atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 9/2023

Peer-Review: 21.06.2023

Wie man ein sicheres PROFINET-Gerät entwickelt

Organisatorische und technische OT-Security-Maßnahmen bei der Entwicklung von PROFINET-Geräten

Karl-Heinz Niemann, Hochschule Hannover; Andreas Walz, Hochschule Offenburg; Simon Merklin, Endress+Hauser Digital Solutions; Dominik Ziegler, Siemens AG; Boris Waldeck, Phoenix Contact Electronics

Das PROFINET Protokoll wurde in der aktuellen Version um Security-Funktionen erweitert. Damit können für PROFINET flexible Netzwerkarchitekturen unter Berücksichtigung von OT-Security Anforderungen entworfen werden, die durch die bisher erforderliche Netzwerksegmentierung nicht möglich waren. Neben den Herstellern der Protokollstacks sind nachfolgend auch die Komponentenhersteller gefordert, eine sichere Implementierung in ihren Geräten umzusetzen. Die erforderlichen Maßnahmen gehen dabei über die Nutzung eines sicheren Protokollstacks hinaus. Der Beitrag zeigt am Beispiel eines Ethernet-APL Messumformers mit PROFINET-Kommunikation die künftig von PROFINET-Geräteherstellern zu berücksichtigenden technischen und organisatorischen Rahmenbedingungen.

#PROFINET Security #Sicherer Produktentwicklungslebenszyklus #IEC 62443

How to develop a secure PROFINET device

Organizational and technical OT security measures for the development of PROFINET devices

The PROFINET protocol has been expanded in the current version to include security functions. This allows flexible network architectures with the consideration of OT security requirements to be designed for PROFINET, which were not possible due to the network segmentation previously required. In addition to the manufacturers of the protocol stacks, component manufacturers are also required to implement a secure implementation in their devices. The necessary measures go beyond the use of a secure protocol stack. Using the example of an Ethernet-APL transmitter with PROFINET communication, this article shows which technical and organizational framework conditions will have to be considered by PROFINET device manufacturers in the future.

#PROFINET security #Secure development lifecycle #IEC 62443

1. Beschreibung der aktuellen Situation

Mit der Version 2.4MU4 der PROFINET-Spezifikation [1, 2] stellt PROFIBUS & PROFINET International (PI) OT-Security Funktionen für PROFINET zur Verfügung. Diese Funktionen dienen als Basis für die Hersteller von Automatisierungskomponenten und Automatisierungssystemen, um Komponenten und Systeme zu entwickeln, die hohe Standards in Bezug auf die OT-Security erfüllen. Das PROFINET-Security-Konzept basiert auf der kryptografischen Absicherung der PROFINET-Kommunikation und weiteren Maßnahmen. Wesentliche Features des PROFINET-Security-Konzeptes sind:

- Ausstattung der PROFINET-Devices und PROFINET-Controller mit digitalen Identitäten über digitale Zertifikate.
- Sicherer Aufbau der Kommunikationsbeziehungen unter Nutzung des TLS-Protokolls (asymmetrische Kryptografie).
- Sichere Kommunikation, insbesondere für den Echtzeitkanal, unter Nutzung symmetrischer Kryptografie.
- Schutz der Gerätebeschreibungsdateien ((GSD)-Dateien) durch eine digitale Signatur.

Eine detailliertere Beschreibung des PROFINET-Security-Konzeptes findet sich z. B. in [3 bis 6].

Mit der Spezifikation des PROFNET-Security-Konzeptes stehen die Hersteller von Automatisierungskomponenten nun vor der Herausforderung, diese Security-Funktionen in ihre Geräte zu integrieren. Der folgende Beitrag beschreibt die wesentlichen Aufgaben und Prozesse aus der Sicht eines Herstellers für Ethernet-APL-Feldgeräte, die in Verbindung mit dem PROFINET-Protokoll betrieben werden.
In diesem Dokument werden die Begriffe „Sicherheit“ und „Security“ im Sinne der OT-Security verwendet. Es geht also um den Schutz von Produktionsanlagen gegen Cyber-Angriffe.

2. Die Rolle eines Feldgeräteherstellers im Security-Prozess

Feldgerätehersteller stehen zurzeit vor mehreren Herausforderungen. In der Vergangenheit wurden Feldgeräte vorwiegend mit einer 4 … 20 mA Schnittstelle mit HART-Protokoll oder über einen Feldbus, wie PROFIBUS-PA, ausgestattet. Die bestehenden Interface-Portfolios werden künftig um ein Ethernet-APL Interface ergänzt, bzw. durch dieses ersetzt. Ethernet-APL ist ein Zweidraht-Ethernet, welches Feldgeräte sowohl mit Daten als auch mit Energie versorgt. Durch dieses Interface werden die Feldgeräte bei Einsatz von PROFINET zu PROFINET-Devices und müssen alle Anforderungen erfüllen, die an PROFINET-Devices gestellt werden. Das gilt auch für den Aspekt der Security. In [7] beschreiben die Autoren, welche Security-Anforderungen an ein APL-Feldgerät gestellt werden.

Eine Beschreibung der verschiedenen Rollen im OT-Security-Prozess soll nun folgen.

Abbildung 1 zeigt, dass an den Feldgerätehersteller im Rahmen der Feldgeräteentwicklung technische und organisatorische Anforderungen gestellt werden. Erfüllt der Feldgerätehersteller diese, ist er in der Lage, ein sicheres Feldgerät auf den Markt zu bringen. Derartige Geräte werden für den Aufbau einer Produktionsanlage verwendet. Der Anlagenplaner (Systemintegrator) muss wiederum technische und organisatorische Anforderungen bei der Planung berücksichtigen. Die sicheren Feldgeräte gehen in den Planungsprozess ein, weil sie die Basis für die Erfüllung der systemweiten Security-Anforderungen darstellen. Die vom Systemintegrator geplante Anlage wird dann errichtet, in Betrieb genommen und an den Betreiber übergeben. Der Anlagenbetreiber muss wiederum organisatorische Anforderungen in Bezug auf den Anlagenbetrieb beachten. Eine detaillierte Beschreibung der hier beschriebenen Rollen und der zugeordneten Aufgaben findet sich in [8].

Im Weiteren soll der in Abbildung 1 rot eingerahmte Teil mit Fokus auf einen Feldgerätehersteller betrachtet werden. Die folgenden Kapitel fokussieren daher auf die Feldgeräteentwicklung und zeigen, welche organisatorischen und technischen Anforderungen vom Feldgerätehersteller zu beachten sind, um am Ende der Entwicklung ein sicheres Feldgerät an den Markt liefern zu können.

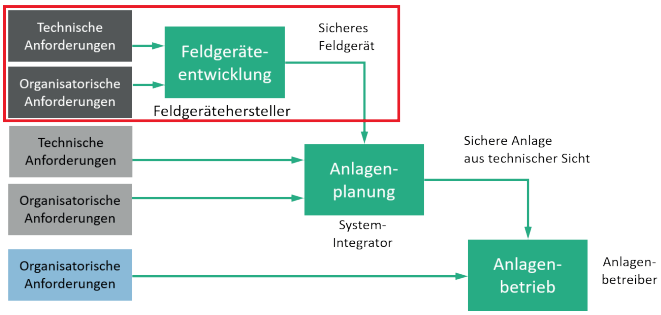

Abbildung 1: Die Rollen im OT-Security-Prozess

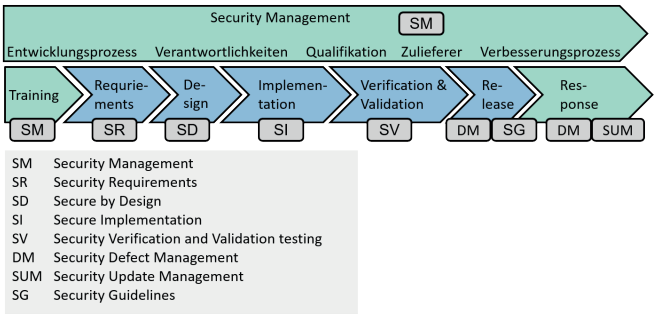

Abbildung 2: Die Bestandteile des sicheren Entwicklungslebenszyklus

3. Die Entwicklung eines sicheren Feldgerätes

Die OT-Security-Anforderungen an Feldgeräte wurden bereits in früheren Beiträgen betrachtet [9, 10]. Aus diesem Grund soll auf die Ermittlung der Security-Anforderungen an dieser Stelle nicht näher eingegangen werden. Stattdessen fokussiert dieser Beitrag auf den Entwicklungsprozess zur Entwicklung eines sicheren Feldgerätes und die erforderlichen Prozessschritte.

Die Norm IEC 62443 hat sich als die wesentliche Norm für die OT-Security etabliert. Eine Übersicht zur IEC 62443 findet sich in [11]. Die IEC 62443 definiert u. a. die Rolle des Komponentenherstellers. Siehe hierzu auch die Rollenbeschreibung in Abbildung 1. In diesem Beitrag hat der Feldgerätehersteller diese Rolle inne. Für diese Rolle sind die beiden folgenden Teile der Norm relevant:

» DIN EN IEC 62443-4-1 [12]: Dieser Teil befasst sich mit dem sicheren Entwicklungslebenszyklus für die Entwicklung von Automatisierungskomponenten. Hier finden sich also im Wesentlichen die organisatorischen Anforderungen.

» DIN EN IEC 62443-4-2 [13]: Dieser Teil beschreibt die technischen Anforderungen, die an die Komponenten zu stellen sind.

Die beiden folgenden Kapitel werden sich nun im Detail mit den Anforderungen dieser beiden Normen befassen.

3.1 Organisatorische Anforderungen an den sicheren Entwicklungslebenszyklus

Die IEC 62443-4-1 beschreibt die Voraussetzungen, die eine Entwicklungsorganisation zwingend erfüllen muss, um Produkte, die die Sicherheitsanforderungen erfüllen, zu entwickeln. Dabei wird ein standardisierter Entwicklungsprozess, der sichere Entwicklungslebenszyklus (engl. SDL = *Secure development lifecycle*), zu Grunde gelegt.

Abbildung 2 zeigt die wesentlichen Bestandteile des SDL. Ziel des SDL ist es zu gewährleisten, dass OT-Security-Anforderungen über den gesamten Lebenszyklus des Produktes berücksichtigt werden und dass die Qualität der Implementierung in Bezug auf die OT-Security-Anforderungen von gleichbleibender Qualität ist. Diese Bestandteile des SDL werden im Folgenden näher betrachtet.

3.1.1 Management des Sicherheitslebenszyklus (Security Management)

Dieser Teil beschreibt, wie das Management des SDL erfolgen soll. Der Entwicklungsprozess ist definiert, implementiert und überprüft, Verantwortlichkeiten sind definiert und

zugewiesen. Die erforderliche Qualifikation des Personals wurde definiert und wird durch kontinuierliche Schulungen aufrechterhalten und verbessert. Anforderungen an Zulieferteile (z. B. Protokollstacks) sind definiert und werden überwacht. Hierbei geht es darum, dass auch bei den Zulieferteilen Sicherheitsanforderungen zu berücksichtigen sind und dass auch Benachrichtigungen der Hersteller zu Schwachstellen verfügbar sind. Die Sicherheit der Entwicklungsumgebung wird sichergestellt und überwacht. Das betrifft z. B. den Integritätsschutz wichtiger Dateien, den Schutz und die sichere Aufbewahrung privater Schlüssel, und die Überwachung der Security-Eigenschaften von extern bereitgestellten Komponenten, wie z. B Protokollstacks. Die Organisation muss in der Lage sein, ihre sicherheitsbezogenen Probleme zu handhaben, z. B. indem Schwachstellenmeldungen von Kunden oder anderen Organisationen entgegengenommen und nach einem definierten Prozess bearbeitet werden. Der beschriebene Prozess muss regelmäßig verifiziert und kontinuierlich verbessert werden.

3.1.2 Anforderungen (Requirements)

Dieser Abschnitt der Norm befasst sich mit den Prozessen zur Behandlung der Security-Anforderungen (Requirements). Zunächst wird das IT-Sicherheitsumfeld des Produktes beschrieben (engl. Security Context). Diese Beschreibung ist erforderlich, damit definiert ist, welche Sicherheitseigenschaften die Umgebung des Produktes bereitstellt und welche Anforderungen die Komponente selber erfüllen muss. In einem nächsten Schritt ist eine Bedrohungsanalyse zu erstellen, welche alle auf die Komponente einwirkenden Bedrohungen erfasst und bewertet. Hier sind bei Feldgeräten insbesondere die Kommunikationsinterfaces (z. B. PROFINET-Schnittstelle, OPC-UA-Schnittstelle, Bluetooth-Schnittstelle, Bediendisplay) zu berücksichtigen. Eine detaillierte Risikoanalyse für ein Feldgerät findet sich in [10]. Auf Basis dieser Anforderungen werden nun die IT-Sicherheitsanforderungen für die Komponente und die IT-Sicherheitsanforderungen für das Umfeld, in dem die Komponente betrieben wird, erarbeitet. Diese Anforderungen (engl. Security-Requirements) sind vorzugsweise in einem Requirements-Management-Tool zu dokumentieren und über den Produktenwicklungslebenszyklus nachzuhalten.

3.1.3 Gesicherter Entwurf (Design)

Dieser Teil der Norm befasst sich mit dem gesicherten Entwurf. Die Norm [12] schreibt hierzu: *„Es muss ein Prozess angewendet werden, mit dem ein gesicherter Entwurf entwickelt und dokumentiert wird, der jede Schnittstelle des Produkts einschließlich physikalischer und logischer Schnittstellen kennzeichnet und beschreibt.“* Weiterhin wird im Rahmen dieses Normteils das Defense-in-Depth-Konzept für die Komponente erarbeitet. Dieses Konzept beschreibt das Ineinandergreifen von komponentenbezogenen Schutzmaßnahmen in Verbindung mit externen Maßnahmen. Weitere Informationen zum Thema Defense-in-Depth finden sich in [14 bis 16].

Der System-/Software-Entwurf ist dann einer Entwurfsprüfung zu unterziehen. Hierbei sind bewährte Methoden des gesicherten Entwurfs, wie z. B. Verringerung der Angriffsfläche, Methode der minimalen Rechte und die Dokumentation aller Vertrauensgrenzen einzusetzen.

3.1.4 Gesicherte Implementierung

Die Norm [12] schreibt zu diesem Thema: *„Es muss ein Prozess angewendet werden, um sicherzustellen, dass Überprüfungen der Implementierung durchgeführt werden, um sicherheitsbezogene Probleme im Zusammenhang mit der Implementierung des gesicherten Entwurfs zu kennzeichnen, zu beschreiben und bis zum Abschluss zu verfolgen.“*. Mögliche Verfahren zur Überprüfung sind z. B. die Definition und Überwachung von Codierungsregeln insbesondere in Bezug auf die IT-Sicherheit, statische Codeanalyse, Kennzeichnung von IT-Sicherheitsanforderungen im Code, Validierung von Eingaben die Vertrauensgrenzen überschreiten etc.

3.1.5 Verifizierung und Validierung

Dieser Abschnitt befasst sich mit der Verifikation der IT-Sicherheitsanforderungen. Hierzu gehören z. B. funktionale Prüfungen, Performance-Prüfungen [17] sowie Grenzwert- und Randbedingungsprüfungen. Den Tests sollten allgemein gültige Testkonzepte zu Grunde liegen, wie sie zum Beispiel in [18 bis 20] beschrieben sind.

Beim Entwurf der Tests ist besonderer Fokus auf das Auffinden von Sicherheitslücken zu legen. Die sollte Fuzzing und Penetration-Testing mit einbeziehen. Die Prüfer sollten dabei unabhängig von der Entwicklung agieren.

3.1.6 Behandlung sicherheitsbezogener Probleme

Das Unternehmen muss in der Lage sein, Meldungen in Bezug auf Schwachstellen bzw. Defekte in den eigenen Produkten entgegenzunehmen und zu bearbeiten. Das betrifft auch Schwachstellenmeldungen von Drittanbieterkomponenten (z. B. Protokollstacks, Betriebssysteme). Dies kann z. B. über ein spezielles E-Mail-Konto oder über eine Webseite erfolgen. Es ist ein Prozess zu etablieren, der eine systematische und zeitnahe Bearbeitung solcher Meldungen sicherstellt. Hierzu kann der Hersteller z. B. ein Product-Security-and-Incidence-Response-Team (PSIRT) einrichten. Das Ergebnis der Bearbeitung sollte der meldenden Person mitgeteilt werden. Weiterhin ist, bei Vorliegen einer Schwachstelle, eine Information an die Nutzer herauszugeben (Security Bulletin, Security Advisory). Für das Schwachstellen-Management und für die Offenlegung von Schwachstellen existieren eigene Normen [21, 22].

3.1.7 Sicherheitsaktualisierungen (Security Update Management)

Auf Grund einer Defekt-Meldung kann es erforderlich sein, dass die Software des Produktes über einen Security Patch aktualisiert wird. Es ist ein Prozess zu etablieren, der die Erstellung solcher Updates ermöglicht. Die Security Patches sind zu dokumentieren und unabhängig von anderen Updates bereitzustellen. Häufig verwenden Feldgeräte abhängige Komponenten, wie z. B. Echtzeitbetriebssysteme und/oder Protokollstacks. Derartige Komponenten sind in Bezug auf die Meldung von Schwachstellen zu überwachen und es sind ggf. erforderliche Updates auch für das eigene Produkt zu erzeugen.

Nutzer der Software-Updates müssen in der Lage sein, die Echtheit der Updates zu überprüfen. Dies kann z. B. durch eine digitale Signierung der SW-Pakete erfolgen.

3.1.8 Security Guidelines
Der Hersteller muss dem Anwender Security-relevante Informationen zur Verfügung stellen. Dies umfasst:

- Dokumentation des zu Grunde gelegten Defense-in-Depth-Konzeptes.
- Maßnahmen in Bezug auf das Defense-in-Depth-Konzept, die von der Umgebung zu erwarten sind.
- Richtlinien für die Härtung der Komponenten, z. B. durch Ausschalten nicht benötigter Dienste und durch Aufforderung zur Änderung von Standard-Passworten.
- Richtlinien für eine gesicherte Entsorgung, z. B. das Löschen von digitalen Zertifikaten.
- Richtlinien für einen gesicherten Betrieb, z. B. Aktionen, die ein Anwender oder Administrator durchführen muss.
- Richtlinien zur Nutzerkontenverwaltung.

Die Dokumentation ist in regelmäßigen Abständen auf Konsistenz, Vollständigkeit und Korrektheit zu überprüfen.

3.2 Anwendbarkeit und Umsetzung der organisatorischen Anforderungen auf einen Ethernet-APL-Messumformer

Die im vorangehenden Abschnitt 3.1 beschriebenen Prozessanforderungen stellen die organisatorische Basis für die Entwicklung sicherer Produkte dar. Diese organisatorischen Anforderungen bestehen unabhängig von der Größe oder Komplexität des betrachteten Gerätes. Anbieter von Ethernet-APL-Messumformern sollten sich demzufolge mit diesen Anforderungen auseinandersetzen und diese in den Entwicklungslebenszyklus integrieren.
Für die Umsetzung der Anforderungen kann ein stufenweises Vorgehen mit den folgenden Schritten sinnvoll sein:

1. Erstellen eines Ausbildungsplans und Start der Security-Trainings für das Personal. Dieses Training sollte an die Rollen der Mitarbeitenden (z. B. SW-Entwickler, SW-Architekt, SW-Tester) angepasst sein.
2. Dokumentation des Entwicklungslebenszyklus und Erstellen der erforderlichen Dokumente und Templates.
3. Aufbau der Infrastruktur wie z. B. Webseite für Security-Advisories, sowie einer Stelle für Entgegennahme von Schwachstellenmeldungen.
4. Aufbau einer Infrastruktur zur Erzeugung und Herausgabe von Security Patches einschließlich Meldesystem an die Kunden.
5. Etablierung von Prozessen zum Security-Monitoring von abhängigen Komponenten (z. B. Betriebssysteme, Protokollstacks). Planung von Security-Lieferantenaudits.
6. Integration der Security-relevanten Arbeitspakete in den bisherigen Entwicklungslebenszyklus und Training der Mitarbeitenden.
7. Auswahl einer Komponente für einen ersten Durchlauf der Prozesse. Vorzugsweise sollte es sich dabei um eine neu zu entwickelnde Komponente handeln, damit alle wesentlichen Schritte des Entwicklungslebenszyklus durchlaufen werden. Bei einer bereits bestehenden Komponente ist mit einem entsprechenden Nachdokumentationsaufwand zu rechnen, obwohl das Produkt bereits im Markt ist.
8. Anforderungen definieren:
   a. Erarbeiten und Dokumentieren des Defense in Depth-Konzeptes.
   b. Erstellen der Risikoanalyse.
   c. Ableitung der Security-Requirements aus der Risikoanalyse.
   d. Ableitung der Security-Requirements aus dem Normteil IEC 42443-4-2 [13], welcher die Security-Anforderungen an eine Komponente definiert.
   e. Integration der Security-Requirements in das Requirements-Management, vorzugsweise über ein entsprechendes Tool.
9. Implementierung:
   a. Gesicherten Entwurf überwachen.
   b. Design-Reviews durchführen.
   c. Code-Reviews durchführen.
   d. Schwachstellenanalyse durchführen.
   e. Verifikation und Test:
   f. Test der Security-Funktionalität.
   g. Penetration-Test.
   h. Vulnerability-Test
   i. Last-Test. Siehe hierzu auch [17].
10. Dokumentation:
    a. Dokumentation Defense-in-Depth-Konzept.

Tabelle 1: Definition der Security-Level [13]

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

b. Dokumentation Anforderungen an Umgebung im Rahmen des Defense-in-Depth-Konzeptes.

c. Dokumentation zur Härtung der Komponente.

11. Freigabe.

Bei der Etablierung dieser Prozesse sind die folgenden Aspekte zu beachten:

» Dokumentation des Prozesses.

» Leitfrage: Wo steht geschrieben, dass Sie das so machen?

» Dokumentation der Prozessergebnisse (z. B. Risikoanalyse, Defense-in-Depth-Konzept.

» Leitfrage: Existieren zu dem entwickelten Produkt alle erforderlichen Artefakte wie Spezifikationen, Code-Review Protokolle, Prüfdokumentationen?

» Nachweis, dass die Prozesse bei der Entwicklung des Produktes angewandt wurden.

» Leitfrage: Sind für diese Softwareversion alle erforderlichen Dokumente erstellt und alle Security-Requirements implementiert und getestet?

» Kontinuierliche Verbesserung des Prozesses.

» Leitfrage: Welche Verbesserungen haben Sie seit dem letzten Durchlauf vorgenommen?

Die Autoren sind der Meinung, dass es sinnvoll ist, zunächst den sicheren Entwicklungslebenszyklus einzuführen. Die Norm IEC 62443-4-1 [12] kennt vier unterschiedliche Reifegrade (engl. Maturity Level). Die Reifegrade ML1 bis ML4 beschreiben, wie stabil und etabliert die Security-Prozesse im Unternehmen verankert sind.

» Der Reifegrad **ML1** beschreibt z. B. dass in dem Unternehmen Prozesse teilweise undokumentiert und ggf. nicht nachvollziehbar sind.

» Reifegrad **ML2** hat der Hersteller „die Fähigkeit, die Entwicklung eines Produkts nach den schriftlich niedergelegten Leitlinien (einschließlich Ziele) zu verwalten. Der Hersteller kann außerdem nachweisen, dass das Personal, das den Prozess durchführen wird, die Fachkenntnisse zur Durchführung hat, dafür ausgebildet ist und/oder nach schriftlichen Vorgehensweisen arbeitet."

» Reifegrad **ML3:** „Die Leistungsfähigkeit eines Herstellers mit dem Reifegrad 3 ist innerhalb der Herstellerorganisation nachweislich wiederholbar. Die Prozesse sind durchgeführt worden und es liegen nachprüfbare Nachweise dafür vor."

» Reifegrad **ML4** definiert hingegen stark kontrollierte und ständig verbesserte Prozesse.

In einem nachfolgenden Schritt sollten dann die Produkt-Requirements gemäß IEC 62442-4-2 [13] bearbeitet werden.

3.3 Technische Security-Anforderungen an ein Ethernet-APL Messumformer

Nachdem im vorangehenden Abschnitt die organisatorischen Anforderungen an eine Entwicklungsorganisation beschrieben wurden, folgt nun die Betrachtung der technischen Anforderungen. Bevor die Anforderungen im Detail erörtert werden, sind zunächst zwei Einordnungen zu treffen: Der zu erreichende Ziel-Security-Level (Target-Security-Level) und der Typ des Gerätes.
Der Security-Level beschreibt die Fähigkeiten eines Angreifers, wie in Tabelle 1 dargestellt.
Tabelle 1 zeigt, dass mit steigendem Security Level die angenommenen Fähigkeiten des Angreifers zunehmen. Für die Festlegung der Security-Anforderungen ist zunächst die Festlegung des Ziel-Security-Levels erforderlich (also des Levels, den man mit seinem Produkt erreichen möchte). Es ist nachvollziehbar, dass die Anforderungen der Norm mit wachsendem Security-Level ansteigen. In der Norm werden für höhere Security-Level zusätzliche Requirement-Enhancements (RE) zu definiert, die zu erfüllen sind. Der angestrebte Security-Level ist in der Bedrohungsanalyse entsprechend zu berücksichtigen. Für Automatisierungssysteme mit typischen Anforderungen geht der VDMA bei einem Leitfaden [23] von einem Security-Level 2 aus.

Weiterhin unterscheidet die IEC 62443-4-2 [13] unterschiedliche Komponententypen, die teilweise unterschiedlichen Anforderungen genügen müssen. Es sind die folgenden Komponententypen definiert:

» Softwareanwendungen (SAR);

» Eingebettete Geräte (EDR);

» Host-Geräte (HDR); und

» Netzwerkkomponenten (NDR).

Ein Ethernet-APL-Messumformer ist in die Kategorie „Eingebettetes Gerät (EDR)“ einzuordnen. Mit diesen beiden Festlegungen können dann in einem nächsten Schritt die Komponentenanforderungen der Norm betrachtet werden. Die Norm IEC 62443-4-2 [13] definiert die folgenden Anforderungsgruppen (engl. Foundational Requirements):

» Identifizierung und Authentifikation

» Nutzungskontrolle

» Systemintegrität

» Vertraulichkeit der Daten

» Eingeschränkter Datenfluss

» Rechtzeitige Reaktion auf Ereignisse

» Verfügbarkeit der Ressourcen

Im Weiteren soll an einem exemplarischen Ethernet-APL-Messumformer die Anwendung dieser Anforderungen auf das Gerät diskutiert werden.
Abbildung 3 zeigt einen exemplarischen Ethernet-APL Messumformer. Es wird für diese Betrachtung ein Maximum an Schnittstellen angenommen. Reale Messumformer werden typischerweise über weniger Schnittstellen verfügen. Es ist zu erkennen, dass im Wesentlichen die Schnittstellen des Messumformers nach außen betrachtet werden, weil über diese Wege potenzielle Angreifer am Ehesten einen Zugang zum Gerät erlangen können.

3.3.1 Identifizierung und Authentifikation

Dieser Teil der Norm gibt vor, dass menschlichen Nutzer, die mit dem Gerät interagieren, identifiziert und authentifiziert werden müssen. Im vorliegenden Anwendungsfall wären dies z. B. menschliche Nutzer, die über einen Webserver oder einer drahtlose Vor-Ort-Kommunikation mit dem Gerät interagieren. Es ist zu erkennen, dass diese Anforderungen über das PROFINET-Security-Konzept hinausgehen, weil hier weitere Schnittstellen, neben der PROFINET-Schnittstelle, zu betrachten sind. Das gleiche gilt auch für Software-Prozesse und andere Komponenten. So müsste sich auch ein OPC-UA-Client, der auf den OPC-UA-Server des Gerätes zugreift, authentisieren. Diese Funktion kann durch eine

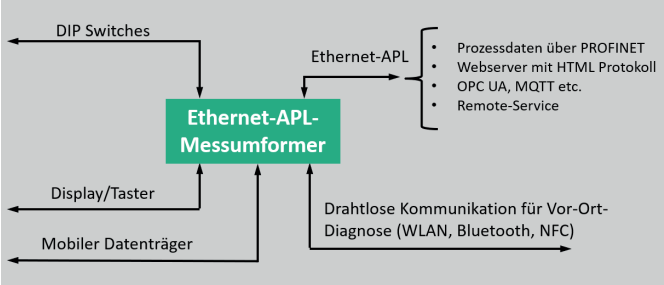

Abbildung 3: Exemplarischer Ethernet-APL Messumformer mit Schnittstellen

Nutzerkontenverwaltung aber auch durch digitale Zertifikate aus einer Public-Key-Infrastruktur (PKI-Zertifikate) erfolgen. Auch die Nutzung des Displays für die Eingabe von Konfigurationsdaten ist mitzubetrachten.

3.3.2 Nutzungskontrolle

Diese Anforderungsgruppe steht im Zusammenhang mit den Anforderungen aus dem vorangehenden Kapitel. Es wird gefordert, dass die Komponenten die geforderte Autorisierung auch durchsetzen und dass inaktive Sitzungen (z. B. Webserverzugriff durch Browser) automatisch geschlossen werden. Das gilt auch für Remote-Service-Verbindungen. Um einen übermäßigen Ressourcenverbrauch und eine möglicherweise damit einhergehende Fehlfunktion durch viele parallele Verbindungen zu verhindern, ist die Anzahl paralleler Verbindungen zu begrenzen. So könnte man z. B. festlegen, dass der Messumformer nur eine Verbindung des Webservers akzeptiert und weitere Verbindungsversuche ablehnt. Der Messumformer muss Security-relevante Ereignisse mit Zeitstempel protokollieren und für Analysezwecke persistent speichern.

3.3.3 Systemintegrität

Vorausgesetzt wird, dass die Kommunikationsverbindungen integritätsgeschützt sind. Hier kommt nun das PROFINET-Security-Konzept zum Tragen. Durch den Einsatz eines PROFINET-Protokollstacks mit Security-Funktion kann diese Forderung für die PROFINET-Schnittstelle erfüllt werden. Das gleiche gilt für die OPC-UA-Schnittstelle und für die Web-Server-Schnittstelle. Hier stehen jeweils sichere Protokollvarianten zur Verfügung. Die Schnittstellen müssen für eingehende Daten eine Validierung vornehmen. Z.B. sollen überlange oder falsch formatierte Datenpakete, die evtl. bewusst für einen Angriff verwendet werden, erkannt und verworfen werden. Dabei darf der Messumformer einem potenziellen Angreifer keine verwertbaren Rückinformationen liefern.
Die Integrität von Sitzungen soll durch individuell erzeugte Sitzungskennungen gewährleistet werden, die nach Ende der Sitzung zu verwerfen sind. Dies soll z. B. so genannte Replay-Angriffe verhindern. Auch diese Forderung wird durch das PROFINET-Security-Konzept gewährleistet.
Die Integrität des Boot-Prozesses muss gemäß der Norm ebenfalls sichergestellt werden.

3.3.4 Vertraulichkeit der Daten

Die Vertraulichkeit von Daten ist in der OT-Security, im Gegensatz zur IT-Security, von geringerer Bedeutung, weil

Tabelle 2: Security-Klassen bei PROFINET

Höchste gegenseitig unterstützte Security Klassen	GSD Dateien	Record-Data-Services		Echtzeitkommunikation	
	Integritätsschutz	Integritätsschutz	Vertraulichkeit	Integritätsschutz	Vertraulichkeit
1	V	–	–	–	–
2	V	√	√	√	–
3	V	√	√	√	√

(V: verpflichtend, –: nicht unterstützt, √: standardmäßig aktiviert)

Prozessdaten in der Regel einen geringen Schutzbedarf in Bezug auf die Vertraulichkeit haben. Dennoch wird dieses Thema in der Norm adressiert. Zum einen in Bezug auf den Schutz von ruhenden Daten, für die eine Leseberechtigung erforderlich ist, zum anderen in Bezug auf das Löschen von Daten, für die eine Leseberechtigung vorgesehen ist. Weiterhin fordert die Norm, dass die Komponente „*kryptografische Sicherheitsmechanismen nach den in der Informationstechnik allgemein anerkannten IT-Sicherheitsgepflogenheiten und -empfehlungen verwendet*“ [13].
Das PROFINET-Security-Konzept adressiert das Thema Vertraulichkeit in Form von drei verschiedenen Security-Klassen.
Tabelle 2 zeigt die drei Security-Klassen bei PROFINET. Security-Klasse 1 führt den Integritätsschutz bei GSD-Dateien ein. Klasse 2 ermöglicht einen Schutz der Integrität und Vertraulichkeit bei Record-Data-Services und einen Integritätsschutz bei der Echtzeitkommunikation. Klasse 3 ermöglicht dann ergänzend den Schutz der Vertraulichkeit bei der Echtzeitkommunikation. Diese Abstufung wurde gewählt, weil der Schutz der Vertraulichkeit durch Verschlüsselung rechenintensiv ist und weil davon ausgegangen wird, dass bei Echtzeitdaten lediglich ein geringer Bedarf in Bezug auf den Schutz der Vertraulichkeit besteht. Es wird daher unterstellt, dass in vielen Anwendungen lediglich Funktionen der Security-Klasse 2 zum Einsatz kommen werden.

3.3.5 Eingeschränkter Datenfluss

Bei dieser Anforderungsgruppe geht es im Wesentlichen um das Abschottungskonzept einer Produktionsanlage und die Aufteilung einer Anlage in verschiedene Security-Zonen. Dieser Aspekt wird, da er für einen Ethernet-APL-Messumformer irrelevant ist, in dieser Veröffentlichung nicht weiter betrachtet.

3.3.6 Rechtzeitige Reaktion auf Ereignisse

Dieser Aspekt der Norm betrachtet die Erfassung, Bereitstellung von Event-Logs sowie den Zugriff auf diese Logs. Zur Erstellung dieser Logs ist eine kontinuierliche Überwachung der Komponenten zu realisieren, um Sicherheitsverstöße erkennen und protokollieren zu können.

3.3.7 Verfügbarkeit der Ressourcen

Dieser Abschnitt der Norm widmet sich u.a. dem Schutz vor Denial-of-Service-Angriffen. Damit werden Angriffe angesprochen, die darauf abzielen, die Verfügbarkeit einer Ressource, z. B. durch Fluten des Gerätes mit Anfragen, zu kompromittieren. Zur Erfüllung dieser Anforderung müssen die Geräte ihre Ressourcen (z. B. Rechenleistung und Speicher) gegen Überlastung schützen. Das geschieht zum einen durch entsprechende Vorkehrungen im Protokollstack (Verwerfen von Datenpaketen bei Überlastung) zum anderen dadurch, dass z. B. die Anzahl paralleler Verbindungen begrenzt wird. Darüber hinaus wird eine Mindest-Lastfestigkeit für PROFINET Devices in [17] gefordert.
Die Aspekte Datensicherung, System-Wiederherstellung und Notstromversorgung sind für Ethernet-APL-Messumformer nicht relevant.
Weiterhin muss die Komponente die Konfiguration der Netzwerk- und Sicherheitseinstellungen unterstützen. So ist zu erwarten, dass sich nicht benötigte Dienste (z. B. Web-Server) deaktivieren lassen oder schon im Auslieferungszustand deaktiviert sind. Ziel ist es, das Gerät mit der gerade benötigten Funktionalität (geringste Funktionalität) zu betreiben und auf nicht benötigte Dienste zu verzichten, da diese potenzielle Einfallstore für Angreifer sein könnten.
Das Erstellen eines Asset-Inventories (Liste aller Komponenten einer Anlage mit deren Hardware- und Software-Version) ist eine grundlegende Maßnahme in der OT-Security. Von den Komponenten wird erwartet, dass diese die Erstellung eines solchen Inventories durch ein entsprechendes Interface unterstützen.

3.4 Anwendbarkeit und Umsetzung der technischen Anforderungen auf einen Ethernet-APL-Messumformer.

Die Auflistung der verschiedenen Anforderungen in Kapitel 3.3 hat drei Klassen von Anforderungen aus der IEC-62443-4-2 aufgezeigt:

1. Anforderung ist für einen Ethernet-APL Messumformer irrelevant: Z. B. Notstromversorgung, Schutz der Zonengrenze

2. Anforderung ist relevant und durch das PROFINET-Security Konzept abgedeckt: Z. B. Integritätsschutz der Kommunikation, Vertraulichkeitsschutz der Kommunikation.

3. Anforderung ist relevant, aber vom Feldgerät abhängig: Z. B. Integritätsschutz der Software beim SW-Update, Integrität des Boot-Prozesses (engl. Secure-Boot), etc.

Darüber hinaus sind ggf. weitere gerätespezifische Anforderungen zu ergänzen, die im Rahmen der Risikoanalyse (Siehe Kapitel 3.1.2) ermittelt wurden.

Für Feldgerätehersteller ist eine entsprechende Einordnung der Anforderungen der IEC 62443-4-2 wichtig, damit klar ist, welche Anforderungen den Hersteller selbst betreffen. Das PROFINET-Security-Konzept liefert einen wesentlichen Baustein zu Absicherung der PROFINET-Kommunikation. Es ist jedoch zu beachten, dass der Gerätehersteller weitere Security-Anforderungen, die das Gerät selber betreffen, zusätzlich zu berücksichtigen hat. Die Arbeitsgruppe CB/PG10 PROFINET Security von PROFIBUS & PROFINET International erarbeitet derzeit eine Tabelle, die eine entsprechende Einordnung vornimmt. Zu gegebener Zeit wird diese Tabelle der Allgemeinheit zur Verfügung gestellt werden.
Es ist weiterhin zu beachten, dass die Norm IEC 62443-4-2 für steigende Security-Level zusätzliche Anforderungen (so genannte Requirement Enhancements) definiert. Bei einer detaillierten Analyse der Anforderungen ist demzufolge der angestrebte Target-Security-Level zu beachten.

4. Zusammenfassung

Dieser Beitrag liefert einen Einstieg und einen groben Überblick über die beiden Normen. Es ist in jedem Fall erforderlich, die Normen für die weitere Arbeit heranzuziehen.
Die Ausführungen der vorangehenden Kapitel haben am Beispiel eines Ethernet-APL-Messumformers gezeigt, dass Feldgerätehersteller zwei wesentliche Aufgaben zu bewältigen haben. Zum einen sind die Entwicklungsprozesse am sicheren Entwicklungslebenszyklus nach IEC 62443-4-1 [12] auszurichten. Zum anderen sind die Komponentenanforderungen nach der IEC 62443-4-2 [13] bei der Entwicklung der Hard- und Software zu beachten. PROFIBUS & PROFINET International stellt mit der aktuellen PROFINET Spezifikation die wesentlichen Bausteine für die Absicherung der PROFINET Kommunikation zur Verfügung. Dennoch müssen die Hersteller von Ethernet-APL-Messumformern eine Reihe weiterer Anforderungen bei der Entwicklung ihrer Komponenten beachten, die nicht durch das PROFINET Protokoll abgedeckt sind.
Nach erfolgter Umsetzung der beiden Normteile können Hersteller die Entwicklungsorganisation und das Produkt zertifizieren lassen. Diese Zertifizierung erfolgt durch einen externen Zertifizierer. Es ist zu beachten, dass neben dem initialen Audit wiederkehrende Audits erforderlich sind.

5. Danksagung

Die Ergebnisse dieses Beitrags basieren auf der Arbeit der Arbeitsgruppe CB/PG10 PROFINET Security. Die Autoren danken den Arbeitskreismitgliedern für ihren Beitrag, ohne den dieser Artikel nicht möglich gewesen wäre.

Referenzen

[1] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO. Version 2.4 MU4 Order- Nr. 2.722, 2023. https://www.profibus.com/download/profinet-specification.

[2] PROFIBUS Nutzerorganisation e.V.: Application Layer services for decentralized periphery. Technical Specification for PROFINET IO, Version 2.4 MU4 – Nov. 2022 Nr. 2.712, 2023. https://de.profibus.com/downloads/profinet-specification/.

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

[4] Niemann, K.-H.: IT security extensions for PROFINET. 17th International Conference on Industrial Informatics (INDIN). IEEE 2019. S. 407–412. DOI: 10.1109/INDIN41052.2019.897220.

[5] Niemann, K.-H., Walz, A. u. Sikora, A.: Security Extensions for PROFINET. Concepts, Status, and Prospects. Embedded World Conference 2023 Proceedings. WEKA Fachmedien GmbH 2023, S. 99–104.

[6] Niemann, K.-H.; Walz, A.; Merklin, S.; Ziegler, D.; Waldeck, B.: PROFINET — Sichere Kommunikation im Produktionsbereich. Wie kann PROFINET zur Erfüllung der Anforderungen der IEC 62443 beitragen? In (VDI-Wissensforum GmbH Hrsg.): 24. Leitkongress der Mess- und Automatisierungstechnik Automation 2023. Transformation by Automation. VDI-Verlag GmbH, 2023; S. 391–402.

[7] Niemann, K.-H. u. Merklin, S.: OT Security Requirements for Ethernet-APL field devices. atp magazin 63 (2022) 5, S. 44–51. DOI: https://doi.org/10.25968/opus-2603.

[8] PROFIBUS Nutzerorganisation e.V.: OT-Security für Produktionsanlagen mit PROFINET. Eine Einordnung der IEC 62443 für Betreiber, Integratoren und Hersteller Nr. 7.341, 2022. https://www.profibus.com/download/white-paper-ot-security-classification-of-iec62443.

[9] Niemann, K.-H. u. Merklin, S.: IT-Security für Automatisierungssysteme mit Ethernet-APL-Feldgeräten - Anforderungen und Schutzmaßnahmen. Automation 2022 - Automation creates sustainability. 23. Leitkongress der Mess- und Automatisierungstechnik. Düsseldorf: VDI Verlag GmbH 2022, S. 149–160.

[10] Niemann, K.-H. u. Merklin, S.: OT-Sicherheitsanforderungen für Ethernet-APL-Feldgeräte: Technologischer Wandel kann zu besserem Schutz führen. Deutsche Fassung des englischen Originalbeitrags. atp Magazin 63 (2022) 5. https://doi.org/10.25968/opus-2320.

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

[12] DIN EN IEC 62443-4-1 (VDE 0802-4-1):2018-10. IT -Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1 :2018); Deutsche Fassung EN lEC 62443-4-1 :2018

[13] DIN EN IEC 62443-4-2 (VDE 0802-4-2):2019-12. 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

[14] Department of Homeland Security: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Recommended Practice, 2009. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf.

[15] Kuipers, D. u. Fabro, M.: Control Systems Cyber Security: Defense in Depth Strategies INL/EXT-06-11478, 2006. https://www.osti.gov/biblio/911553.

[16] Abdelghani, T.: Implementation of Defense in Depth Strategy to Secure Industrial Control System in Critical Infrastructures. American Journal of Artificial Intelligence 3 (2019) 2, S. 17

[17] PROFIBUS Nutzerorganisation e.V.: PROFINET Netload Robustness Guideline (former Security Level 1 Netload). (former Security Level 1 Netload) Nr. 7.302, 2022. https://www.profibus.com/download/profinet-netload-robustness-guideline-former-security-level-1-netload

[18] Broekman, B. u. Notenboom, E.: Testing embedded software. London: Addison-Wesley 2008

[19] Grünfelder, S.: Software-Test für Embedded Systems. Ein Praxishandbuch für Entwickler, Tester und technische Projektleiter. dpunkt.verlag 2013
[20] Vigenschow, U.: Testen von Software und Embedded Systems. Professionelles Vorgehen mit modellbasierten und objektorientierten Ansätzen. Heidelberg: dpunkt.Verl. 2010
[21] ISO/IEC FDIS 30111:2019(E):2019-07. Information technology — Security techniques — Vulnerability handling processes
[22] ISO/IEC 29147:2018(E):2018-10. Information technology — Security techniques — Vulnerability disclosure
[23] Fuhr, David et al.: Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau, 2016. https://industrialsecurity.vdma.org/documents/16227999/16499033/1492086887896_INS_NAM_2016_Industrial_Security_IEC62443.pdf/c2e80bdb-c820-42cb-b3cc-fedd68571e1e

AUTOREN

Prof. Dr.-Ing. Karl-Heinz Niemann (geb. 1959) vertritt seit 2005 die Bereiche Prozessinformatik und Automatisierungstechnik an der Hochschule Hannover (HsH). Seit Anfang 2023 ist er Vorstand des Institutes für Sensorik und Automation der HsH. Zusätzlich ist er im Mittelstand Digitalzentrum Hannover und im Zukunftslabor Produktion des ZDIN tätig. Von 2002 bis 2005 war er an der Fachhochschule Nordostniedersachsen (heute Leuphana Universität) für den Bereich Prozessdatenverarbeitung zuständig. Zuvor war er in führenden Positionen in der Entwicklung von Prozessleitsystemen bei ABB, Elsag Bailey und Hartmann & Braun tätig.

Kontakt
Hochschule Hannover
Fakultät I - Elektro- und Informationstechnik
Postfach 92 02 61, 30441 Hannover
✆ Tel. +49 511 92 96 12 64
@ Karl-Heinz.Niemann@HS-Hannover.de
https://hs-h.de/isa
https://orcid.org/0000-0001-8931-6789

Dipl.-Phys. Andreas Walz ist wissenschaftlicher Mitarbeiter am Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) an der Hochschule Offenburg. Zu seinen Forschungsgebieten gehört die Cybersicherheit in industriellen Automatisierungsanlagen. Neben seiner Beteiligung an den Arbeiten innerhalb des PI-Arbeitskreises CB/PG10 Security, ist er aktiver Teilnehmer weiterer Industriearbeitskreise, wie z. B. der IG safety/security bei CAN in Automation e. V. sowie der Industrial Ethernet Security Harmonization Group, einer Gruppe von Cybersecurity-Experten von OPCF, FieldComm Group, ODVA, und PI.

M. Sc. Simon Merklin (geb. 1989) ist Cyber Security Spezialist und Leiter des Product Security Marketings bei Endress+Hauser. Er hat am Karlsruher Institut für Technologie Wirtschaftsinformatik mit Schwerpunkt Sicherheit und Kryptographie studiert und seine Masterarbeit über Distributed Ledger Technologies geschrieben. Darüber hinaus war er an der IEC 62443-4-1 Zertifizierung von Endress+Hauser beteiligt und ist Mitglied der PROFINET Security Working Group bei PROFIBUS und PROFINET International.

Dr.-techn. Dominik Ziegler ist Security Expert bei Siemens AG. Sein Schwerpunkt liegt auf der industriellen Kommunikationssicherheit. Er leitet den PI-Arbeitskreis CB/PG10 Security, welcher sich mit der Entwicklung von Sicherheitsstandards und -protokollen für industrielle Automatisierungssysteme auf Basis von PROFINET beschäftigt. Neben seiner Arbeit an der Entwicklung von Kommunikationsstandards beschäftigt sich er sich auch mit den Auswirkungen nationaler Vorschriften wie der EU CRA und internationaler Standards wie der IEC 62443.

Dipl.-Ing. Boris Waldeck ist Master Specialist Security PLCnext Technology und Product Solution Security Expert bei Phoenix Contact Electronics GmbH in Bad Pyrmont. Er ist verantwortlich für die IEC 62443-4-1 SDL Zertifizierung der BU Automation Systems und die IEC 62443-4-2 Produktzertifizierung der PLCnext Control. Als PSSE unterstützt er bei der Einführung des SDL und Produktzertifizierungen nach IEC 62443 mit Blick auf die in der EU kommenden gesetzlichen Regelungen CRA und NIS2.