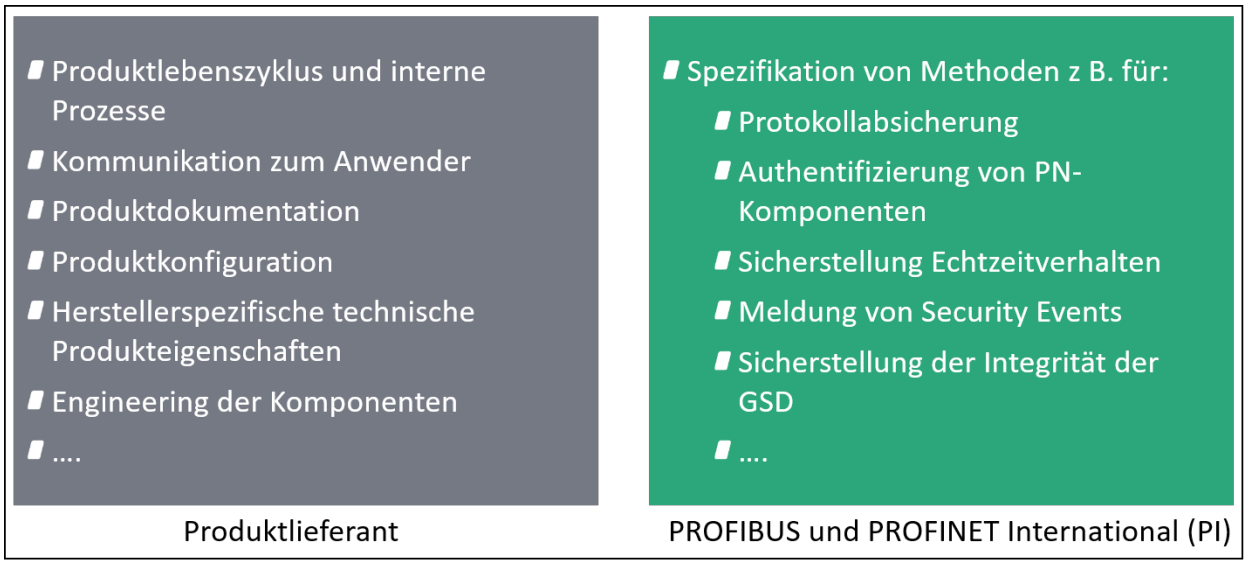

Abbildung 5: Abgrenzung Produktlieferant und PI, wesentliche Aufgaben

Abbildung 5 zeigt eine Abgrenzung der Verantwortlichkeiten [DIN_EN_62443-4-2] zwischen den einzelnen Herstellern und PI. Es ist zu erkennen, dass generische Anforderungen in Bezug auf die Entwicklungsprozesse, die Kommunikation zum Anwender, die Produktdokumentation, die Produktkonfiguration, etc. in der Verantwortung des Herstellers liegen. Hierzu gibt dieses Dokument lediglich Empfehlungen für die Hersteller. In der Verantwortlichkeit von PI liegt die herstellerübergreifende Funktionalität von PROFINET in Bezug auf Protokollerweiterungen zu Sicherstellung der in Tabelle 1 definierten Schutzziele. Hierauf wird sich das Dokument im Folgenden fokussieren.

5.3 Verbleibende Anforderungen an die PROFINET Protokollerweiterung

Wie die Abgrenzung im vorangehenden Kapitel 5.2 zeigt, sollen im Weiteren nur noch die Aspekte betrachtet werden, die herstellerübergreifend und PROFINET-Protokoll-bezogen betrachtet werden können. Tabelle 2 bildet die in Tabelle 1 definierten generischen Schutzziele auf PROFINET-spezifische Schutzziele ab. Die Anforderungen sind nach den Betriebsphasen eines PROFINET Systems (Konfiguration, Hochlauf, Betrieb) und nach den generischen Schutzzielen (Integrität, Verfügbarkeit, Vertraulichkeit, Autorisierung, Nicht-Abstreitbarkeit) sortiert.

Tabelle 2: PROFINET spezifische Schutzziele

lfd. Nr.	Betriebsphase	Generisches Schutzziel	Spezifisches Schutzziel	Priorität	Kommentar
1	Betrieb	Integrität	Der vom Anwender vorgegebene Betrieb (etablierte Application Relation, bestehend aus IO-Daten, Alarmen und Record Daten) eines IO Controllers mit einem projektierten IO Device darf nicht verfälscht oder verändert werden.	hoch	Verhinderung bzw. Erkennen einer Manipulation der Daten, Unterdrückung von Alarmen. Schutz vor unberechtigtem Zugang zu den Komponenten.
2	Betrieb	Integrität / Authentizität / Autorisierung	Nicht autorisierter Zugriff eines IO-Supervisors bzw. Manipulation der vom IO Supervisor übertragenen Daten ist zu verhindern.	hoch	Ein IO Supervisor kann im laufenden Betrieb die Konfiguration des IO Devices ändern, azyklische Daten lesen und schreiben, Eingänge lesen und auch Ausgänge setzen.
3	Betrieb	Integrität	Die Integrität der Uhrzeit-Synchronisation ist zu gewährleisten.	mittel	Verfälschungen der Uhrzeit können bei der Signalfolgeerfassung (Sequence of Events) zu fehlerhaften Informationen führen.
4	Betrieb	Integrität	Die Integrität der PROFINET IRT-Clock-Synchronisation bzw. künftig der TSN Synchronisation ist zu gewährleisten.	hoch	Bei Verletzung der Integrität ist das Echtzeitverhalten des Systems nicht gewährleistet.
5	Betrieb	Verfügbarkeit	Die Verfügbarkeit einer bestehenden Kommunikationsbeziehung zwischen IO Controller und IO Device (etablierte Application Relation, bestehend aus IO-Daten, Alarmen und Record Daten) ist sicherzustellen.	hoch	Festigkeit gegen Störeinflüsse (z. B. Überlastung / Denial of Service oder manipulierte Datenpakete) ist in bestimmten Grenzen sicherzustellen. Z. B. durch Priorisierung der Echtzeitkommunikation in der Bearbeitung oder durch Deaktivierung nicht benötigter Services. Hinweis: Teil dieser Maßnahmen liegt beim Implementierer.
6	Betrieb	Verfügbarkeit	Die Verfügbarkeit von Redundanzfunktionen, z.B. Medienredundanz ist zu gewährleisten.	mittel	Das Schutzkonzept muss auch redundante Kommunikationsnetzwerke umfassen.

lfd. Nr.	Betriebsphase	Generisches Schutzziel	Spezifisches Schutzziel	Priorität	Kommentar
8	Betrieb	Vertraulichkeit	Die Vertraulichkeit der Device und Modulidentifikation (Seriennummer, Bestellnummer, Hersteller.	gering	Information kann zur Vorbereitung eines Angriffs genutzt werden. Abwägung zwischen Notwendigkeit der Netzwerkdiagnose und Schutz gegen Ausspähen ist zu treffen.
9	Betrieb	Vertraulichkeit	Die Netzwerktopologie darf nicht ausgelesen werden können.	gering	Abwägung zwischen Notwendigkeit der Netzwerkdiagnose und dem Schutz gegen Ausspähen des Netzwerkes.
10	Betrieb	Vertraulichkeit	Die Vertraulichkeit der Uhrzeitinformation (SoE, IRT, TSN) ist zu gewährleisten.	Keine Anforderung.	----
11	Betrieb	Verfügbarkeit Vertraulichkeit Integrität	Die Verfügbarkeit, Vertraulichkeit und Integrität von Diagnosedaten, die von PROFINET-Komponenten über das Simple Network Management Protokoll (SNMP) bereitgestellt werden, ist sicherzustellen.	gering	Das Interface dient zur Anbindung von Netzwerk-Management-Systemen und ist für den Echtzeitbetrieb nicht relevant. Daher Priorität gering.
12	Hochlauf	Integrität / Authentizität	Die Identität eines PROFINET Gerätes (Stationsname, IP-Adresse, Subnetzmaske) ist sicherzustellen. (DCP Merkmale)	gering	Sichere Identifikation des Gerätes wird künftig über kryptografisch gesichertes Verfahren sichergestellt. Daher wird eine kryptografische Absicherung des bisher verwendeten DCP-Verfahrens als nicht notwendig erachtet.
13	Hochlauf	Integrität	Die Integrität der Konfigurationsdaten, die von einem IO Controller zu einem IO Device übertragen werden ist sicherzustellen.	hoch	Durch Verfälschen der Konfigurationsdaten könnten von einem IO Device ungültige Daten zum IO Controller übertragen werden, ohne dass dieser dies feststellen kann.

lfd. Nr.	Betriebsphase	Generisches Schutzziel	Spezifisches Schutzziel	Priorität	Kommentar
15	Hochlauf	Integrität	Die Integrität der IP-Netzwerkkonfiguration (DCP) vor Aufbau einer Kommunikationsbeziehung ist sicherzustellen.	gering	Durch einen Angriff während der Netzwerkkonfiguration kann Verkehr umgeleitet werden. Priorität ist auf gering gesetzt, weil durch eine Ende-zu-Ende Sicherung Angriffe zu einem späteren Zeitpunkt erkannt werden.
16	Hochlauf	Integrität	Die Integrität der PROFINET Netzwerkkonfiguration (NoS) vor Aufbau einer Kommunikationsbeziehung ist sicherzustellen.	gering	Durch einen Angriff während der Netzwerkkonfiguration kann Verkehr umgeleitet werden. Priorität ist auf gering gesetzt, weil durch eine Ende-zu-Ende Sicherung Angriffe zu einem späteren Zeitpunkt erkannt werden.
17	Hochlauf	Verfügbarkeit	Die Verfügbarkeit einer etablierten Kommunikationsbeziehung muss nach einem Netzausfall sichergestellt sein.	hoch	Automatischer Wiederanlauf nach Netzausfall.
18	Hochlauf	Vertraulichkeit	Die Vertraulichkeit der Konfigurationsdaten, die von einem IO Controller zu einem IO Device übertragen werden ist sicherzustellen.	mittel	Aus den Konfigurationsdaten kann ein angreifende Person Informationen über die Zusammensetzung der IO Daten gewinnen und dies für einen Angriff ausnutzen.
19	Hochlauf	Vertraulichkeit	Die Vertraulichkeit der IP- Netzwerkkonfiguration vor Aufbau einer Kommunikationsbeziehung ist sicherzustellen.	kein Schutzziel	Es gibt keine kritischen Informationen in diesem Punkt, die der Vertraulichkeit bedürfen.
20	ohne Zuordnung	Vertraulichkeit	Die Vertraulichkeit der PROFINET Netzwerkkonfiguration (NoS) vor Aufbau einer Kommunikationsbeziehung ist sicherzustellen.	kein Schutzziel	---
21	ohne Zuordnung	Authentizität	Ein IO Device darf nicht von einem anderen IO Controller kontrolliert werden, als in der Planung vorgesehen.	hoch	Verhindern eines Man-in-the-Middle-Angriffs.

lfd. Nr.	Betriebsphase	Generisches Schutzziel	Spezifisches Schutzziel	Priorität	Kommentar
23	Ohne Zuordnung	Vertraulichkeit	Die Vertraulichkeit privater Schlüssel bei evtl. eingesetzten kryptografischen Verfahren ist zu gewährleisten.	hoch	Bei Bruch der Vertraulichkeit könnten Netzwerkteilnehmer eine falsche Identität vorgaukeln.
24	Engineering	Integrität / Authentizität	Die Integrität und Authentizität der Daten in der Gerätestammdatei (GSD Datei) ist sicherzustellen.	hoch	Durch Verfälschung der GSD können von einem IO Device ungültige Daten an den IO Controller gesendet werden, ohne dass dies der IO Controller bemerken kann. Gilt auch für die Gegenrichtung.
25	Engineering	Vertraulichkeit	Die Vertraulichkeit der Daten in der Gerätestammdatei (GSD) ist sicherzustellen.	kein Schutzziel	---
26	Wartung	Integrität	Die Integrität der Firmware in einem IO Controller ist zu gewährleisten.	hoch	Ist herstellerspezifisch zu lösen.
27	Wartung	Integrität	Die Integrität der Firmware in einem IO Device ist zu gewährleisten.	hoch	Ist herstellerspezifisch zu lösen.

Die PROFINET-spezifischen Schutzziele in Tabelle 2 sind noch durch weitere Anforderungen zu ergänzen, die sich nicht den generischen Schutzzielen zuordnen lassen. Hier sind zu nennen:

- Das Echtzeitverhalten des PROFINET Systems ist auch bei Realisierung von Schutzmaßnahmen sicherzustellen. Anmerkung: Da die geplanten kryptografischen Maßnahmen in den PROFINET Geräten zusätzlichen Rechenaufwand verursachen, ist davon auszugehen, dass die Security-Maßnahmen, bei gleicher Hardwareausstattung, einen Einfluss auf die Zykluszeit haben können.
- Die einzusetzenden Schutzmaßnahmen müssen dem aktuellen Stand der Technik entsprechen.
- Die einzusetzenden Schutzmaßnahmen sollten so weit wie möglich über ein Softwareupdate aktualisierbar sein, sofern diese nicht mehr dem Stand der Technik entsprechen.
- Das Security-Konzept sollte wirtschaftlichen Überlegungen folgen. Hierunter fallen: Kosten für die Implementierung, Kosten für die Wartung, Zeit bis zum Markteintritt.
- Die Koexistenz von PROFINET-Komponenten mit und ohne Schutzmaßnahmen in einem System muss möglich sein. Dabei darf ein Angreifer einen ungesicherten Betrieb nicht erzwingen können.
- Der Tausch von defekten Geräten im laufenden Betrieb ohne Notwendigkeit ein Engineering-Werkzeug zu nutzen, muss weiterhin möglich sein.

- Eine Anlage muss nach einem Spannungsausfall ohne Verbindung zum Internet anlaufen können (Schwarzstartfähigkeit).

- Während des Betriebs sollten keine zusätzlichen fest installierten Systemkomponenten erforderlich sein. Zusätzliche Komponenten für die Inbetriebnahme des Systems (PKI, Validierung von Zertifikaten) können erforderlich sein.

- Die vorhandenen PROFINET Profile, wie z. B. PROFIsafe, müssen uneingeschränkt anwendbar bleiben.

- Die zu definierende IT-Security-Lösung sollte skalierbar sein, um sich an Anforderungen unterschiedlicher Anwender anpassen zu können.

- Die zu definierende Lösung muss die installierte Basis berücksichtigen. Eine Kompatibilität zu bestehenden Installationen ist sicherzustellen. Das Zufügen von Komponenten, die mit aktivierten IT-Sicherheitsfeatures ausgestattet sind, darf den Betrieb einer Bestandsanlage nicht gefährden.

Auf Basis dieser Anforderungen und der zugehörigen Priorisierung werden im folgenden Kapitel entsprechende Schutzmaßnahmen abgeleitet.

6 Beschreibung des Konzeptes für eine PROFINET Protokoll Security

Das folgende Kapitel beschreibt die grundlegenden Konzepte, mit denen ein PROFINET System künftig abgesichert werden soll. Zum heutigen Zeitpunkt stellt dieses Konzept zunächst einen Arbeitsansatz dar, der sich im Verlauf der weiteren technischen Evaluierung noch ändern kann. In Kapitel 6.1 wird zunächst ein einfaches PROFINET-System definiert, an dem die Betrachtungen durchgeführt werden sollen. Kapitel 6.2 definiert dann Security-Klassen, da nicht alle Security-Anforderungen für alle System gelten. Kapitel 6.3 zeigt eine Migrationsstrategie für Bestandsanlagen auf. Kapitel 6.4 beschreibt die grundlegenden Konzepte. In Kapitel 6.5 folgt dann eine Beschreibung der gewählten Schutzmaßnahmen auf Basis so genannter Building-Blocks. Das Kapitel wird abgeschlossen mit ergänzenden Maßnahmen für Hersteller und Betreiber.

6.1 Betrachtungsgegenstand

Für die weiteren Betrachtungen wird zunächst eine PROFINET-Anlage definiert, die in Abbildung 6 dargestellt ist. Die Anlage wird im Rahmen des in Kapitel 3 beschriebenen Zellenschutzkonzeptes betrieben.

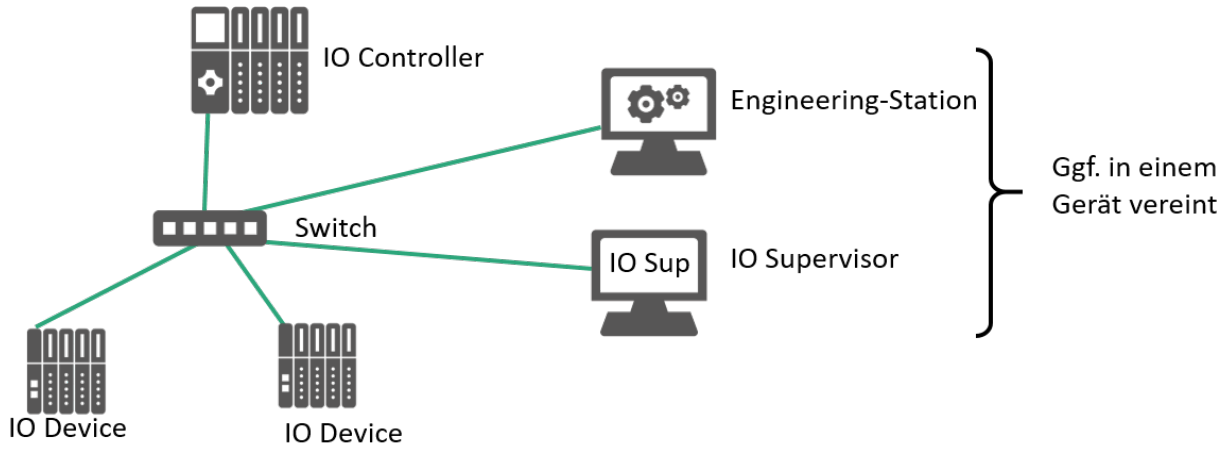

Abbildung 6: PROFINET-Beispielanlage

Die Beispielanlage besteht aus einem IO Controller, dem zwei IO Devices zugeordnet sind sowie einem Switch. Eine Engineering-Station wird für die Konfiguration des Systems verwendet. Zusätzlich ist ein IO Supervisor an das System angebunden. Für beide Systeme existieren menschliche Nutzer, denen bei Bedarf entsprechende Nutzerrollen zugewiesen werden können. Hierbei kann es sich z. B. um ein zusätzliches Werkzeug zur Inbetriebnahme oder zur Diagnose des Bussystems handeln. In vielen Fällen übernimmt das Engineering Werkzeug gleichzeitig die Funktion des IO Supervisors. Obwohl ein separater Switch bei Systemen evtl. nicht erforderlich ist, weil die Komponenten über integrierte Switches verfügen, wird dieser dennoch zusätzlich mit betrachtet. Dies ist erforderlich, da der Switch ggf. auch Konfigurationsdaten, z. B. in Bezug auf virtuelle Netzwerke, enthalten kann. In der Beispielanlage wird ein herkömmlicher Switch ohne PN-Funktionalität eingesetzt.

Zwischen den Komponenten der in Abbildung 6 gezeigten Anlagen bestehen Kommunikationsbeziehungen. Diese werden in Abbildung 7 dargestellt.

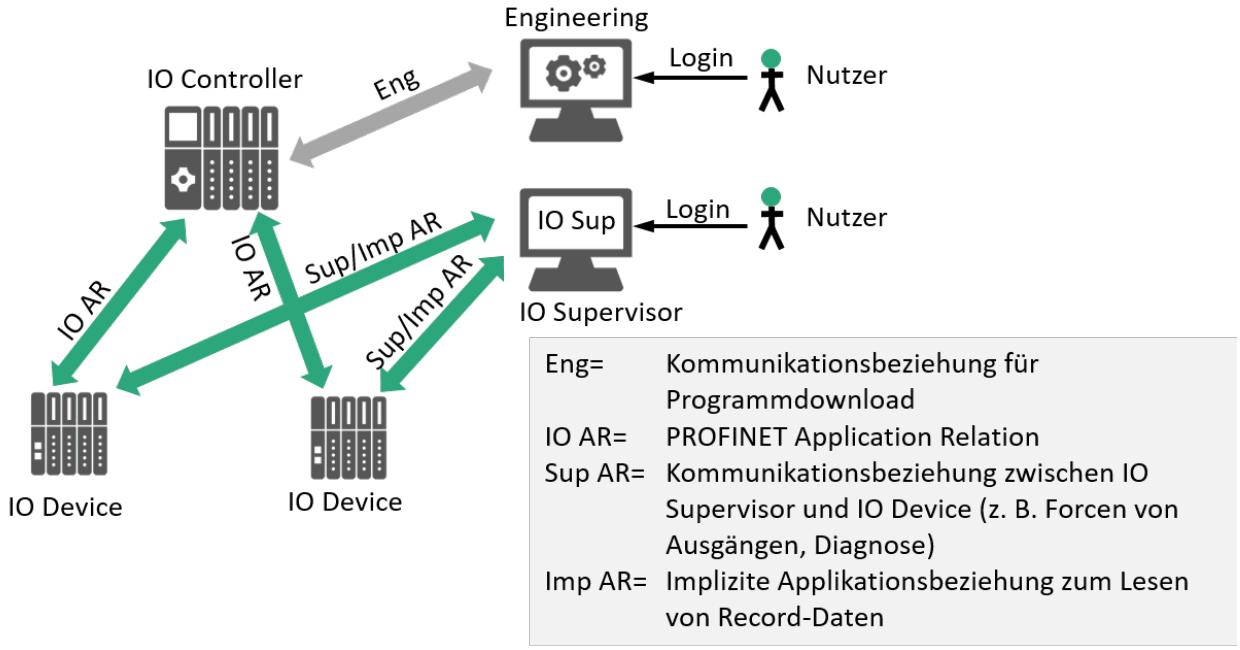

Abbildung 7: Kommunikationsbeziehungen in der Beispielanlage

Aus Sicht von PROFINET sind zunächst einmal die PROFINET IO Application Relations (IO AR) von Interesse. Über die IO AR tauschen der IO Controller und die IO Devices zyklische und azyklische Daten sowie Alarme aus. Parallel dazu kann ein IO Supervisor eine Kommunikationsbeziehung zu den IO Devices (Sup AR) aufbauen um z. B. eine Diagnose durchzuführen, IO-Daten zu lesen oder IOs für Inbetriebnahmezwecke manuell zu setzen.

Neben diesen PROFINET-spezifischen Kommunikationsbeziehungen hat die Engineering-Station eine Kommunikationsbeziehung zum IO Controller, um diesen z. B. mit den Steuerungsprogrammen zu laden (im Bild als „Eng dargestellt). Sowohl für die Engineering-Station, als auch für den IO Supervisor werden in der Regel Zugangsdaten (Logins) benötigt, um die Stationen nutzen zu können.

Bei der folgenden Beschreibung von Maßnahmen für die Absicherung eines PROFINET Systems werden die erläuterten Assets und die zugehörigen Kommunikationsbeziehungen zu Grunde gelegt. Die IO ARs und Sup ARs liegen dabei im Fokus dieses Dokumentes. Die Verbindung zwischen Engineering und IO Controller (Eng) wird mit betrachtet, liegt aber in der Verantwortung der Hersteller, genauso wie andere Tools oder Web-Schnittstellen.

6.2 Definition von Security-Klassen

Die Analyse der PROFINET Schutzziele in Tabelle 2 zeigt, dass die Schutzziele unterschiedlich priorisiert wurden. Dies gilt insbesondere für den Aspekt der Vertraulichkeit. Das Schutzziel der Vertraulichkeit ist nur in bestimmten Anwendungsfällen relevant, bei denen aus dem Mitlesen der IO-Daten auf Betriebsgeheimnisse geschlossen werden kann. Aus [RUN2014a] ist bekannt, dass der Rechenzeitaufwand für die Sicherstellung der Vertraulichkeit (Verschlüsselung) deutlich höher ist als für die Sicherstellung der Integrität, z. B. durch eine kryptografische Prüfsumme. Weiterhin ist davon auszugehen, dass der überwiegende Teil der Anwendungen keine Vertraulichkeit der zyklischen IO Daten als Schutzziel hat. Aus diesem Grund werden drei Security-Klassen gemäß Tabelle 3 definiert.

Tabelle 3: PROFINET Security-Klassen für IT-Security

Security Klasse	Name der Security-Klasse	Definition	Typisches Einsatzgebiet
1	Robustness	Heutiger Stand der der PN-Security gemäß Kapitel 3 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. Es ist noch zu diskutieren, ob diese Klasse eingeführt werden soll.
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 nach außen. 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 der Kommunikationsbeziehungen gewährleistet.	Anlage gemäß Security-Klasse 2 bei der aus den IO-Daten des Systems auf Firmengeheimnisse geschlossen werden kann.

Tabelle 3 zeigt in der rechten Spalte typische Einsatzgebiete für die drei Security-Klassen. Die

Security Klasse 1 stellt kurzfristige inkrementelle Verbesserungen gegenüber dem aktuellen Stand der PN-Security gemäß Kapitel 3 zur Verfügung.

Die **Security-Klasse 2** ist für Anlagen gedacht, bei denen ein erhöhtes Kommunikationsaufkommen zu Bereichen außerhalb der Anlage auftritt oder bei denen der Zugang zum System weniger gut überwacht werden kann. Diese Klasse kommt zum Einsatz, sofern der Betreiber höhere IT-Sicherheitsanforderungen an die Kommunikation über PROFINET hat. Die zyklischen Dienste sind in dieser Betriebsart gegen unautorisierte Modifikationen geschützt. Gleichzeitig ist die Vertrauenswürdigkeit sowie die Integrität und Authentizität der azyklischen Dienste gesichert.

Die **Security-Klasse 3** stellt Integrität, Authentizität und Vertraulichkeit aller Dienste sicher. Es wird davon ausgegangen, dass die Security-Klasse 3 nur in den Fällen zur Anwendung kommt, wo über das Mitlesen von zyklischen IO-Daten auf Betriebsgeheimnisse geschlossen werden kann. Hinweis: Die azyklischen Kommunikationsdienste der Security-Klasse 2 bieten eine Alternative für die Übertragung vertraulicher Daten, wie z. B. Rezepte.

Die Mehrzahl der Anwendungen wird auf Basis der Security-Klassen 1 und 2 arbeiten können.

6.3 Migrationsstrategie

Bestehende Anlagen (Altanlagen) sind in der Regel gemäß der Beschreibung in Kapitel 3 aufgebaut. Die IT-Sicherheit wird hier über das Defense in Depth Konzept sichergestellt. Dies sieht in der Regel eine Abschottung der Anlage nach außen, die Segmentierung des Produktionsnetzes, ein Zugriffschutz und weitere Maßnahmen vor.

Für die Einführung der Security-Klasse 2 wird Hard- und Software benötigt, welche die Anforderungen für die Bereitstellung der zusätzlichen Sicherheitsfunktionen erfüllt. So werden die Baugruppen in der Regel über eine höhere Rechenleistung verfügen müssen. Es ist daher davon auszugehen, dass eine Nachrüstung von Bestandsanlagen durch Software-Updates nicht in allen Fällen möglich sein wird. Ein Umstieg auf die Security-Klasse 2 oder 3 wird daher in der Regel bei Anlagenerneuerungen oder Anlagenerweiterungen erfolgen. Da ein Mischbetrieb von Komponenten aller Security-Klassen möglich sein wird, können in einem Netzwerk alte Anlagenteile mit Security-Klasse 1 parallel zu Anlagenteilen mit Security-Klasse 2 oder 3 betrieben werden.

6.4 Grundlegende Beschreibung der wesentlichen Konzepte

Aus den Schutzzielen in Tabelle 2 lassen sich, unter Berücksichtigung der durchgeführten weiteren Analysen und den zu Grunde liegenden Prioritäten, die folgenden Schutzmaßnahmen für ein PROFINET-System ableiten:

1. Sicherstellung der Authentizität der PROFINET-Teilnehmer durch eine kryptografisch gesicherte digitale Identität, z. B. in Form von Zertifikaten. Die Möglichkeit einer sicheren Speicherung dieser Identität, z. B. in einer besonders gesicherten Hardware-Komponente im jeweiligen Teilnehmer sollte in dem Konzept enthalten sein. Siehe hierzu [SPE2013] [RUN2014b].

2. Sicherstellung der Integrität der Kommunikation durch kryptografische Maßnahmen, z. B. kryptografische Prüfsummen. Diese Sicherung muss alle Kommunikationskanäle des PROFINET-Teilnehmers bestehend aus IP-Kommunikation, PROFINET-Echtzeitkommunikation und Kommunikation für das Netzwerkmanagement umfassen.

3. Sicherstellung des Systemhochlaufs und der Zuordnung von Komponenten, z. B. von IO Devices zu IO Controllern und Engineering-Werkzeugen, durch kryptografische Maßnahmen. Dies gilt auch für einen Systemhochlauf nach einem Verbindungsabbruch.

4. Meldung von Security-relevanten Ereignissen, die durch PROFINET-Devices erkannt werden können. Z. B. durch zusätzliche PROFINET-IT-Sicherheitsalarme.

5. Sicherstellung der Vertraulichkeit azyklischer Daten und der Konfigurationsdaten. Zusätzlich Sicherstellung der Vertraulichkeit für zyklische Daten als **optionale** Funktion in Security-Klasse 3. Hierbei ist zu beachten, dass der Rechenaufwand für eine vertrauliche Kommunikation (Verschlüsselung) signifikant höher ist, als ein einfacher Integritätsschutz, z. B. durch eine kryptografische Prüfsumme. Messwerte hierzu finden sich in [RUN2014b].

6. Gewährleistung von Mindestanforderungen gegen Überlastungsangriffe (Denial of Service). Dieser Aspekt wurde bereits gemäß [PNO2015] im Rahmen von Netload-Tests realisiert. Im Rahmen der weiteren Arbeiten ist zu diskutieren, ob eine höhere Mindestanforderung als Netzlastklasse I gefordert wird.

7. Schutz der Integrität und Authentizität von Gerätestammdateien (GSD)

Weitergehende Anforderungen, z. B. die Integritätsprüfung von GSDs in einem Engineering-Werkzeug, sichere Firmware und ein sicherer Entwicklungsprozess sind, gemäß der in Kapitel 5.2 durchgeführten Abgrenzung, herstellerspezifisch zu implementieren.

Im Weiteren werden die grundlegenden Mechanismen beschrieben, die zum Aufbau einer gesicherten Kommunikation in einem PROFINET-System führen.

6.4.1 Nutzung von Zertifikaten

Das folgende Kapitel befasst sich mit der Verwendung von Zertifikaten im Rahmen des PN-Security Konzeptes.

Abbildung 8: Komponenten mit Zertifikaten

Abbildung 8 zeigt links im Bild den Auslieferungszustand einer IO Komponenten (IO Device, IO Controller), wie es vom Hersteller geliefert wird. In dieser Komponente sollte ein Herstellerzertifikat, im Bild rot dargestellt, abgelegt werden. Dies gestattet es dem Betreiber die Echtheit des Gerätes zu prüfen. So wird ein Schutz gegen unautorisierten Nachbau ermöglicht. Bei der Übernahme der Komponente durch den Betreiber muss dieser ein eigenes Betreiberzertifikat, im Bild grün dargestellt, ergänzen. Gleichzeitig kann der Betreiber das Gerät über sein Betreiberzertifikat in seine eigene Public-Key-Infrastruktur (PKI) einbinden.

Das Zertifikat enthält den öffentlichen Schlüssel der Komponente. Der Nachweis der Authentizität der öffentlichen Schlüssel erfolgt, wie in Abbildung 9 dargestellt, über die Zertifikate und digitale Signaturen. In diesem Fall sind im Bild die Betreiberzertifikate dargestellt. Die Verwaltung der Schlüssel und der Herstellerzertifikate kann über ein Public-Key-Schlüsselmanagement erfolgen, welches z. B. in das Engineering-Werkzeug integriert werden kann.

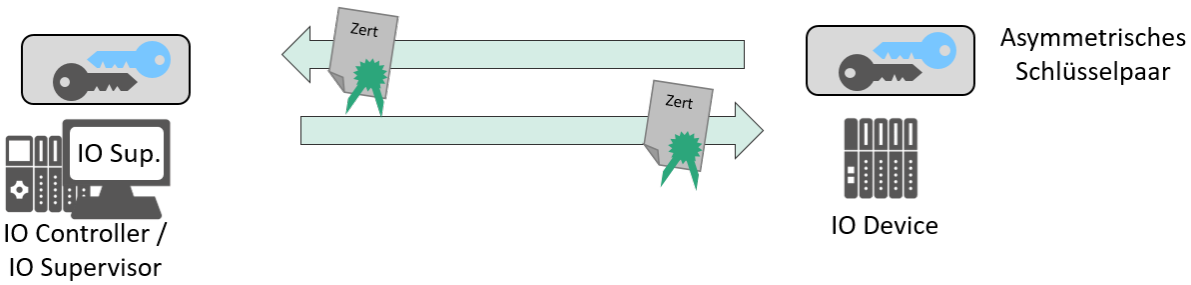

Abbildung 9: Authentizitätsnachweis der öffentlichen Schlüssel über Zertifikate

Auf Basis dieser Authentisierung werden dann nachfolgend die symmetrischen Schlüssel erstellt und ausgetauscht.

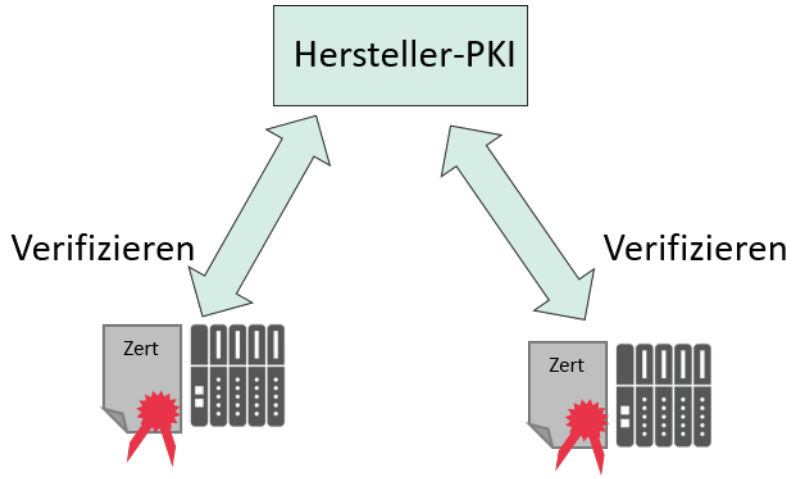

Abbildung 10: Echtheitsprüfung der Geräte mittels Herstellerzertifikat

Wie in Abbildung 10 zu erkennen ist, kann die Originalität und Gültigkeit von Herstellerzertifikaten geprüft werden. Diese Prüfung ermöglicht im Bedarfsfall einen Rückruf von Zertifikaten (Revokation) durch den Hersteller. Es ist zurzeit in Diskussion, ob PROFIBUS & PROFINET International (PI) die Mechanismen zur Gültigkeitsprüfung definieren wird.

6.4.2 Systemhochlauf

Der Hochlauf eines abgesicherten PROFINET-Systems erfolgt, wie in Abbildung 11 dargestellt, in zwei Phasen.

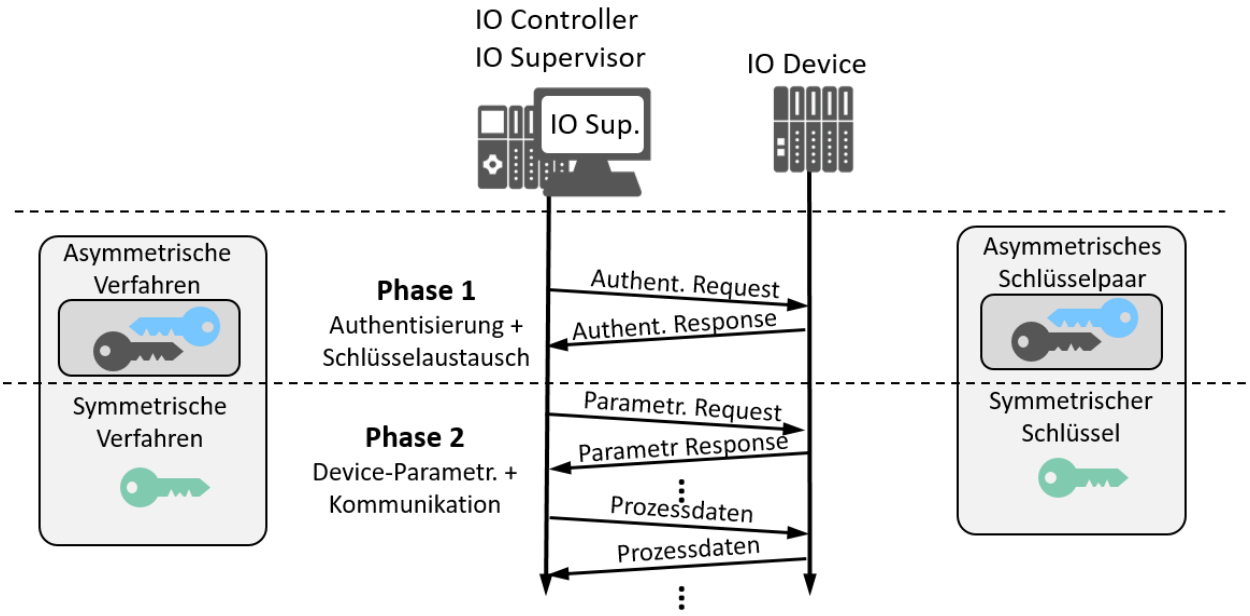

Abbildung 11: Systemhochlauf in zwei Phasen

In der Phase 1 erfolgt zunächst unter Nutzung eines private/public-Key-Verfahrens eine gegenseitige Authentifizierung sowie Schlüsselaustausch zwischen dem IO Controller, bzw. dem IO Supervisor und dem IO Device. Dazu tauschen die Teilnehmer Ihre öffentlichen Schlüssel (blaue Farbe im Bild) aus und handeln einen gemeinsamen symmetrischen Schlüssel (grüne Farbe im Bild) aus, unter dessen Nutzung dann die weitere Kommunikation (Phase 2) erfolgt. Die Umschaltung auf ein symmetrisches Verfahren ist sinnvoll, weil dieses Verfahren weniger Rechenleistung erfordert, als ein asymmetrisches Verfahren. Bei einem Wiederanlauf, z. B. bei Unterbrechung der Kommunikation, wird der beschriebene Ablauf erneut durchlaufen.

6.4.3 Absicherung der zyklischen Nachrichten

Die Absicherung der PROFINET Datenpakete erfolgt über einen Message Authentication Code. Hierbei wird über das Datenpaket eine kryptografische Prüfsumme berechnet. Durch diese Maßnahme können die Integrität und die Authentizität des Nachrichtenpaketes vom Empfänger geprüft werden. In die Berechnung des MACs geht neben einem Sequenzzähler auch der bereits beschriebene symmetrische Schlüssel ein. Der Vorteil dieses Verfahrens ist die relativ einfache Berechnung des MAC. In [RUN2014a] wird die Eignung verschiedener Message Authentication Codes für Datenpakete mit einer für PROFINET typischen Länge evaluiert. In dieser Untersuchung hat sich der HMAC-SHA 256 Algorithmus [NIST198] als performanteste Lösung herausgestellt. Eine finale Auswahl eines MAC-Algorithmus ist allerdings noch nicht erfolgt. Diese Festlegung wird nach einer weiteren Diskussion und Prüfung erfolgen. Es ist davon auszugehen, dass der Algorithmus während des Verbindungsaufbaus ausgehandelt wird, um künftig auf leistungsfähigere Algorithmen umsteigen zu können.

Der Inhalt des Datenpaketes ist weiterhin lesbar. Bei Bedarf kann zusätzlich noch optional eine Verschlüsselung erfolgen um das Schutzziel der Vertraulichkeit zu berücksichtigen.

6.5 Beschreibung der Maßnahmen für PROFINET

Das in Kapitel 6.4 skizzierte IT-Security-Konzept wird auf einer Reihe von Bausteinen aufbauen, die in die in Tabelle 4 beschriebenen Kategorien unterteilt sind.

Tabelle 4: Bausteinkategorien für PROFINET Security

Kategorie	Beschreibung
Basics	Grundlegende Security Maßnahmen
RTA/RTC	Absicherung der zyklischen Layer-2-PROFINET-Kommunikation und der azyklischen Layer-2-basierten Alarmmechanismen.
AR/RPC	Nicht zyklische Kommunikation, um eine Verbindung von einem IO Controller zu einem IO Device aufzubauen.
Trust	Alle Funktionen, die erforderlich sind, um den Kommunikationspartner zu identifizieren und eine Vertrauensbeziehung aufzubauen.
Supervisor	Absicherung der Verbindung zu Konfigurations- bzw. Diagnosewerkzeugen, die über einen PROFINET Lesezugriff oder das Lesen und Schreiben von IO Parametern auf ein IO Device zugreifen oder wie es z. B. ein Diagnosewerkzeug über eine implizite AR beim Lesen von Diagnosedaten tut.
GSD	Schutz der Gerätebeschreibungsdatei, die mit einem IO Device geliefert wird.
Test	Tests, die während der Zertifizierung der PROFINET-Geräte durchzuführen sind um Erfüllung der Security-Anforderungen gemäß den definierten Security-Klassen, Robustheit und Interoperabilität zu gewährleisten.
Hersteller	Aufgaben des Herstellers. Diese Aufgaben werden aus Gründen der Vollständigkeit genannt, sind aber dem Hersteller zugeordnet.
Dokumentation	Bereitstellung Security-relevanter Informationen für Betreiber.

Die folgenden Unterkapitel beschreiben nun die Inhalte der Bausteine.

6.5.1 Baustein Basics

Dieses Kapitel beschreibt grundlegende Maßnahmen zur Absicherung der PROFINET Kommunikation. Die Maßnahmen sind:

1. Schaffen einer Möglichkeit, nicht benötigte PROFINET-Services zu deaktivieren. Hierfür ist im Engineering Werkzeug eine Bedienoberfläche vorzusehen, welche das Deaktivieren nicht benötigter PROFINET- oder sonstiger Dienste ermöglicht. Beispiel: Deaktivieren von Netzwerkmanagementdiensten (SNMP).
2. Erzeugen von Systemalarmen, die auf Security-relevante Ereignisse hinweisen. Beispiel: Werden bei Nutzung von kryptografischen Prüfsummen Datenpakte erkannt, deren kryptografische Prüfsumme nicht korrekt ist, obwohl das Datenpaket selber intakt ist (korrekte CRC), ist ein Systemalarm auszulösen.
3. Begrenzung der DCP-Dienste auf nur lesen (Read only). Damit kann das unautorisierte Verändern des Gerätenamens, Verändern der IP-Adresse und das Zurücksetzen auf Werkseinstellungen verhindert werden.
4. Zurzeit noch in Diskussion: Verwendung sicherer Netzwerkmanagement-Dienste (SNMPv3). Verwendung von Zugangsdaten für den Zugriff auf SNMP-Daten in Geräten. Einrichten eines Zugangsschutzes zu den Netzwerkmanagement Daten (Community String).

6.5.2 Baustein RTA/RTC

Der Baustein RTA/RTC definiert die Absicherung der zyklischen Kommunikation über die in Kapitel 6.4 beschriebenen Message Authentication Codes. Hierzu gehören:

1. Absicherung der zyklischen Layer-2-PROFINET-Kommunikation und der azyklischen Layer-2-basierten Alarmmechanismen über Message Authentication Codes.
2. Schutz gegen Replay Attacken durch zusätzlichen Nachrichtenzähler oder Integritätsschutz der bestehenden Nachrichtenzähler.
3. Regelmäßige Erneuerung des symmetrischen Schlüssels im laufenden Betrieb als Schutz gegen Ausspähung (engl. reverse calculation) des Schlüssels.
4. Option für Security-Klasse 3: Zusätzliche Verschlüsselung der Nachricht.

6.5.3 Baustein AR/RPC

Der Baustein AR/RPC befasst sich mit dem sicheren Aufbau und Betrieb der Application Relation. Hierzu sind die folgenden Maßnahmen vorgesehen:

1. Aufbau der Applikationsbeziehung zwischen IO Controller und IO Device über das in Kapitel 6.4 beschriebene asymmetrische Schlüsselverfahren. (Phase 1 gemäß Abbildung 11). Wird verwendet für:
    a. Verbindungsaufbau einschließlich Security Handshake.
    b. Aushandeln des symmetrischen Schlüssels für zyklische und azyklische Kommunikation.
    c. Änderung des symmetrischen Schlüssels zur Laufzeit.
2. Betrieb der Verbindung unter Nutzung des unter Punkt 1 ermittelten symmetrischen Schlüssels auch für azyklische Nicht-Echtzeit-Kommunikation (z. B. Record Services).

Hinweis: Authentisierung der Kommunikationspartner über Betreiberzertifikate.

6.5.4 Baustein Trust

Der Baustein Trust behandelt die Aspekte der sicheren Identitäten für Assets und Nutzer sowie deren sichere Verwahrung. Hierbei sind insbesondere zu adressieren:

1. Bereitstellung von sicheren Identitäten für Nutzer z. B. durch die Anforderung von Namen und Passwort beim Zugriff auf das Engineering-Werkzeug oder den IO-Supervisor. Hierüber werden die Schutzziele Autorisierung und Nicht-Abstreitbarkeit realisiert.
2. Bereitstellung von sicheren Identitäten für IO Devices, IO Controller und IO Supervisor, z. B. durch Hersteller- und/oder Betreiberzertifikate.
3. Option: Vor der Übertragung des Betreiberzertifikats wird die Identität des Gerätes über das Herstellerzertifikat geprüft.
4. Eine Möglichkeit des Rückrufs von Zertifikaten (Revocation) ist vorzusehen.
5. Vorzugsweise ist eine sichere Speicherung der Schlüsselinformation in besonders gesicherten Hardware Bausteinen (z. B. Trusted Platform Module TPM [BSI2018]) vorzusehen.

6.5.5 Baustein Supervisor

Der Baustein Supervisor befasst sich mit der Absicherung des IO Supervisors. Dies betrifft sowohl den Zugriff des Bedienpersonals auf den IO Supervisor als auch den Zugriff des IO Supervisors auf die IO Devices. Die wesentlichen Maßnahmen sind:

1. Authentifizierung der menschlichen Nutzer des IO Supervisors über Benutzername und Passwort oder eine zentrale Benutzerverwaltung optional auch mit Zertifikaten.
2. Einbindung des IO Supervisors in den gesicherten Verbindungsaufbau gemäß Abbildung 11.

6.5.6 Baustein GSD

Die Gerätebeschreibungsdatei (General Station Description GSD) ist eine auf der Beschreibungssprache GSDML basierende textuelle Datei, welche die Eigenschaften von PROFINET Komponenten enthält. Für die GSD sind die folgenden Erweiterungen vorzusehen:

1. Erweiterung des GSD-Inhaltes um Informationen, welche die Security-Fähigkeiten eines PROFINET Gerätes beschreiben.

2. Schutz des GSD Inhaltes gegen Veränderungen, z. B. durch eine digitale Signatur.

6.5.7 Baustein Test

PROFINET-Geräte der Security-Klasse 1 werden bereits heute im Rahmen der Zertifizierung einem Security Test unterzogen [PNO2015]. Dieser Test fokussiert heute im Wesentlichen auf die Robustheit der Geräte, insbesondere in Bezug auf eine Überlastung (Denial of Service). Diese Tests sind künftig wie folgt zu erweitern:

1. Geräte der Security-Klassen 2 und 3 müssen die Netzlastklasse II gemäß [PNO2015] erfüllen. Die Notwendigkeit der Erweiterung der Netzlasttests ist zu diskutieren.
2. Die Wirksamkeit der zusätzlichen Sicherungsmaßnahmen, z. B. das Auslösen von Alarmen bei Security-relevanten-Ereignissen sind im Rahmen der Zertifizierung zu prüfen. Die Testspezifikation [PNO2017] ist entsprechend zu erweitern.

6.5.8 Baustein Hersteller/Vendor

Gemäß der Abgrenzung in Kapitel 5.2 und 5.3 unterscheidet dieses Dokument zwischen Anforderungen, welche durch Ergänzungen an verschiedenen PROFINET Dokumenten vorzunehmen sind und Ergänzungen, welche in der Hoheit der Hersteller liegen. Dieser Abschnitt gibt den Herstellern Hinweise, welche Maßnahmen herstellerseitig vorzusehen sind. Trotz dieser Empfehlungen verbleiben die Aspekte in der Verantwortung und Entscheidungshoheit der Hersteller. Bei der folgenden Betrachtung wird zwischen Komponentenherstellern und Systemherstellern unterschieden. Es wird davon ausgegangen, dass Systemhersteller alle Komponententypen (IO Controller, IO Device, IO Supervisor, Engineering Tool) herstellen. Bei einem Komponentenhersteller wird davon ausgegangen, dass er nur IO Devices herstellt.

Komponentenhersteller

1. Etablierung eines Prozesses zum Ausstellen und Zurückrufen von Herstellerzertifikaten.
2. Bereitstellung eines sicheren Speicherortes für Schlüsselinformationen für IO Device.
3. Etablierung von Prozessen zur Unterstützung eines Patch Managements für die Software gemäß [IEC_62443-2-3].
4. Berücksichtigung der Entwicklungs- und Dokumentationsanforderungen orientiert an [IEC_62443-4-1] und [IEC_62443-4-2].
5. Sicherstellung der Integrität der Software in IO Device, z. B. durch Signierung der Software, ggf. in Verbindung mit einem Secure Boot.

Systemhersteller

Alle Anforderungen an einen Komponentenhersteller müssen erfüllt sein. Zusätzlich haben Systemhersteller die folgenden Punkte zu erfüllen:

1. Etablierung einer Nutzerverwaltung mit Zuweisung von Nutzerrechten für IO Supervisor und Engineering Werkzeug.
2. Bereitstellung einer Bedienoberfläche für die Konfiguration von Security-Funktionen, z. B. für die Deaktivierung nicht benötigter Dienste, Integritätsprüfung der GSD. Ein Konzept für das Vorgehen im Fall, dass GSD Integritätsprüfung nicht bestanden oder nicht möglich ist, sollte vom Systemhersteller definiert und implementiert werden.
3. Bereitstellung eines sicheren Speicherortes für Schlüsselinformationen und andere kritische Daten für IO Controller, IO Supervisor und ggf. Engineering Werkzeug. Übergangslösungen sind möglich.
4. Bereitstellung eines Werkzeuges für die Erzeugung von Betreiberzertifikaten, z. B. im Engineering Werkzeug oder an anderer Stelle.
5. Sicherstellung der Integrität der Software in IO Controller und IO-Supervisor z. B. durch Signierung der Software, ggf. in Verbindung mit einem Secure Boot.
6. Schutz der Verbindung zwischen Engineering-Werkzeug und IO Controller gegen Manipulation. Hinweis: Diese Kommunikation ist in der Regel herstellerspezifisch realisiert.

7 Zusammenfassung und Ausblick

Die in diesem Dokument gegebenen Informationen sind zunächst relativ allgemein und noch wenig spezifisch. In einem folgenden Schritt sollen nun auf Basis dieses Dokumentes die Teile der PROFINET Spezifikationen ermittelt werden, an denen Ergänzungsbedarf besteht. Voraussichtlich werden dies sein:

- PROFINET Application Layer protocol for decentralized periphery [PNO2018c]
- PROFINET Application Layer services for decentralized periphery [PNO2018b]
- PROFINET Security Richtlinie. Richtlinie für PROFINET [PNO2013]
- Test Specification for PROFINET [PNO2017]
- GSDML Technical Specification for PROFINET [PNO2018a]
- PROFINET Planungsrichtlinie [PNO2014]
- Zusätzliches Dokument: Implementierungshinweise für PROFINET Komponenten (neues Dokument)

Die entsprechenden Arbeitsgruppen von PI werden die erforderlichen Anpassungen erarbeiten und innerhalb von PI zur Diskussion stellen. Hierbei werden dann auch die erforderlichen technischen Detaillierungen vorgenommen werden. Weiterhin wird momentan die Durchführung eines Prototypings diskutiert. Abschließende Ergebnisse liegen noch nicht vor.

In einem nächsten Schritt werden die spezifizierten Security Lösungen an den grundlegenden Anforderungen der Normreihe IEC 62443 gespiegelt und verifiziert. Aus Zeitgründen kann diese Untersuchung nicht Bestandteil dieses Papiers sein.

8 Literaturverzeichnis

[BSI2013] Bundesamt für Sicherheit in der Informationstechnik: Industrial Control System Security: Innentäter. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_061.html, 29.07.2015.

[BSI2018] Bundesamt für Sicherheit in der Informationstechnik (BSI): Das Trusted Platform Module (TPM) und vertrauenswürdige Informationstechnik. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/dastrustedplatformmoduletpm_node.html.

[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_62443-4-2] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V DIN EN 62443-4-2:2017-10; VDE 0802-4-2:2017-10 - Entwurf: Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme (IEC 65/663/CDV:2017); Deutsche Fassung prEN 62443-4-2:2017. Beuth Verlag, 2017.

[DIN_IEC_62443-3-3] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V DIN IEC 62443-3-3:2015-06; VDE 0802-3-3:2015-06 - Entwurf: 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, Berlin, 2015.

[FDA2018] U. S. Food & Drug Administration: CFR - Code of Federal Regulations Title 21, Part 11. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1.

[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_62443-4-1] IEC- International Electrotechnical Commission IEC/NP 62443-4-1: Industrial communication networks – Network and system security – Part 4-1: Product development requirements, 2013.

[IEC_62443-4-2] IEC- International Electrotechnical Commission IEC/NP 62443-4-2: Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components.

[ISO_27001] DIN Deutsches Institut für Normung e. V DIN ISO/IEC 27001: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits- Managementsysteme – Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014), 2015.

[NE_153] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V NE 153: Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme, Leverkusen, 2015.

[NIST_197] NIST Computer Security Division (CSD): Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf.

[NIST198] NIST Computer Security Division (CSD): FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC),

[PNO2013] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Richtlinie. Richtlinie für PROFINEThttps://de.profibus.com/downloads/profinet-security-guideline/.

[PNO2014] PROFIBUS Nutzerorganisation e.V.: PROFINET Planungsrichtlinie. https://de.profibus.com/index.php?eID=dumpFile&t=f&f=49686&token=53a58fd07df8cc843a50cdd9efd29db0c325f4e7.

[PNO2015] PROFIBUS Nutzerorganisation e.V.: Test Specification PROFINET IO Security Level 1 / Netload. Technical Specification for PROFINET. http://www.profibus.com/nc/download/test-and-certification/downloads/profinet-io-net-load-1/display/, 15.07.2014.

[PNO2017] PROFIBUS Nutzerorganisation e.V.: Test Specification for PROFINET Related to PROFINET V2.35. Technical Specification for PROFINET. https://de.profibus.com/downloads/profinet-test-specification/.

[PNO2018a] PROFIBUS Nutzerorganisation e.V.: GSDML - Technical Specification for PROFINET. https://de.profibus.com/downloads/gsdml-specification-for-profinet/.

[PNO2018b] PROFIBUS Nutzerorganisation e.V.: Application Layer services for decentralized periphery. Technical Specification for PROFINET IO. https://de.profibus.com/downloads/profinet-specification/.

[PNO2018c] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery. Technical Specification for PROFINET IO. https://de.profibus.com/downloads/profinet-specification/.

[RUN2014a] Runde, Markus; Hausmann, Stefan; Tebbe, Christopher; Czybik, Björn; Niemann, Karl-Heinz; Heiss, Stefan; Jasperneite, Jürgen: SEC_PRO - Sichere Produktion mit verteilten Automatisierungssystemen. Schlussbericht für das FHprofUnt-Forschungsprojekt mit dem FKZ 1760A10 sowie 17060B10. https://serwiss.bib.hs-hannover.de/frontdoor/index/index/docId/499, 17.12.2014.

[RUN2014b] Runde, Markus: Echtzeitfähige Protokollerweiterung zum Schutz Ethernet-basierter Automatisierungskomponenten. Dissertation zur Erlangung des akademischen Grades Doktoringenieur (Dr.-Ing.). Dissertation, Magdeburg, 2014.

[SHO2014] Shostack, Adam: Threat modeling. Designing for security. Wiley, Indianapolis, IN, 2014.

[SPE2013] Speth, Walter: Nur Befehle befolgt. CPS erfordern sichere Identitäten. In atp-edition 12, 2013; S. 46–52.

[TEB2015] Tebbe, Christopher, Niemann, Karl-Heinz, Runde, Markus: IT-Sicherheit in Pharmaanlagen. In Techno Pharm 1, 2015, Jahrgang 5; S. 34–39. https://www.ecv.de/download/download/Zeitschriften/TechnoPharm/volltext/TP0501_0327.pdf

[VDE2016] VDE Verband der Elektrotechnik Elektronik und Informationstechnik e. V.: VDE Trendreport 2016. Internet der Dinge - Industrie 4.0. http://info.vde.com/goto.php?l=dq8zol.1q7d72d,u=989bcd3af624fa771465a57cdc9eec63,n=98ibt.15cmlin,art_id=98ibu.1t5icbp.

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 96 58 590 • Fax +49 721 96 58 589
E-mail info@profibus.com
www.profibus.com ● www.profinet.com