



PROFINET- Zukünftige OT-Security- Anforderungen : Was fordern NIS2, CER, CRA und IEC 62443

Karl-Heinz Niemann, Boris Waldeck, Timon Eßlinger

Suggested citation:

Niemann, Karl-Heinz, Boris Waldeck, and Timon Eßlinger. 2025. "PROFINET- Zukünftige OT-Security- Anforderungen : Was fordern NIS2, CER, CRA und IEC 62443." *atp Magazin*, no. 2025/09: 46–53. <https://doi.org/10.25968/opus-3710>.

Abstract

Hersteller, Integratoren und Betreiber von Produktionsanlagen müssen sich zunehmend regulatorischen Anforderungen in Bezug auf die OT-Security stellen. Darüber hinaus sind Hersteller gut beraten, wenn sie einschlägigen OT-Security-Normen wie der IEC 62443 folgen. Aus den beschriebenen Anforderungen folgt, dass die „Security“ der industriellen Kommunikation über entsprechende Schutzmaßnahmen sicherzustellen ist. Dieser Beitrag zeigt, wie das Kommunikationsprotokoll PROFINET zurzeit ertüchtigt wird, um die Anforderungen zu erfüllen.

Terms of use

CC BY 4.0



PROFINET- Zukünftige OT-Security- Anforderungen

Was fordern NIS2, CER, CRA und IEC 62443

#PROFINET Security #Cyber Resilience Act #NIS-2-Richtlinie
#CER-Richtlinie

Hersteller, Integratoren und Betreiber von Produktionsanlagen müssen sich zunehmend regulatorischen Anforderungen in Bezug auf die OT-Security stellen. Darüber hinaus sind Hersteller gut beraten, wenn sie einschlägigen OT-Security-Normen wie der IEC 62443 folgen. Aus den beschriebenen Anforderungen folgt, dass die „Security“ der industriellen Kommunikation über entsprechende Schutzmaßnahmen sicherzustellen ist. Dieser Beitrag zeigt, wie das Kommunikationsprotokoll PROFINET zurzeit ertüchtigt wird, um die Anforderungen zu erfüllen.

Manufacturers, integrators, and operators of production systems must increasingly face regulatory requirements with regard to OT security. In addition, manufacturers are well advised to follow relevant OT security standards such as IEC 62443. It follows from the requirements described that the "security" of industrial communication must be ensured via appropriate protective measures. This article shows how the PROFINET communication protocol is currently being upgraded to meet the requirements.

Karl-Heinz Niemann,
Hochschule Hannover
Boris Waldeck,
Phoenix Contact
Timon Eßlinger,
Codewerk

► **PEER-REVIEW:**
7.8.2025

1. Anforderungen an künftige Lösungen

Dieser Abschnitt beschreibt die Anforderungen, die an künftige Automatisierungslösungen zu stellen sind. Hierbei wird zwischen gesetzlichen Anforderungen (Kapitel 1.1) und den Anforderungen aus dem Stand der Technik (Kapitel 1.2) unterschieden.

1. 1 Gesetzliche Anforderungen

Die zunehmende Vernetzung und Digitalisierung in der Industrie haben die Security-Anforderungen deutlich erhöht. Um ein hohes Maß an Cybersicherheit in der gesamten EU zu gewährleisten, wurden mehrere rechtliche Rahmenbedingungen geschaffen, so dass es wichtig ist, dass industrielle Kommunikationsprotokolle wie PROFINET ihre Security-Maßnahmen zur Erfüllung dieser Anforderungen verbessern. Die folgenden Abschnitte beschreiben die gesetzlichen Anforderungen aus verschiedenen Sichten der am Security-Prozess beteiligten Stakeholder.

Betreibersicht: Die NIS2-Richtlinie (Netz- und Informationssicherheitsrichtlinie) [1] ist eine EU-Richtlinie, die darauf abzielt, ein hohes gemeinsames Cybersicherheitsniveau in allen Mitgliedstaaten zu gewährleisten. Sie definiert koordinierte Security-Maßnahmen, Risikomanagement und die Meldung von Vorfällen, um die allgemeinen Cybersicherheitsmaßnahmen in in der EU ansässigen Unternehmen zu verbessern. Die NIS2-Richtlinie adressiert wichtige und besonders wichtige Einrichtungen in definierten Sektoren, wie z. B. Öffentliche Verwaltung, Digitale Infrastruktur, Wasser & Abwasser, Gesundheit, Banken & Finanzen, Transport, Energie, Service Provider, Post und Kurier, Abfall, Chemikalien, Lebensmittel, Industrie sowie Forschung. In Deutschland sind geschätzt ca. 30.000 Unternehmen betroffen. Darüber hin-

aus müssen die betroffenen Unternehmen eine bestimmte Größe in Bezug auf Umsatz und Mitarbeiterzahl überschreiten. Sie ist durch die Mitgliedstaaten der EU jeweils in nationales Recht umzusetzen. Die Umsetzung hätte in Deutschland bis Oktober 2024 erfolgen müssen. Dies ist allerdings bisher (Stand Juli 2025) nicht erfolgt. Die deutsche Umsetzung in Form des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes [2] ist vor der Bundestagswahl nicht mehr im Bundestag verabschiedet worden. Das Gesetzesverfahren ist nun neu zu starten. Trotz der fehlenden Umsetzung sind Betreiber gut beraten, mit der Umsetzung der Maßnahmen auf Basis der NIS2-Richtlinie zu beginnen.

Artikel 21 (1) der NIS2-Richtlinie [1] befasst sich mit Risikomanagementmaßnahmen im Bereich der Cybersicherheit. Sie fordert, dass geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen werden, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Security-Vorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Die in der Richtlinie genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.



Abbildung 1: Grundlegende Anforderungen des CRA.

Es ist also zu erkennen, dass die NIS2-Richtlinie auf den Stand der Technik, auf Normen und auf die Verhältnismäßigkeit der Maßnahmen abhebt. Weiterhin fordert die NIS2-Richtlinie auch die Sicherstellung der Cyber-Sicherheit längs der Lieferkette. Hier kommen nun die Hersteller ins Spiel.

Für Betreiber aus kritischen Sektoren (z. B. Energie, Verkehr, Trinkwasser, Abwasser u. a.) gilt zusätzlich die CER-Richtlinie (EU) 2022/2557 [3], sofern diese als kritische Einrichtungen eingestuft sind. Diese Richtlinie adressiert insbesondere Resilienz-Maßnahmen wie Katastrophenvorsorge, physischen Zugangsschutz, Maßnahmen zum Risikomanagement, personenbezogenes Security-Management und Awareness-Schulungen.

Herstellersicht: Der Cyber Resilience Act (CRA) [4] zielt auf die Verbesserung der Cybersicherheit für Produkte mit digitalen Elementen ab. Sie legt gemeinsame Cyber-Security-Standards in der gesamten EU fest und verpflichtet die Hersteller, die Security ihrer Produkte während ihres gesamten Lebenszyklus zu gewährleisten. Der CRA schreibt grundlegende Anforderungen an das Design, die Entwicklung und die Produktion dieser Produkte sowie Verpflichtungen für den Umgang mit Schwachstellen vor.

Abbildung 1 zeigt die grundlegenden Anforderungen des CRA.

Im Unterschied zur NIS2-Richtlinie ist der CRA ohne Umsetzung in nationales Recht gültig. Das bedeutet:

- Ab dem 11. September 2026 sind aktiv ausgenutzte Schwachstellen an nationale Behörden und die ENISA zu melden. Siehe Artikel 14.
- Ab dem 11. Dezember 2027 gelten alle Anforderungen des CRA. Das CE-Kennzeichen dokumentiert dann, dass ein Produkt mit digitalen Elementen die Anforderungen des CRA erfüllt.

Der CRA wird ab Dezember 2027 den Nachweis der Security längs der Lieferkette für die Betreiber von Anlagen, die unter die NIS2-Richtlinie fallen, entsprechend vereinfachen.

Maschinenbauersicht: Die EU-Maschinenverordnung (2023/1230) [5], im Weiteren MVO genannt, betont die Bedeutung der Cybersicherheit bei der Konstruktion und dem Bau von Maschinen. Sie schreibt vor, dass Hersteller sicherstellen müssen, dass ihre Maschinen während ihres gesamten Lebenszyklus vor Cyberbedrohungen geschützt sind, wobei sowohl die funktionale Sicherheit als auch die Cybersicherheit berücksichtigt werden müssen. Die MVO hebt u. a. auch einen „Schutz vor Korruption“ für Software und Daten hervor.

1.2 Anforderungen aus dem Stand der Technik

Obwohl in [6] aus juristischer Sicht hinterfragt wird, ob Normen den Stand der Technik ausreichend beschreiben, sollen in diesem Beitrag Normen als wesentliche Basis für die Beurteilung dienen. Abbildung 2 fokussiert auf die Herstellersicht und zeigt den Zusammenhang zwischen CRA und MVO in Bezug auf die zu erwartende Normung.

genden Anforderungen in Bezug auf Integrität, Authentizität und ggf. auch Vertraulichkeit im Bereich der industriellen Kommunikation zu erfüllen. Die Spezifikationsarbeiten für PROFINET Security wurden bereits vor einigen Jahren begonnen und liegen in der PROFINET-Spezifikation vor. Die neueste Version 2.4 MU 6 [12] wurde im Sommer 2025 veröffentlicht und löst die MU5 [11] ab.

zusammenfassend die Einflussfaktoren, die auf PROFINET Security wirken. Die NIS2-Richtlinie wirkt dabei nur indirekt über die Forderung nach der Sicherheit der Lieferkette. CRA und MVO wirken mit ihren spezifischen Anforderungen sowohl auf das Produkt selbst als auch auf den Entwicklungslebenszyklus. Die IEC 62443-4-1 wirkt auf den Entwicklungslebenszyklus, die IEC 62443-4-2 auf das Produkt.

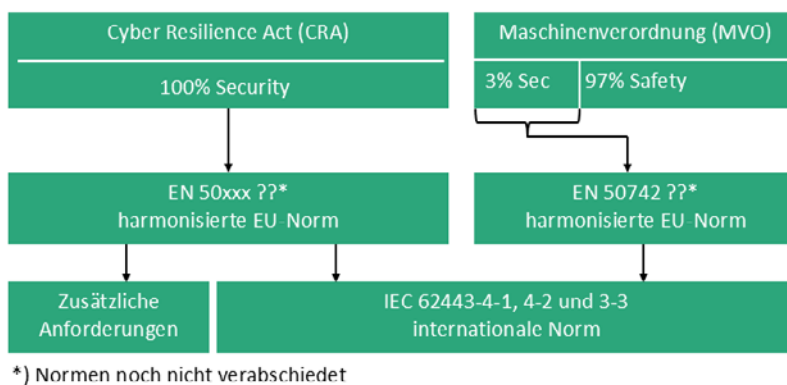


Abbildung 2: Wie passen EU-Maschinenverordnung und Cyber-Resilience-Act zusammen?

Abbildung 2 zeigt zunächst, dass CRA und MVO OT-Security-Anforderungen definieren. Während der CRA sich vollständig auf die Security fokussiert, ist bei der MVO die Security nur ein kleiner Teil. Der Rest betrachtet die funktionale Sicherheit (Safety).

1.3 Auswirkungen der Anforderungen auf PROFINET Security

Um die beschriebenen gesetzlichen Anforderungen zu erfüllen, ist es für PROFINET unerlässlich, die grundle-

Die Arbeiten haben sich dabei im Wesentlichen an den Anforderungen der IEC 62443-4-2 [9] orientiert. Ein Teil der Anforderungen wird durch das PROFINET-Protokoll direkt erfüllt, ein Teil der Anforderungen, die nicht PROFINET-spezifisch sind, muss durch die Hersteller erfüllt werden. Eine vollständige Auflistung des Erfüllungsgrades der Anforderungen ist in diesem Beitrag aus Platzgründen nicht möglich. PI arbeitet zurzeit an einem entsprechenden Dokument. Abbildung 3 zeigt

2. Beschreibung PROFINET Security

Das folgende Kapitel zeigt, mit welchen Security-Merkmalen PROFINET die in Kapitel 1 definierten Anforderungen technisch umsetzt. PROFINET Security wird in die Klassen 1 (Robustness), 2 (Integrity & Authenticity) und 3 (Confidentiality) unterteilt. Die höhere Security-Klasse beinhaltet stets die Anforderungen der niedrigeren Klasse. Klasse 1 beinhaltet Absicherungen gegen bekannte Angriffe, jedoch keine kryptografische Absicherung der Daten auf Protokollebene. Mit Klasse 2 werden die Authentizität und Integrität des PROFINET-Protokolls sichergestellt. Klasse 3 stellt, zusätzlich zur Klasse 2, Verschlüsselung der IO-Daten bereit, um Vertraulichkeit zu gewährleisten.

PROFINET Security berücksichtigt nicht die Absicherung zwischen Controller und Engineering-Tool. Diese Absicherung muss der Hersteller selbst vornehmen.

Die Spezifikation der Security-Klasse 1 ist unter [10] verfügbar. Klasse 2 und 3 sind spezifiziert und wurden mit der PROFINET-Protokollspezifikation MU6 im Sommer 2025 veröffentlicht.

Betreiber sollten sich die Frage stellen, welche Security-Klasse benötigt wird. Die Vertraulichkeit der Daten (Klasse 3) spielt im industriellen Umfeld meist

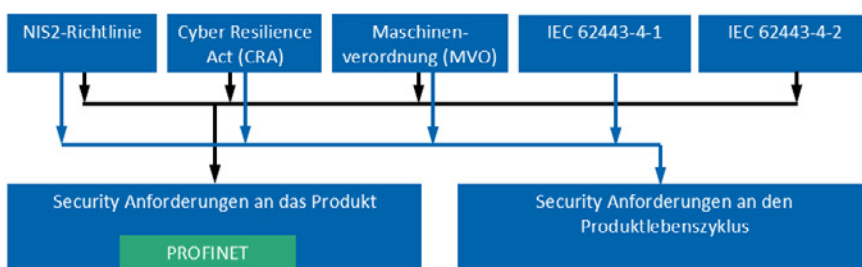


Abbildung 3: Einflussfaktoren auf PROFINET Security

eine untergeordnete Rolle. Viel wichtiger ist es, die Datenauthenticität und -integrität sicherzustellen, wofür Security-Klasse 2 ausreicht. Wenn Vertraulichkeit jedoch unabdingbar ist, beispielsweise bei der Übertragung geheimer Rezepturen, muss Klasse 3 gewählt werden.

2.1 Security-Klasse 1

Klasse 1 – umgangssprachlich „Robustness“ – bietet drei Kernfunktionalitäten, die eine schrittweise Verbesserung des bestehenden Zonenschutzes ermöglichen.

1. DCP-Read-Only-Mode: Sobald eine PROFINET Application Relation (PN-AR) zwischen Controller und Device abgeschlossen aufgebaut ist, kann mit DCP lediglich lesend zugegriffen werden. Dadurch werden Angriffe verhindert, bei denen die IP-Adresse oder der Name-of-Station im laufenden Betrieb per DCP geändert werden, um Kommunikationsabbrüche herbeizuführen.
2. SNMPv1/v2-Konfiguration: Da das von PROFINET genutzte Netzwerkprotokoll SNMPv1/v2 keine Authentisierung bietet, kann über Klasse 1 SNMP entweder komplett deaktiviert, in einen Read-Only-Modus versetzt oder die SNMP-Community-Strings individuell für den Schreib- bzw. Lesezugriff freigeschaltet werden.
3. GSDX: In der Vergangenheit hatten Endanwender keine Möglichkeit, die Echtheit einer GSD-Datei zu verifizieren – etwa, ob sie tatsächlich vom angegebenen Hersteller stammt – oder sicherzustellen, dass deren Inhalte (wie IDs, Parameter etc.) nicht verändert wurden. Das GSDX-Format erweitert dafür die bestehende GSD mit einer Signatur durch den Produkthersteller. In Abbildung 4 ist der Ablauf des GSD-Signie-

rungs-Prozesses dargestellt. Der Hersteller kann mithilfe eines Signing-Tools der PI und seines eigenen Hersteller-Zertifikats die GSD-Datei signieren und als GSDX bereitstellen. Kompatible Engineering-Tools können GSDX-Dateien importieren und Signaturen auf deren Echtheit hin überprüfen. Zur Signaturprüfung muss das Engineering-Tool nicht mit dem Internet verbunden sein, da die gesamte Zertifikatskette innerhalb der GSDX-Datei eingebettet ist. Abbildung 4 zeigt den Signierungsvorgang der GSD-Datei und die Verifikation beim Nutzer.

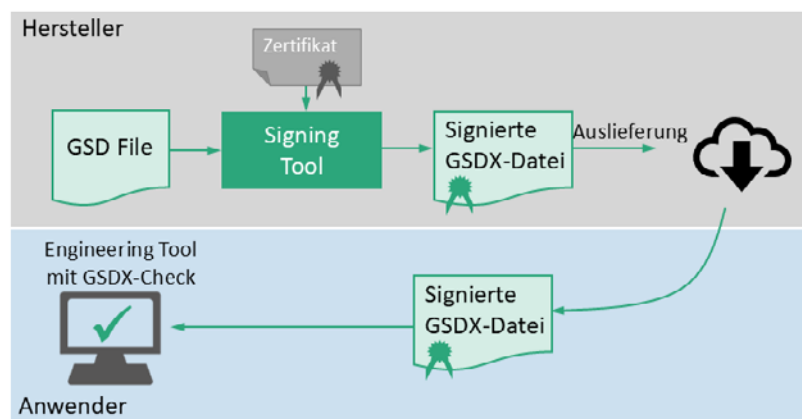


Abbildung 4: Signierung der GSD-Datei und Verifikation beim Nutzer

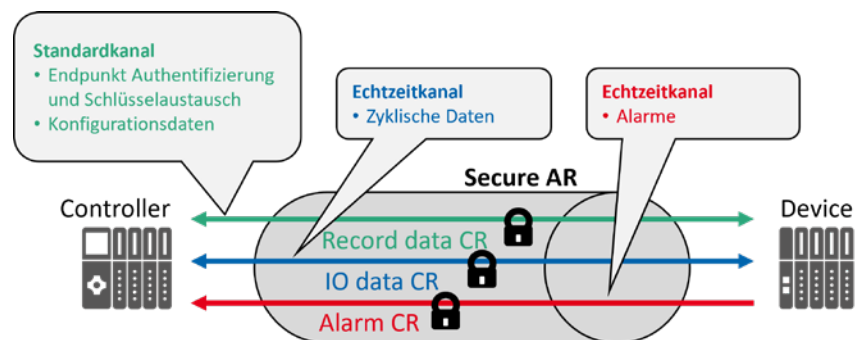


Abbildung 5: PROFINET Sichere AR mit mehreren Kommunikationsbeziehungen

2.2 Security-Klasse 2 und 3

Security-Klasse 2 gewährleistet, dass Angreifer keine unbemerkten Manipulationen an PROFINET-IO-Daten vornehmen können. Die Klasse 3 bietet zusätzlich Verschlüsselung, sodass eine Interpretation der Daten durch Angreifer nicht möglich ist.

Der Kern der Security-Klasse 2 ist die Absicherung der PROFINET-Application Relation (AR) zwischen Controller und Device, wobei sich beide Endpunkte beim Hochlauf gegenseitig über X.509-Zertifikate [13] authentifizieren. Hier wird das Protokoll EAP-TLS sowohl für Security-Klasse 2 als auch für Security-Klasse 3 verwendet. Nach erfolgreicher Authentisierung handeln beide Teilnehmer einen gemeinsamen symmetrischen Schlüssel für die Datenübertragung der Record-Daten, I/O-Daten und Alarme aus. Zur Aufrechterhaltung eines hohen Schutzniveaus wird der symmetrische Schlüssel während

der Kommunikation in regelmäßigen Abständen aktualisiert.

Mithilfe des symmetrischen Schlüssels werden die drei in Abbildung 5 dargestellten Kommunikationsbeziehungen abgesichert. Der Schutz von Integrität und

Tabelle 1: Übersicht der Security-Klassen. Legende: (V) Verpflichtend, (-) Nicht unterstützt (✓) Funktion unterstützt, kann durch Konfiguration aktiviert werden

Höchste gegenseitig unterstützte Sicherheitsklasse	GSD-Datei	Record CR		I/O-Daten CR		Alarm CR	
	Integrität, Authentizität	Integrität, Authentizität	Vertraulichkeit	Integrität, Authentizität	Vertraulichkeit	Integrität, Authentizität	Vertraulichkeit
1	V	-	-	-	-	-	-
2	V	✓	-	✓	-	✓	-
3	V	✓	✓	✓	✓	✓	✓

Authentizität wird für alle drei Kommunikationsbeziehungen mittels eines Message Authentication Codes (MAC) gewährleistet. Die Vertraulichkeit wird dagegen erst bei Klasse 3 für die I/O-Daten eingeführt. Eine Übersicht der verschiedenen Stufen ist in Tabelle 1 dargestellt. Durch authentifizierte und autorisierte Konfiguration kann die Verschlüsselung für Fehleruntersuchungen deaktiviert werden.

Mit den Security-Klassen 2 und 3 ist es ebenfalls möglich, die Kommunikationsbeziehungen (CRs) zwischen abgesicherten und nicht abgesicherten Teilnehmern granular zu steuern. So kann der Betreiber einen Mischbetrieb zwischen sicheren und unsicheren Teilnehmern erlauben. Falls dies nicht gewünscht ist, kann das Gerät über den sogenannten „Security Mode“ – nicht zu verwechseln mit der Security-Klasse – in den Zustand versetzt werden, dass ausschließlich sichere Verbindungen zum Gerät zugelassen sind.

2.3 Zertifikatsmanagement

Um eine sichere Kommunikation innerhalb eines PROFINET-IO-Systems zu gewährleisten, werden die Geräte gemäß IEEE 802.1 AR [14] mit Zertifikaten und privaten Schlüsseln ausgestattet. Bei PROFINET Security werden folgende X.509-Zertifikate betrachtet:

IDeVID (Initial Device Identifier): Hier handelt es sich um ein nicht löschbares Zertifikat, das initial vom Hersteller ins Gerät eingebracht wird und in einem TPM (Trusted Platform Module)

oder einem anderen sicheren Element verwaltet wird. Das Zertifikat wird üblicherweise über die Hersteller-PKI signiert. Die IDeVID hat keine direkte Funktion für PROFINET Security, mit ihr kann jedoch ein sicheres Onboarding des Devices beim Betreiber erfolgen.

LDeVID-Generic (Local Device Identifier – Generic): Dieses Zertifikat wird vom Anlagenbetreiber auf das Gerät gebracht und bildet die weitere Basis für das Einbringen bzw. Austauschen des LDeVID-PN-Zertifikats.

LDeVID-PN (Local Device Identifier – PROFINET): Dieses Zertifikat ist applikationsspezifisch und wird bei PROFINET Security für die gegenseitige Authentisierung zwischen PROFINET-Controller und Device eingesetzt.

Mit der Einführung der PROFINET-Security-Klassen 2 und 3 wurde das sogenannte PROFINET-Security-Configuration-Management (SCM) geschaffen. Diese Protokollerweiterung ermöglicht den geschützten Umgang mit sensiblen, Security-relevanten Daten. Eine zentrale Rolle in diesem Prozess nimmt der Security-Infrastructure-Handler (SIH) ein – eine neu definierte Funktionseinheit, die für die Initiierung und Steuerung des Austauschs von SCM-Protokollen zwischen den beteiligten PROFINET-Komponenten verantwortlich ist.

Zu den Aufgaben des SIH gehören unter anderem das Bereitstellen, Aktualisieren, Entfernen und Deaktivieren von

Security-Konfigurationen, Zertifikaten, Schlüsseln und Vertrauensankern. In der Praxis ist diese Funktionalität meist direkt im PROFINET-Controller integriert, kann aber alternativ auch durch spezielle Engineering- oder Diagnosewerkzeuge bereitgestellt werden.

3. Security-Planung einer PROFINET-Anlage

Zur Erfüllung der Anforderungen, die im Kapitel 1 beschrieben wurden, sind neben den technischen Eigenschaften der verwendeten Komponenten zusätzlich im Rahmen der Planung generische Aufgaben zu erledigen, die im Folgenden kurz beschrieben werden:

Bestimmung der Bestandteile und Komponenten, die während des Security-Planungsprozesses berücksichtigt werden müssen.

Ermittlung bereits vorhandener Dokumente, die vom Kunden oder Anlagenbetreiber erstellt wurden, wie beispielsweise Risikoeinschätzungen oder die Definition des Security-Kontextes.

Festlegung des Security-Kontextes: Dieser umfasst die Risikobewertung und die Schutzmaßnahmen, die sich aus der Betriebsumgebung des Systems ergeben. Dabei spielen Standort, Einsatzzweck, Betriebsbedingungen, externe Schutzvorkehrungen und bekannte Bedrohungen eine Rolle.

Durchführung einer Bedrohungs- und Risikoanalyse, z. B. nach IEC 62443-3-2

[15] oder nach VDI 2182 [16]: Ziel dieser Untersuchung ist die Identifizierung potenzieller Gefahren für das Automatisierungssystem oder die Produktionsanlage. Auf Basis des möglichen Schadensausmaßes und der Wahrscheinlichkeit des Ereignisses wird eine Risikoanalyse erstellt. Falls erforderlich, werden Maßnahmen zur Risikominimierung formuliert und die erforderlichen Security-Level gemäß IEC 62443 definiert.

Erarbeitung des Defense-in-Depth-Konzeptes [17]: Dieses Konzept beruht auf der Implementierung mehrerer Security-Schichten, um ein hohes Schutzniveau zu gewährleisten und die Auswirkungen des Ausfalls einzelner Security-Komponenten zu minimieren. Durch die Kombination verschiedener Schutzmaßnahmen auf unterschiedlichen Ebenen wird die Security der Anlage insgesamt erhöht.

Netzwerkplanung und Festlegung von Zonen und Conduits. Die OT-Security basiert unter anderem auf der gezielten Segmentierung von Netzwerken, um das Automatisierungsnetz vor externen Bedrohungen zu schützen. Dabei werden verschiedene Netzwerksegmente als Zonen definiert. Ein Conduit stellt eine logische Gruppierung von Kommunikationskanälen dar, die Security-Anforderungen für die Verbindung zwischen zwei oder mehr Zonen erfüllen. Zur Erläuterung der Zonen und Conduits siehe IEC 62443-1-1 [18].

Definition grundlegender Security-Merkmale für das Automatisierungssystem oder die Produktionsanlage.

Planung spezifischer PROFINET-Security-Funktionen gemäß den Anforderungen. Siehe hierzu den folgenden Abschnitt.

Dokumentation der Ergebnisse aus dem Planungsprozess.

Einholen der Genehmigung oder Abzeichnung durch den Kunden oder Anlagenbetreiber für die festgelegte Security-Planung.

Für weitere Details bzgl. der Planung sei auf die IEC 62443-2-4 [19] verwiesen. Die hier beschriebenen Planungsschritte sind sinnvoll, um die planungsspezifischen Schritte zur Erfüllung der gesetzlichen und normativen Anforderungen gemäß Kapitel 1 vorzubereiten. Die beschriebenen Arbeitsschritte sind unabhängig vom eingesetzten Kommunikationssystem und somit unabhängig von PROFINET. Im folgenden Abschnitt sollen nun die PROFINET-spezifischen Planungsschritte beschrieben werden.

Planung der sicheren Kommunikation mit PROFINET: PROFINET-Geräte, die PROFINET Security nutzen, werden mit einem digitalen Zertifikat des Herstellers (IDevID) ausgeliefert und erhalten ein zweites digitales Zertifikat des Anlagenbetreibers (LDevID). Die Überprüfung des Herstellerzertifikats und die Bereitstellung des Anlagenbetreiberzertifikats müssen geplant werden, und für die Inbetriebnahme muss die entsprechende Infrastruktur vorhanden sein.

GSDX-Dateien für PROFINET-Geräte: PROFINET-Geräte, die Security unterstützen, werden mit digital signierten GSDX-Dateien geliefert. Diese Dateien werden vom Engineering-Tool importiert. Während des Planungsprozesses muss sichergestellt werden, dass digital signierte GSDX-Dateien verfügbar sind.

Planung von Security-Beziehungen: Das zu planende Automatisierungssystem besteht in der Regel aus Geräten, die PROFINET Security unterstützen, und kann auch Geräte enthalten, die keine Security unterstützen (Altgeräte). Die Anwendungsbeziehungen müssen ent-

sprechend geplant werden. Alle Geräte, die Security unterstützen, müssen für die Verwendung einer geschützten Anwendungsbeziehung konfiguriert werden.

Planung der Protokollierung von Security-Ereignissen: Die Erfassung und Protokollierung Security-relevanter Ereignisse liefert hilfreiche Informationen für die Erkennung von Anomalien und für forensische Untersuchungen. PROFINET-Geräte unterstützen die Protokollierung von Ereignissen. Es sollte geplant werden, diese Ereignisse zu sammeln und an ein Security-Informations- und Managementsystem (SIEM) zu übermitteln.

PROFIBUS & PROFINET International arbeitet zurzeit an einer „Planungsrichtlinie Security“, um die Anwender bzgl. der Security-Planung zu unterstützen.

4. PROFINET Security als Enabler für eine sichere Produktion

Die zunehmende Vernetzung industrieller Automatisierungssysteme erfordert eine systematische Umsetzung von Cyber-Security-Maßnahmen entlang des gesamten Lebenszyklus von Komponenten und Anlagen. PROFINET Security bietet hierfür ein gestuftes Security-Konzept, das auf den Anforderungen der IEC-62443-Reihe basiert und in drei Security-Klassen unterteilt ist.

Die regulatorischen Anforderungen aus der NIS2-Richtlinie [1], dem Cyber Resilience Act (CRA) [4] und der EU-Maschinenverordnung (MVO) [5] verlangen von Betreibern, Integratoren und Komponentenherstellern die Umsetzung technischer und organisatorischer Maßnahmen. Mit der PROFINET-Security-Klasse 2 und geeigneter Netzwerksegmentierung lassen sich heute schon erste sichere Lösungen realisieren. Hierbei wären konkret zu nennen:

- CRA
 - Integritätsschutz der Kommunikation
 - Teilweise Erfüllung der Anforderungen der IEC-62442-4-2, soweit durch das PROFINET-Protokoll zu erfüllen. Es wird davon ausgegangen, dass wesentliche Anforderungen aus dieser Norm Teil der harmonisierten EU-Normen werden.
 - Security by Default.
 - Schutz vor unberechtigtem Zugriff.
 - Vertraulichkeit und Integrität der Kommunikation
 - Minimierung des Datenaufkommens.
 - Begrenzung der Angriffsfläche.
 - Aufzeichnung und Überwachung sicherheitsrelevanter Ereignisse.
- NIS 2
 - Unterstützung der Betreiber in Bezug auf den Aspekt Sicherheit der Lieferkette.
- MVO
 - Schutz der Kommunikation gegen vorsätzliche oder unabsichtliche Korruption.
 - Schutz gegen Angriffe böswilliger Dritter

Jedoch werden zukünftige Anforderungen, insbesondere im Hinblick auf flexible IoT-Strukturen, nur durch Implementierungen der PROFINET-Security-Klassen 2 und 3 erfüllbar

sein. Darüber hinaus liefert die Einhaltung der in IEC-62443-4-1 definierten sicheren Entwicklungsprozesse seitens der Hersteller einen Beitrag, um die in der NIS2-Richtlinie geforderte Security entlang der Lieferkette aus Betreibersicht seitens des Herstellers zu unterstützen.

PROFINET Security ist ein zentraler Baustein für die Absicherung moderner Produktionssysteme. Die sichere Erfassung und Verarbeitung von Daten ist die Voraussetzung für die Einhaltung der regulatorischen Vorgaben sowie auch für die technische Umsetzung von Digitalisierungsstrategien. Dazu zählen etwa die Optimierung von Fertigungsprozessen, die Integration von IT- und OT-Systemen sowie der Abgleich zwischen physischer und digitaler Produktionsebene.

Zur Sicherstellung der Verfügbarkeit konformer Geräte im PROFINET-Security-Ökosystem ist eine frühzeitige Beteiligung der Komponentenhersteller an der Implementierung sowie an Interoperabilitätstests (Plugfests) erforderlich. Durch die enge Zusammenarbeit aller beteiligten Akteure, der Hersteller, der Gremien von PROFIBUS & PROFINET International (PI) aber auch der Betreiber, wird die technische Grundlage für eine sichere, gesetzeskonforme und zukunftsfähige industrielle Automation geschaffen.

IEC 62443 Security industrieller Automatisierungs- und Steuerungssysteme als Basis zur PROFINET-Security-Implementierung

Die PROFINET-Spezifikation MU 2.4 MU6 [12] der PROFIBUS & PROFINET International (PI) (wurde im Sommer 2025 veröffentlicht) definiert die Anforderungen an die Security von PROFINET-Geräten, insbesondere für die Security-Klassen 2 und 3.

Die IEC 62443-4-1 [8] konzentriert sich auf den sicheren Produktentwicklungsprozess beim Komponentenhersteller und stellt sicher, dass Komponenten, während ihres gesamten Lebenszyklus sicher sind.

Die IEC 62443-4-2 [9] legt die technischen Security-Anforderungen für die Implementierung der Security-Klassen 2 und 3 an die Integrität, Authentizität und Vertraulichkeit der Kommunikation für PROFINET-Security-Komponenten fest.

Die IEC 62443-3-3 [7] beschreibt die Anforderungen, die ein Systemintegrator bezgl. Zugriff, Vertraulichkeit, Integrität und Verfügbarkeit aus Lösungssicht implementieren muss. Der PROFINET Design Guideline Security definiert die technische Umsetzung oder zusätzlich erforderliche organisatorische Maßnahmen (erscheint im Herbst 2025).

IEC 62443-2-1 [20] definiert die Betreibersicht der Security und die Umsetzung der ISO 27001/2 ISMS-Security-Richtlinien und -verfahren für den Betrieb von Anlagen und Maschinen.

IEC 62443-2-3 [21] erklärt als technischer Report ein Regelwerk zur Freigabe und Installation von regelmäßigen Security-Updates und Maßnahmen zur Softwarepflege, um langfristig ein hohes Sicherheitsniveau zu gewährleisten.

IEC 62443-2-4 [19] definiert die Fähigkeiten, Anlagen sicher in Betrieb zu nehmen und zu warten.

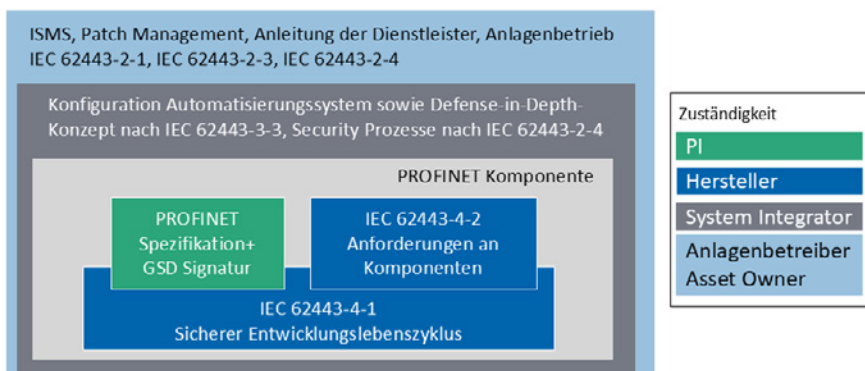


Abbildung 6: Verantwortlichkeiten und zugehörige Normteile im Security-Prozess

Diese Standards werden um die PROFINET-spezifischen Regelungen in der Planungs- und Inbetriebnahme-Richtlinie ergänzt. Um die Implementierung, Konformität und Interoperabilität nach der PROFINET-Security-Spezifikation entwickelter Geräten und Systeme zu erleichtern, hat die PROFIBUS & PROFINET International ein IEC-62443-Whitepaper [22] veröffentlicht, in dem eine Einordnung von PROFINET Security in den Kontext der IEC 62443 erfolgt. Abbildung 6 zeigt abschließend das Zusammenspiel der Akteure im Security-Prozess und die zugehörigen Teile der Norm IEC 62443.

5. Referenzen

- [1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). In: Amtsblatt der Europäischen Union
- [2] Bundesministerium des Innern und für Heimat: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz). Gesetzentwurf der Bundesregierung, 2024.
- [3] Europäisches Parlament und des Rat der Europäischen Union: Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates. CER Richtlinie, L 333/164. 2022
- [4] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (Text von Bedeutung für den EWR). CRA. In: Amtsblatt der Europäischen Union, S. 1–81
- [5] Europäisches Parlament und Rat der Europäischen Union: Verordnung (EU) 2023/1230 des Europäischen Parlaments und Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates. Maschinenverordnung, 2023
- [6] Seibel, M.: Abgrenzung der „allgemein anerkannten Regeln der Technik vom „Stand der Technik“ O. Neue Juristische Wochenzeitung (NJW) (2013) 41, S. 3000–3004
- [7] DIN EN IEC 62443-3-3:2020-01 VDE 0802-3-3:2020-01:2020-01. Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + COR1:2014); Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019. <https://www.dinmedia.de/de/norm/din-en-iec-62443-3-3/311519620>
- [8] 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 IEC 62443-4-1 :2018. <https://www.dinmedia.de/de/norm/din-en-iec-62443-4-1/292194568>
- [9] 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. <https://www.dinmedia.de/de/norm/din-en-iec-62443-4-2/312858287>
- [10] PROFIBUS Nutzerorganisation e.V.: Security Class 1 for PROFINET-Security Order No.: 7.312, 2023. <https://www.profibus.com/download/profinet-security-guideline>
- [11] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO. Version 2.4 MU5 #alt# Order-Nr. 2.722, 2024. <https://www.profibus.com/download/profinet-specification>
- [12] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery Technical Specification for PROFINET IO. Version 2.4 MU6 Order-Nr. 2.722, 2024. <https://www.profibus.com/download/profinet-specification>
- [13] RFC 5280:2008-05. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. <https://datatracker.ietf.org/doc/html/rfc5280>
- [14] IEEE 802.1AR-2018:2018. IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity. <https://ieeexplore.ieee.org/document/8423794>
- [15] DIN EN IEC 62443-3-2:2021-12 VDE 0802-3-2:2021-12:2021-12. IT-Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 62443-3-2:2020); Deutsche Fassung EN IEC 62443-3-2:2020 <https://www.dinmedia.de/de/norm/din-en-iec-62443-3-2/344299957>
- [16] VDI/VDE 2182 Blatt 1:2020-01. Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. <https://www.dinmedia.de/de/technische-regel/vdi-vde-2182-blatt-1/314114388>, abgerufen am: 05.05.2015
- [17] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, 2016. https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- [18] IEC/TS IEC/TS 62443-1-1:2009:2009-07. Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. <https://webstore.iec.ch/publication/7029>,
- [19] DIN EN IEC 62443-2-4:2024-11 VDE 0802-2-4:2024-11:2024-11. IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2023); Deutsche Fassung EN IEC 62443-2-4:2024. <https://www.dinmedia.de/de/norm/din-en-iec-62443-2-4/380674327>
- [20] DIN EN IEC 62443-2-1:2020-10 - Entwurf VDE 0802-2-1:2020-10:2020-10. IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber (IEC 657/756/CDV:2019); Deutsche und Englische Fassung prEN IEC 62443-2-1:2019. <https://www.dinmedia.de/de/norm-entwurf/din-en-iec-62443-2-1/327919389>
- [21] IEC TR 62443-2-3:2015:2015-06. Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment. Technical Report. <https://webstore.iec.ch/en/publication/22811>
- [22] Niemann, K.-H.: OT security for production plants with PROFINET. A classification of IEC 62443 for operators, integrators and manufacturers Nr. 7.342, Karlsruhe 2022. <https://www.profibus.com/download/white-paper-ot-security-classification-of-iec62443>

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. 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. Er leitet bei PROFIBUS & PROFINET International den Arbeitskreis CB/PG3 – Installation Guides und ist Mitglied im Arbeitskreis CB/PG10 – Security.

Prof. Dr.-Ing. Karl-Heinz Niemann

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

Timon Eßlinger, M.Sc. (geb. 1994), leitet das IT- und OT-Sicherheitsteam bei der Codewerk GmbH. Er ist spezialisiert auf die Absicherung industrieller Komponenten und kritischer Infrastrukturen im Kontext der IEC 62443, von den Anforderungen über die sichere Entwicklung bis hin zu Penetrationstests. Er ist Mitglied der Arbeitsgruppen PI CB/PG10 Security bei PROFIBUS & PROFINET International und im AK 351.0.6A IT-Sicherheit in Bahnsystemen bei der Deutschen Elektrotechnischen Kommission (DKE).

Timon Eßlinger, M.Sc.

Codewerk GmbH
Östliche Rheinbrückenstr.50 | BK 148
76187 Karlsruhe
E-Mail: timon.esslinger@codewerk.de
Webseite: <https://www.codewerk.de/>

Dipl.-Ing. Boris Waldeck (geb. 1963) ist Master Specialist Security PLCnext Technology und Product Solution Security Expert (PSSE) bei Phoenix Contact GmbH & Co. KG in Bad Pyrmont. Er ist verantwortlich für die IEC 62443-4-1 Secure Development life cycle (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. Er ist Mitglied der Arbeitsgruppe PI CB/PG10 Security bei PROFIBUS & PROFINET International und im AK Industrial Security des VDMA.

Dipl.-Ing. Boris Waldeck

PHOENIX CONTACT GmbH & Co. KG
Dringenauer Str. 30
31812 Bad Pyrmont
E-Mail: bwaldeck@phoenixcontact.com
Webseite: <https://www.phoenixcontact.com>,
<https://phoe.co/Cyber-Security>