Beitrag von Feldgeräten der Zukunft zur Anlagensicherheit (OT Security)

Dipl.-Ing. (FH), Dipl.-Ing (HTL) Markus Hoh, Endress+Hauser Flowtec AG, Reinach (Schweiz);
Prof. Dr.-Ing. Karl-Heinz Niemann, Hochschule Hannover, Hannover

Kurzfassung

Dieser Beitrag adressiert einleitend die aktuelle Bedrohungslage aus Sicht der Industrie mit einem Fokus auf das Feld und die Feldgeräte. Zentral wird dann die Frage behandelt, welchen Beitrag Feldgeräte im Kontext von hoch vernetzten Produktionsanlagen für die künftige IT-Sicherheit leisten können und müssen. Unter anderem werden auf Basis der bestehenden Standards wie IEC 62443-4-1 [1], IEC 62443-4-2 [2] oder der VDI 2182-1 [3] und VDI 2182-4 [4] ausgewählte Methoden und Maßnahmen am Beispiel eines Durchflussmessgerätes vorgestellt, die zur künftigen Absicherung von Feldgeräten notwendig sind.

Abstract

This paper addresses the current threat situation from the industry's point of view with a focus on the field and field devices. The central question will be: What contribution field devices can and must deliver to future IT security concepts in the context of highly networked production facilities? Based on existing standards such as IEC 62443-4-1 [1], IEC 62443-4-2 [2] or VDI 2182-1 [3] and VDI 2182-4 [4], examples of selected methods and measures or the future safeguarding of field devices will be presented, using the example of a flowmeter.

1. Die aktuelle Situation der IT-Sicherheit

Die Bedrohungslage für Produktionsanlagen in Bezug auf die IT-Sicherheit hat sich in letzter Zeit verschärft. Die IT-Sicherheit von Produktionsanlagen, häufig auch OT-Security genannt, stellt Hersteller, Integratoren und Betreiber vor große Herausforderungen. Cyberangriffe über Schadsoftware bedrohen nicht nur den Bürobereich. WannaCry, Havex, Black-Energy und andere führen auch zu Schäden an Produktionsanlagen, Energieversorgungsnetzen und anderen kritischen Infrastrukturen. So beziffert das Pharma-Unternehmen Merck in seinem Quartalsbericht [5] den Umsatzausfall durch Befall mit Schadsoftware auf 175 Mio. USD. Die verschärfte Bedrohungslage und das zunehmende Schadensausmaß erfordern einen weitergehenden Schutz der Produktionsanlagen. Zudem ändert sich momentan die Architektur von

Automatisierungsanlagen, sodass auch unter diesem Gesichtspunkt weitere Überlegungen zum Schutz von Produktionsanlagen anzustellen sind.

2. Zukünftige Industrie-4.0-Kommunikation

Im Kontext von Industrie 4.0 ist eine Veränderung der Strukturen von Automatisierungssystemen zu erkennen. In vielen Anlagen erfolgt, wie in Bild 1 dargestellt, eine so genannte horizontale und vertikale Integration [6]. Eine besondere Rolle spielen hierbei auch moderne Kommunikationstechnologien wie z. B. Industrial Ethernet und Wireless (WirelessHART, WLAN, LoRaWAN o.ä.).

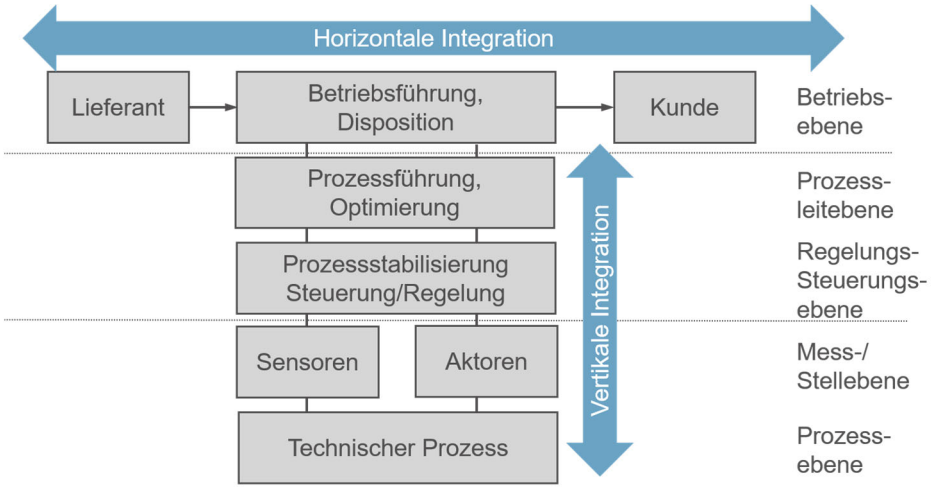

Bild 1: Horizontale und vertikale Integration in einer Produktionsanlage

Die horizontale Integration betrifft die Verbindung der Geschäftsprozesse über die Grenzen des Unternehmens hinweg. So werden Kunden und Lieferanten auch Bestandteil einer digital vernetzten Lieferkette. Bei der vertikalen Integration werden Daten aus dem Produktionsbereich über die Ebenengrenzen der Automatisierungspyramide hinweg kommuniziert. So könnte z. B. ein Messumformer über eine Verwaltungsschale [7] zusätzlich zum Messwert, Qualitätsdaten an die Betriebsebene liefern. Einen vergleichbaren Ansatz verfolgt die NAMUR Open Architecture (NOA) [8]. Diese vertikale Integration ist aber in Hinsicht auf die IT-Sicherheit problematisch, da die Daten nun die Grenzen zwischen dem Produktionsbereich (OT) und dem Office-Bereich (IT) überschreiten. Ein zunehmender Datenaustausch dieser – bisher meist gegeneinander abgeschotteten – Bereiche ist die Folge. Die Auswirkungen einer solchen Kommunikation mittels einer Verwaltungsschale auf die IT-Sicherheit sind zu berücksichtigen [9].

Bild 2 zeigt eine weitere Veränderung in der industriellen Kommunikation im Kontext von Industrie 4.0. In der linken Bildhälfte ist eine klassische, hierarchische Automatisierungsstruktur einer Teilanlage dargestellt, wie sie heute noch oft in der Prozessindustrie anzutreffen ist. Die Controller verfügen jeweils über einen eigenen Feldbus, über den die Remote IOs und andere Geräte angebunden sind. Im rechten Teil von Bild 2 ist eine Struktur mit einer starken Vernetzung im Sinne von Industrie 4.0 auf Basis von Industrial Ethernet dargestellt. Alle Komponenten sind nun über ein einheitliches Netzwerk miteinander verbunden. Dies hat Vorteile in Bezug auf die vertikale Integration. Alle Komponenten sind über das Netzwerk direkt erreichbar.

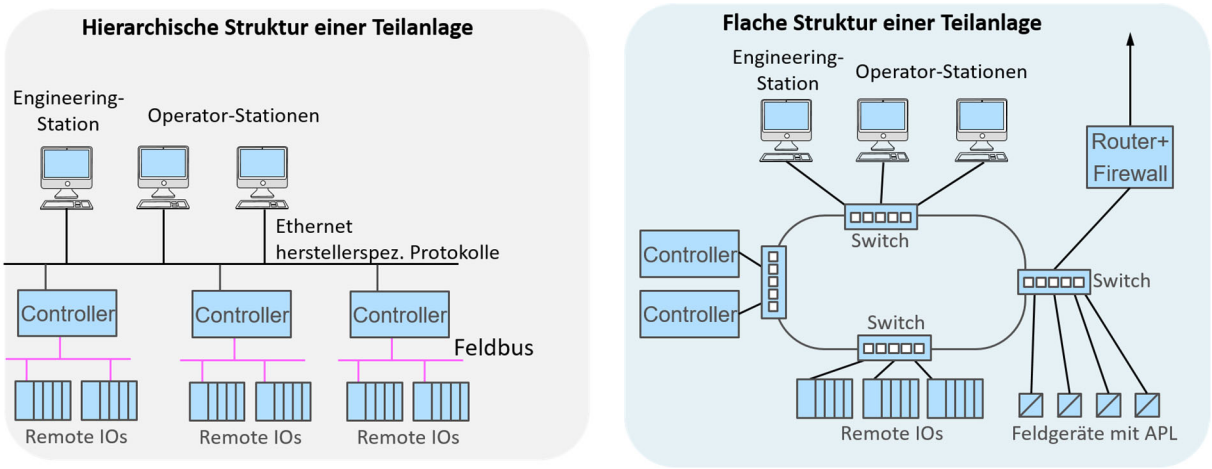

Bild 2: Änderung der Kommunikation im Kontext von Industrie 4.0

Ein Nachteil dieser Kommunikationsstruktur ist, dass alle Komponenten nun auch für potenzielle Angreifer direkt erreichbar sind. Das gilt auch für Feldgeräte, wie sie in Bild 2 unten rechts dargestellt sind. Waren bisher in der Regel speicherprogrammierbare Steuerungen lohnende Angriffsziele, werden nun die Feldgeräte als „ressourcen-schwächste“ Teilnehmer am Netz für potenzielle Angreifer interessant.

Mit dem so genannten Advanced Physical Layer (APL) für Ethernet in der Prozessindustrie gemäß IEEE 802.3-10SPE [10, 11] wird künftig die Möglichkeit bestehen, Feldgeräte direkt an das Ethernet-basierte Automatisierungsnetzwerk anzubinden. Der Advanced Physical Layer wird dabei zukünftig vor allem die folgenden Funktionen bieten:

- Zweileiteranschluss
- Standardisierter Steckverbinder
- Speisung der Geräte über Zweileiteranschluss

- Betrieb von Feldgeräten und Switches im Ex-Bereich.
- Austausch von Geräten im laufenden Betrieb unter Ex-Bedingungen

Diese digital kommunizierenden Geräte können dann auch über Middleware-Protokolle bei Bedarf Statusinformationen an übergeordnete Ebenen (z. B. auch Cloud) liefern.

3. Die Änderung der Integrationsmöglichkeiten von Feldgeräten

Klassische Feldgeräte mit 4…20-mA-Interface und HART-Protokoll kommunizieren im Wesentlichen über das HART-Interface und ggf. zusätzlich noch über Display und Taster sowie eine proprietäre Service-Schnittstelle mit der Umgebung.

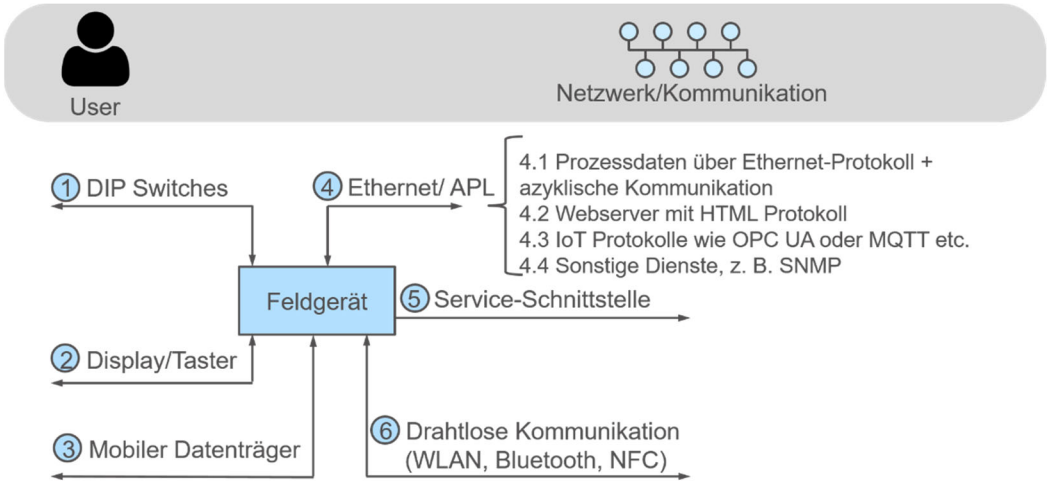

Bild 3: Zukünftige Schnittstellen eines Feldgerätes

Mit der Einführung intelligenter Feldgeräte und dem im Kapitel 2 beschriebenen Advanced Physical Layer wird sich die Anzahl der Kommunikationsmöglichkeiten und -protokolle deutlich erhöhen. Bild 3 zeigt ein Feldgerät einschließlich der zukünftig zu erwartenden zusätzlichen Schnittstellen. DIP-Switches ❶, Display/Taster ❷ und Service-Schnittstelle ❺ sind aus den klassischen Feldgeräten bekannt. Die 4…20-mA-Schnittstelle mit HART-Protokoll wird durch die Ethernet/APL-Schnittstelle ❹ abgelöst. Über diese physische Schnittstelle wird künftig parallel eine Reihe von Diensten/Protokollen abgewickelt werden. Das können z. B. sein:

- Bereitstellung der Echtzeit-Prozessdaten über ein Industrial Ethernet Protokoll, z. B. PROFINET. Es sind hierbei die zyklische Echtzeitkommunikation und die azyklische Kommunikation zu berücksichtigen.
- Webserver für Diagnose und Parametrierung.

- Industrie-4.0-Protokolle (Verwaltungsschale), wie z. B. OPC-UA, MQTT, DDS oder ähnliches. Bereitstellung von Service- und Diagnoseinformationen.
- Sonstige Dienste, z. B. SNMP für Netzwerk-Management.

Neben der drahtgebundenen Ethernet-Schnittstelle ❹ wird möglicherweise zusätzlich eine drahtlose Schnittstelle ❻ mit WLAN, Bluetooth, NFC oder auch WirelessHART zur Verfügung stehen, um Teile der oben genannten Dienste auch drahtlos anbieten zu können. Es ist in Bild 3 zu erkennen, dass die genannten zusätzlichen Interfaces und Protokolle als potenzielle Einfallstore für Cyber-Angriffe auf das Feldgerät zu sehen sind. Daher befasst sich das folgende Kapitel mit möglichen Bedrohungen, die auf ein Feldgerät einwirken können.

4. IT-Security-Bedrohungsanalyse eines Feldgerätes und abgeleitete Maßnahmen

Aus Bild 3 ist abzuleiten, dass künftige Feldgeräte mehr Schnittstellen aufweisen, als bisher genutzte Feldgeräte. Diese zusätzlichen Schnittstellen müssen auf ihre IT-Security-Eigenschaften überprüft und ggf. zusätzlich geschützt werden.

Feldgeräte sind in der Regel Bestandteil einer Automatisierungsanlage. Diese Anlage ist im Idealfall im Rahmen eines Defense-in-Depth-Konzeptes abgesichert [12]. Bei diesem Konzept werden Komponenten des Automatisierungssystems durch weiter außenliegende Schutzmaßnahmen geschützt. Die Norm DIN IEC 62443-3-3 [13] beschreibt die Anforderungen und Maßnahmen zur Realisierung eines Defense-in-Depth-Konzeptes einer Automatisierungsanlage. Es ist daher davon auszugehen, dass Feldgeräte in einer geschützten Umgebung betrieben werden. Dennoch bestehen auch in dieser geschützten Umgebung Risiken, die durch entsprechende Maßnahmen im Feldgerät selber beherrscht werden müssen. Ursache hierfür können z. B. Angriffe sein, die weiter außen liegenden Schutzmaßnahmen kompromittiert haben oder aber Innentäter, die direkten Zugriff zum Automatisierungsnetzwerk haben. Laut einer Studie der BITKOM [14] gehen 62% aller Angriffe von aktuellen oder ehemaligen Mitarbeitern aus. Tabelle 1 zeigt anhand der in Kapitel 3 beschriebenen Schnittstellen einige ausgewählte Risiken, denen ein Feldgerät, trotz des Defense-in-Depth-Konzeptes, ausgesetzt ist und welche Schutzmaßnahmen möglich sind.

Tabelle 1: Exemplarische Auswahl möglicher Bedrohungen für ein Feldgerät

Nr.	Interface	Mögliche Bedrohung	Mögliche Schutzmaßnahmen
1	DIP-Switches	Unautorisierter Zugang zum Gerät. Unautorisierte Konfigurationsänderung.	Zugang zum Gerät beschränken
2	Display/Taster	Zugang zum Gerät über Standardpasswort oder Standard-Administrator-Passwort	Aufforderung zur Änderung des Standard-Passwortes. Keine festen Administrator-Passworte.
3	Mobile Datenträger	Einspielen von nicht autorisierten Konfigurationsänderungen über mobile Datenträger in Verbindung mit Neustart Gerät	Vorsehen einer Autorisierung zum Einspielen von Konfigurationsänderungen
4.1	Ethernet Prozessdaten	„Man in the middle“-Angriff auf Kommunikation zwischen Feldgerät und Controller	Schutz des Echtzeitprotokolls mittels kryptografischer Maßnahmen
4.2	Ethernet Web-Server	Nicht autorisierter Zugriff auf Webserver mit nicht geändertem Standard-Passwort	Autorisierung der Nutzer bei Zugriff über Webserver sicherstellen
4.3	Ethernet IoT-Protokolle	„Man in the middle“-Angriff auf IoT-Kommunikation (z. B. OPC-UA, MQTT) in Verbindung mit ungesicherten Varianten dieser Protokolle	Nutzung der kryptografisch abgesicherten Varianten dieser Middleware-Protokolle
4.4	Ethernet, SNMP-Protokoll	Zurücksetzen des Gerätes über SNMP-Zugriff	Nutzung kryptografisch abgesicherter SNMP-Protokollvarianten in Verbindung mit Nutzerautorisierung
5	Service-Schnittstelle	Nicht autorisierte Änderung von Geräteparametern über Service-Schnittstelle	Autorisierung von Nutzern der Service-Schnittstelle vorsehen
6.	Drahtlose Kommunikation	Sinngemäß gelten die gleichen Bedrohungen wie bei Schnittstelle 4	Sinngemäß gelten die gleichen Maßnahmen wie bei Schnittstelle 4

Die Aufstellung in Tabelle 1 gibt nur einen kleinen Ausschnitt möglicher Bedrohungen wieder. In einer exemplarischen Untersuchung der Autoren an einem Pilotgerät konnten 55 verschiedene Bedrohungsszenarien für ein Feldgerät identifiziert werden. Weitere Informationen zu dieser Untersuchung finden sich in [15]. Die beispielhaft durchgeführte Bedrohungsanalyse liefert drei Kategorien von Maßnahmen:

- **Kategorie 1:** Maßnahmen, die durch den Betreiber oder Integrator umzusetzen sind. Es kann sich hierbei z. B. um eine Arbeitsanweisung handeln, die das Ändern von Standardpasswörten auf geräteindividuelle oder zumindest bereichsindividuelle Passworte vorschreibt. Der Hersteller muss die Möglichkeit, das Passwort zu ändern allerdings in die Gerätesoftware integriert haben.
- **Kategorie 2:** Maßnahmen, die durch den Gerätehersteller in das Gerät zu integrieren sind. So z. B. die Unterstützung sicherer Ausführungen der o. g. IoT-Protokolle, wie z. B. OPC-UA [16].
- **Kategorie 3:** Maßnahmen, die zunächst eine Standardisierung im Bereich der verwendeten Kommunikationsprotokolle erfordern. Hier ist z. B. das Absichern der Kommunikation etwa durch kryptografische Maßnahmen zu nennen [17], die zur Zeit noch nicht verfügbar ist.

Es ist zu erkennen, dass bei allen drei Kategorien die Mitwirkung des Feldgeräteherstellers erforderlich ist. Sei es, dass Hinweise auf Aktionen bei der Inbetriebnahme gegeben werden (Kategorie 1), dass gesicherte Varianten von Kommunikationsprotokollen vom Gerät unterstützt (Kategorie 2) oder dass sichere Methoden der SW-Entwicklung eingesetzt werden. Möglicherweise sind auch Maßnahmen noch nicht umsetzbar, weil die Standardisierung noch nicht ausreichend fortgeschritten ist (Kategorie 3). Es stellt sich nun die Frage, was der Hersteller eines Feldgerätes in Bezug auf die IT-Security leisten muss und an welchen Richtlinien er sich orientieren kann. Diese Frage wird im folgenden Abschnitt behandelt.

5. Der IT-Security-Prozess für den Hersteller eines Feldgerätes

Bild 4 zeigt die Akteure im IT-Sicherheitsprozess und die entsprechenden Normteile der IEC 62443 gemäß der Norm IEC 62443-2-2 [18].

Es ist aus Bild 4 zu erkennen, dass der Hersteller eines Feldgerätes (Produktlieferant) im Wesentlichen von den Normteilen 3-3 und 4-2 Anforderungen an das System bzw. die Komponenten erhält, während der Teil 4-1 vor allem Anforderungen an den Entwicklungsprozess betrachtet. Diese drei Normteile sollen im Folgenden näher betrachtet werden.

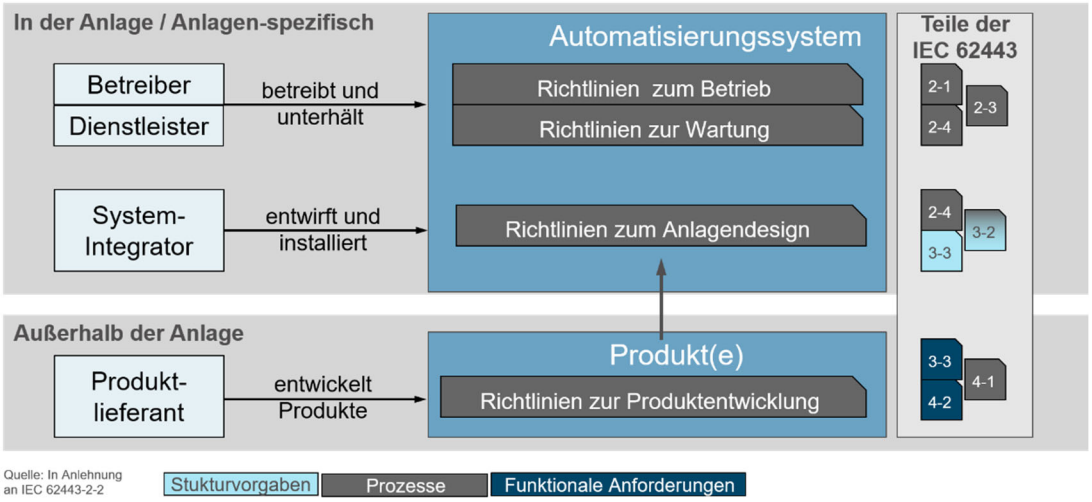

Bild 4: Akteure im Sicherheitsprozess und zugeordnete Teile der IEC 62443 (In Anlehnung an [18])

Die Norm **DIN EN IEC62443-4-1 [1]** befasst sich mit den IT-Security-Prozessen, die zur Entwicklung einer Komponente für ein Automatisierungssystem relevant sind. Die wesentlichen Abschnitte dieser Norm sind:

- Verwaltung der IT-Sicherheit
- Spezifikation der IT-Sicherheitsanforderungen
- IT-Sicherheit durch Entwurf
- Gesicherte Implementierung
- Verifikations- und Validierungsprüfung der IT-Sicherheit
- Behandlung von Mängeln der IT-Sicherheit
- IT-Sicherheitsrichtlinien

Es ist an den Abschnitten zu erkennen, dass die Norm im Wesentlichen die Verankerung des Themas IT-Security im Entwicklungsprozess sowie die gesicherte Berücksichtigung der Anforderungen bei der Produktentwicklung und Produktverifikation betrachtet. Darüber hinaus ist aus das Thema der Kommunikation zwischen Kunde und Lieferant (Meldungen von Security-Fehlern) und vice versa (Product Alerts, Release Notes) Bestandteil der Norm. Darüber hinaus definiert die Norm auch, welche Dokumentation der Hersteller für die Komponente bereitzustellen hat.

Die Norm **DIN EN 62443-4-2** [2] erweitert die Systemanforderungen der DIN IEC 62443-3-3 [13] um komponentenspezifische Anforderungen CR (engl. Component Requirement) und weitergehende Anforderungen RE (engl. Requirement Enhancement). Die Norm betrachtet vier unterschiedliche Klassen: Softwareanwendungen, Host-Geräte, eingebettete Geräte und Netzwerkkomponenten. Viele der Anforderungen gelten für alle vier Komponentenarten und werden zu einer Komponentenanforderung (CR) zusammengefasst. Für jeden Security Level (SL) werden, angepasst an den Schärfegrad, entsprechend angepasste Anforderungen definiert. Je höher der Security Level (möglich sind SL 1 bis SL 4), umso höher sind auch die Anforderungen an die Komponente. Beispiele für komponentenspezifische Anforderungen (CR) können z. B. sein (Auszug):

- CR 1.1 - Nutzerauthentifizierung
- CR 1.6 - Verwaltung drahtloser Zugriffsverfahren
- CR 1.11 - Erfolglose Anmeldeversuche
- CR 2.2 - Nutzungskontrolle von Funkverbindungen
- CR 2.5 - Sitzungssperrung
- CR 2.7 - Kontrolle gleichzeitiger Sitzungen
- CR 3.1 - Kommunikationsintegrität

Die hier genannten Beispiele stellen lediglich eine exemplarische Auswahl dar. In Summe definiert die Norm ca. 100 CR und RE, auf die an dieser Stelle jedoch nicht im Detail eingegangen werden kann.

Die Norm **DIN IEC 62443-3-3** [13] definiert auf Systemebene Anforderungen an ein Automatisierungssystem. Da viele der CR und RE der DIN EN 62443-4-2 [2] aus diesen Anforderungen abgeleitet werden, ist eine Mitbetrachtung des Teils 3-3 sinnvoll und notwendig. Aus dieser Norm leiten sich eventuell auch übergeordnete Schutzmaßnahmen eines Systems im Rahmen eines Defense-in-Depth-Konzeptes ab, die bei der Absicherung einer Komponente berücksichtigt werden können.

Neben den drei genannten Normen der IEC 62443 Normreihe soll noch ein Blick auf die Norm VDI 2182-4 [4] geworfen werden. Diese Norm betrachtet den Entwicklungsprozess für automatisierungstechnische Komponenten gemäß den Design-Prinzipien:

- Secure by Default
- Secure by Design
- Secure by Implementation

- Secure by Deployment

Nach diesen Aspekten sortiert, gibt die Norm Hinweise, wie einzelne Aspekte der IT-Security im Produktentwicklungsprozess berücksichtigt und adäquat realisiert werden können.

6. Fazit

Dieser Beitrag fokussiert auf die Anforderungen an einen Komponentenhersteller und die erforderlichen Schritte, die dieser umzusetzen hat. Dabei sind sowohl die Organisation der Entwicklung (Prozesse) als auch die Anforderungen an das Produkt (funktionale Anforderungen) zu berücksichtigen. Für eine erfolgreiche Umsetzung der IT-Sicherheit in der Produktion ist in jedem Fall das Zusammenspiel von Herstellern, Integratoren und Betreibern gemäß Bild 4 erforderlich. Dabei sind sowohl technische Anforderungen an die Produkte [2] als auch Anforderungen an die Organisation [1] zur beachten. Im Rahmen einer Zertifizierung wird man in der Regel zunächst die Entwicklungsprozesse betrachten, bevor man sich den Produkteigenschaften zuwenden wird.

Wie Bild 5 zeigt, definiert die IEC 62443-1-5 [19] den IT-Security Reifegrad (Protection Level PL) einer Produktionsanalage in Abhängigkeit von den technischen Voraussetzungen (Security Level SL) und dem Reifegrad der Organisation (Maturity Level ML).

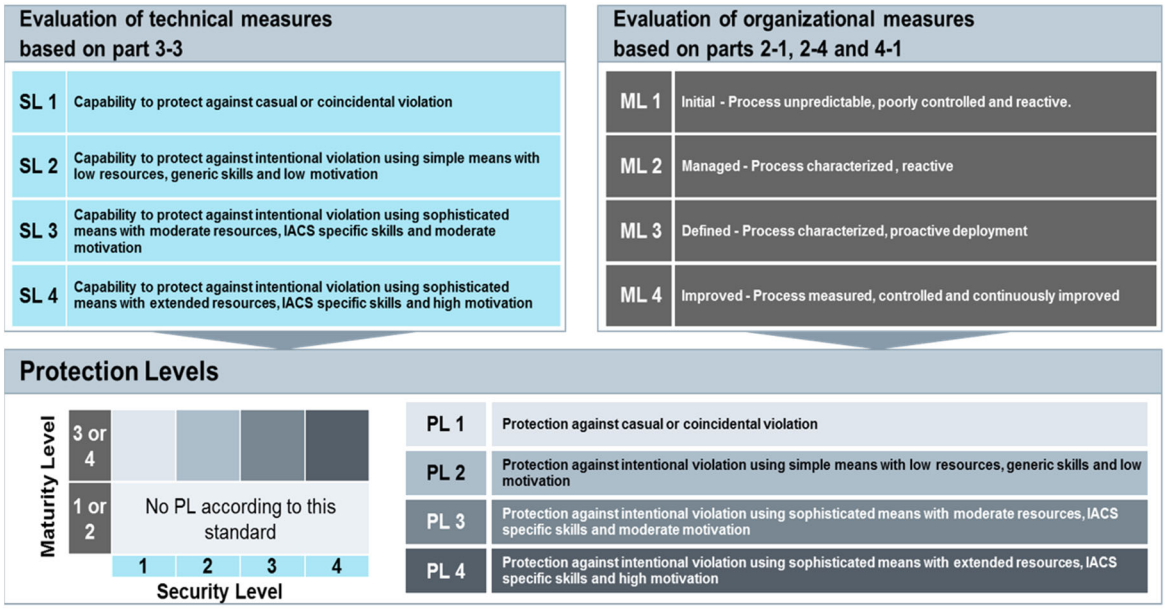

Bild 5: Zusammenhang zwischen technischen und organisatorischen Maßnahmen [19]

Nur durch die gemeinsame Berücksichtigung technischer **und** organisatorischer Maßnahmen ist die IT-Sicherheit in der Produktionsanlage im Kontext der Anforderungen von Industrie 4.0 zu gewährleisten. Das gilt sowohl für den in diesem Beitrag betrachteten Entwicklungsprozess als auch für die Prozesse bei Betreibern und Integratoren [20].

Literaturangaben

[1] 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

[2] DIN EN 62443-4-2 (VDE 0802-4-2):2017-10. 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

[3] VDI/VDE 2182 Blatt 1:2011-01. Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell

[4] VDI/VDE 2182 Blatt 4:2018-11. Informationssicherheit in der industriellen Automatisierung Empfehlungen zur Umsetzung von Security-Eigenschaften für Komponenten, Systeme und Anlagen

[5] Merck: Merck Announces Third-Quarter 2017 Financial Results, Kenilworth N. J. 2017. https://www.mrknewsroom.com/news-release/financial-news/merck-announces-third-quarter-2017-financial-results

[6] Wollschläger et. al.: Kommunikation im Industrie-4.0-Umfeld. Welchen Herausforderungen hat sich die industrielle Kommunikation im Kontext von Digitalisierung und Industrie 4.0 zu stellen? https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2018/April/Kommunikation_im_Industrie-4.0-Umfeld/Kommunikation_im_Industrie-4.0-Umfeld_Download-Neu.pdf

[7] Gebhardt, P. u. Spiegel, C. Chachaj, A.: Integrierte Verwaltungsschale nach RAMI 4.0 für Vier- und Zweileiter-Feldgeräte. In: Automation 2017. Technology networks processes : 18. Leitkongress der Mess- und Automatisierungstechnik : Kongresshaus Baden-Baden, 27. und 28. Juni 2017. VDI-Berichte, Bd. 2293. Düsseldorf: VDI Verlag GmbH 2017

[8] Diedrich, C., Schörder, T. u. Riedl, M.: Kommunikationskonzept von NAMUR Open Architecture - NOA. 8. Jahreskolloquium „Kommunikation in der Automation“ (KommA 2017). 2017, ohne Seitenzählung

[9] ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie: Security in der Verwaltungsschale, Frankfurt/Main 2017. https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Whitepaper_Security_der_Verwaltungsschale_SG_Sicherheit_im_ZVEI/ZVEI_WP_Security_der_Verwaltungsschale__I.40__Download_12.04.17.pdf

[10] Hähniche, J., Brandt, D. D. u. Xu, D.: IEEE 802.3cg (10SPE) – 10 Mb/s Single Pair Ethernet meeting Industrial Automation objectives. ODVA 2017 Industry Conference & 18th Annual Meeting. 2017

[11] Hähniche, J., Lüder, S. u. Kessler, M.: Prozessautomatisierung im Wandel – wie neue Übertragungstechnologien dazu beitragen. 8. Jahreskolloquium „Kommunikation in der Automation“ (KommA 2017). 2017, ohne Seitenzählung

[12] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[13] DIN IEC 62443-3-3 (VDE 0802-3-3):2015-06. 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)

[14] Berg, A. u. Maaßen, H.-G.: Wirtschaftsschutz in der digitalen Welt. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf

[15] Niemann, K.-H. u. Hoh, M.: Anforderungen an die IT--Sicherheit von Feldgeräten. Schutzlösungen für hoch vernetzte Produktionsanlagen. In: atp-edition 59 (2017) 12, S. 42–53

[16] Armstrong, R. u. Hunkar, P.: The OPC UA Security Model For Administrators. Whitepaper, 2010. https://opcfoundation.org/wp-content/uploads/2014/05/OPC-UA_Security_Model_for_Administrators_V1.00.pdf

[17] PROFIBUS Nutzerorganisation e.V.: Security Extensions for PROFINET - PI White Paper for PROFINET, Karlsruhe 2018. https://www.profibus.com/specific_link_will_be_added_after_review

[18] IEC 62443-2-2 TC65/717/NP:2018-09. Security for industrial automation and control systems - Part 2-2: IACS protection levels

[19] IEC / ISA-62443-1-5:2017-07. Security for industrial automation and control systems - Part 1–5: Industrial automation and control system protection levels

[20] Niemann, K.-H.: Organisation der IT-Sicherheit in der Produktion. In zehn Schritten zur sicheren Produktionsanlage. In: atp Magazin (2018) 11-12, S. 80–89

Beitrag ist erschienen in:

20. Leitkongress der Mess- und Automatisierungstechnik
AUTOMATION 2019
Autonomous Systems and 5G in Connected Industries
Baden-Baden, 02. und 03. Juli 2019
VDI-Berichte, Herausgeber: VDI Wissensforum GmbH
VDI-Verlag 2019
ISSN 0083-5560
ISBN 978-3-18-092351-2