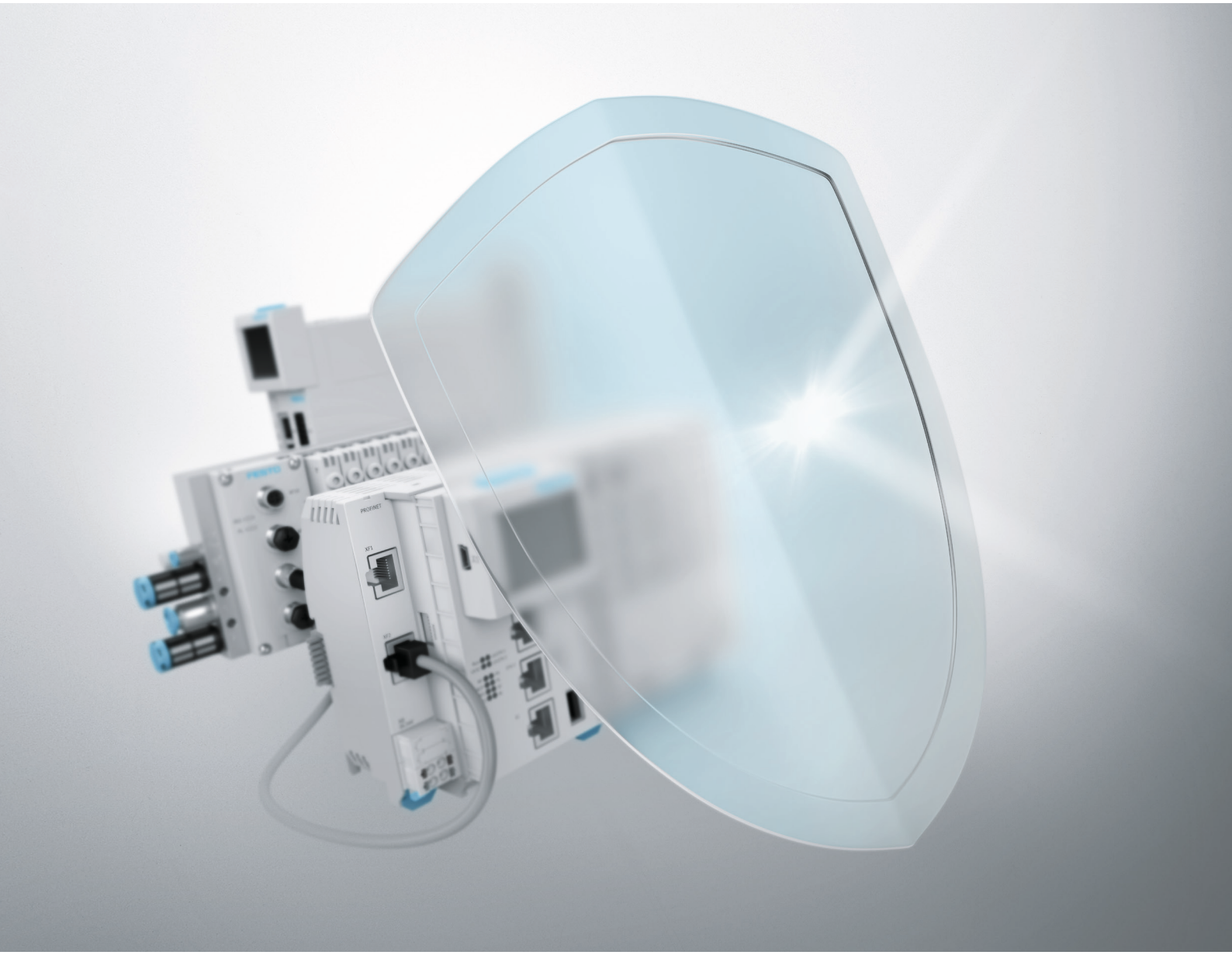
Security Whitepaper
für Festo Steuerungen

FESTO



Inhaltsverzeichnis

1.	**Einleitung**	3
1.1	Zielsetzung und Anwendungsbereich des Dokuments	3
1.2	Definitionen / Glossar	3
1.2.1	Angreifer Kategorien	3
1.2.2	Norm IEC 62443	3
2.	**Security-Strategie**	4
2.1	Verantwortlichkeiten für Security nach IEC 62443	5
2.2	Defense in Depth	6
3.	**Einsatzzweck und Einsatzumgebungen**	7
3.1	Typische Einsatzumgebung	7
3.2	Funktionalitäten	8
4.	**Advisories / Vulnerabilities**	9
4.1	Festo PSIRT	9
4.2	Security Advisories	9
5.	**Risiken**	10
6.	**Maßnahmen**	11
6.1	Physischer Zugriffsschutz	11
6.2	Digitaler Zugriffsschutz	11
6.3	Upgrade der Firmware / Einspielen von Patches	11
6.4	Sicherheit von aufgebrachten (SPS) Programmen	12
6.5	Sicherheit von aufgebrachten Konfigurationen	12
6.6	Passwörter	12
6.7	Netzwerkarchitektur / Netzwerksegmentierung	13
6.7.1	Ethernet-Ports und Kommunikationsbeziehungen	15
6.7.2	Weitere digitale physische Schnittstellen	15
6.8	Backup / Restore	15
6.9	Außerbetriebnahme	16
6.10	Servicefall	16
6.10.1	Remote Support	16
6.10.2	Support bei Festo – Reklamationena	16

© Copyright 2023, Festo SE & Co. KG

1. Einleitung

1.1 Zielsetzung und Anwendungsbereich des Dokuments

Dieses Dokument soll Anwendern von Festo Steuerungsprodukten einen Einstieg und eine Hilfestellung geben, wie Festo Steuerungen unter dem Aspekt der Cyber Security möglichst sicher eingesetzt werden können. Die Produkte wurden nach dem Stand der Technik zum Zeitpunkt der Markteinführung entwickelt.

Um die Produkte möglichst sicher einsetzen zu können, bedarf es weiterer Maßnahmen, um das Risiko eines Cyberangriffs auf diese Systeme zu minimieren.

Diese werden in diesem Dokument beschrieben.

Das Dokument bezieht sich auf folgende Festo Produktfamilien:

- CPX-E-CEC-*
- CECC-*
- CPX-CEC-*
- CDPX-*

1.2 Definitionen / Glossar

1.2.1 Angreifer Kategorien

62443 SL Level	Bedrohung	Typischer Angreifer
SL 1	Schutz vor unbeabsichtigtem oder zufälligem Missbrauch.	Unbeabsichtigte Verwendung
SL 2	Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.	Script Kiddy
SL 3	Schutz vor vorsätzlichem Missbrauch mit anspruchs-vollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation.	APT Groups
SL 4	Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation.	State Actor

1.2.2 Norm IEC 62443

Die Norm IEC 62443 ist eine internationale Norm für die Cyber Security von Industriellen Kontrollsystems (IACS).

© Copyright 2023, Festo SE & Co. KG

2. Security-Strategie

Eine Security-Strategie behandelt folgende Kernziele:

Kernziele	
Confidentiality	• Stealing of intellectual property or secrets (Password, certificates)
Integrity	• Manipulation of production processes • Manipulation for unlicenced use or missuse
Availability	• Denial of Service (DOS) Attacks to disturb production

Weiterführende Informationen und Empfehlungen stellt z.B. das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seiner Homepage bereit
BSI - Industrielle Steuerungs- und Automatisierungssysteme (ICS) (bund.de)

Festo Produkte und deren Security-Strategie können nur Teil einer ganzheitlichen Security-Strategie sein, um eine Maschine oder Produktionsanlage vor Bedrohungen zu schützen.

Dem Kunden obliegt die Aufgabe die Security-Strategie für die Maschine oder Produktionsanlage festzulegen, kontinuierlich weiterzuentwickeln und an die Bedrohungslage anzupassen.

Die Evaluierung, ob Festo Produkte in das Sicherheitskonzept der Maschine oder Produktionsanlage integriert werden können, muss ebenfalls durch den Kunden vorgenommen werden.

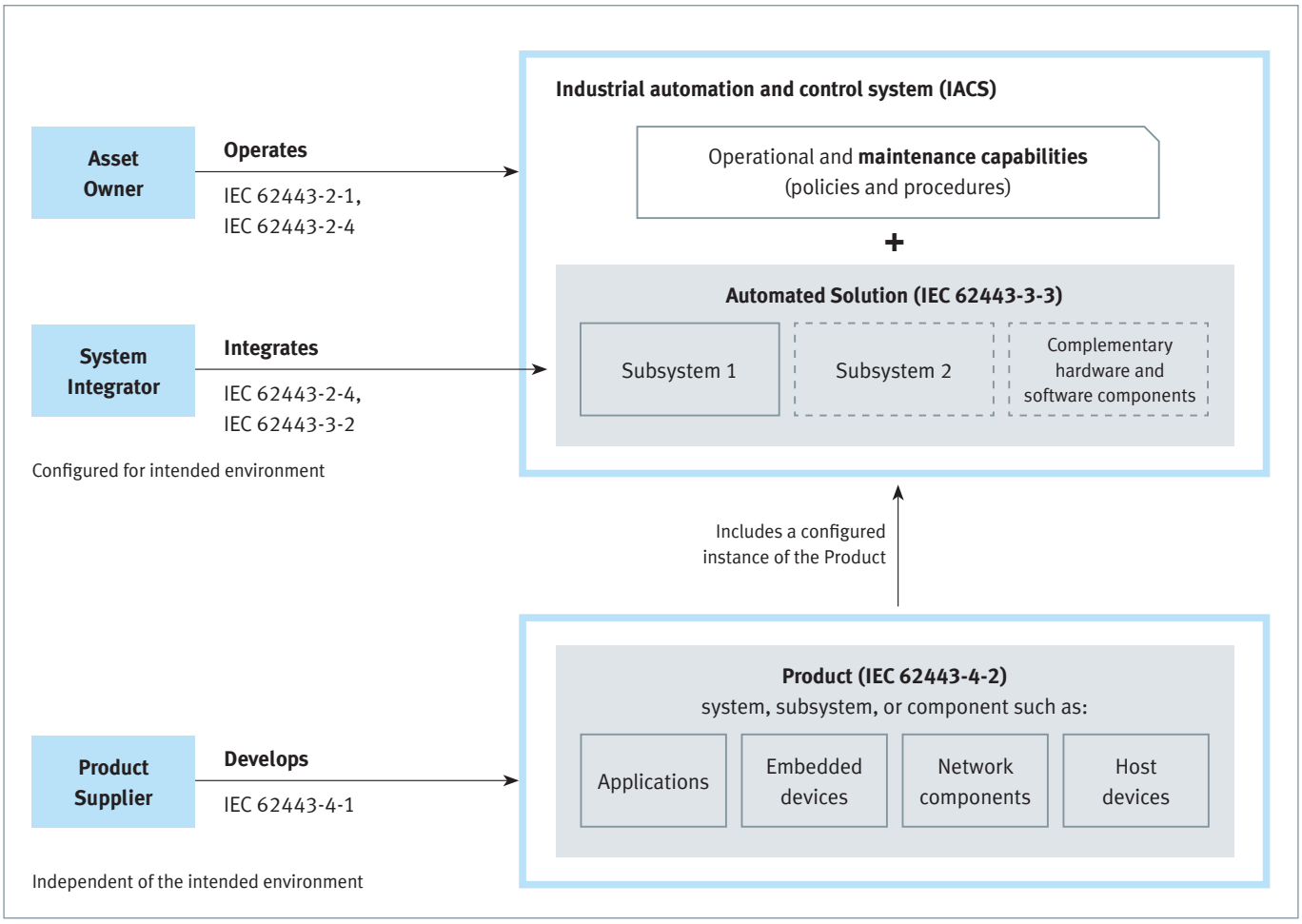
Festo als der Komponentenanbieter entwickelt die Produkte nach dem jeweiligen Stand der Technik. Bestehende Produkte können aus Gründen der Rückwärtskompatibilität Funktionen enthalten (siehe auch **Abschnitt 3.2**), die nicht mehr vollumfänglich den heutigen Sicherheitsanforderungen genügen.

Programme oder Konfigurationsdaten, die vom Kunden erstellt (z.B. SPS-Programme, Scripte etc.) und auf Festo Produkte aufgebracht werden, können zu unsicheren Systemen führen. Es obliegt dem Kunden geeignete Maßnahmen zu ergreifen, sodass diese Programme oder Konfigurationen die Systemsicherheit nicht beinträchtigen.

Wichtig bei der Security-Strategie ist auch zu betrachten, dass diese nicht nur die Hardware- und Software-Maßnahmen betrifft, sondern auch die Menschen in der Organisation miteinschließen soll.

© Copyright 2023, Festo SE & Co. KG

2.1 Verantwortlichkeiten für Security nach IEC 62443



Die wesentlichen Sicherheitsanforderungen an Komponenten werden durch den jeweiligen Einsatz in einer Anlage bzw. einem System durch den Anlagenbetreiber und / oder Systemintegrator definiert. Daraus leiten sich dann die Anforderungen an die jeweiligen Komponenten ab.

Wichtig ist auch die Betrachtung, dass alle Akteure (d.h. Asset Owner, System Integrator und Product Supplier) in ihrem jeweiligen IT-Verantwortungsbereich (der Maßgeblich auf die Schnittstelle IT/OT wirkt) auch entsprechende Prozesse und Maßnahmen ergreifen.

Nähere Details zur Bestimmung der Bedrohungen und Risiken sind in **Kapitel 5** Risken beschrieben.

Weitere Informationen vom VDMA für den Anlagenbetreiber und Systemintegrator finden Sie in folgendem Leitfaden unter:
http://www.festo.com/leitfaden-iec62443

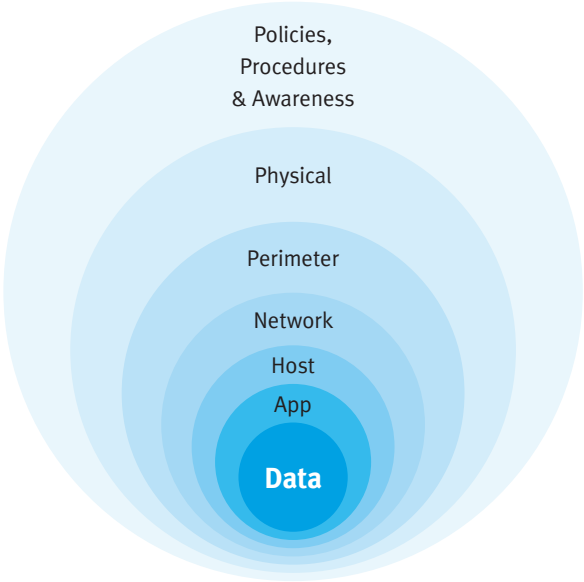
Eine mögliche Bezugsquelle für die Norm ist die DKE unter:
http://www.festo.com/dke-iec62443

Weitere Informationen zur Motivation und zu Techniken von Angreifern finden sie unter:
http://www.festo.com/know-the-opponent

© Copyright 2023, Festo SE & Co. KG

2.2 Defense in Depth

Defense in Depth ist ein wesentlicher Teil der Security-Strategie, die Maßnahmen auf verschiedenen Ebenen umfasst, um die Assets einer Organisation zu schützen.



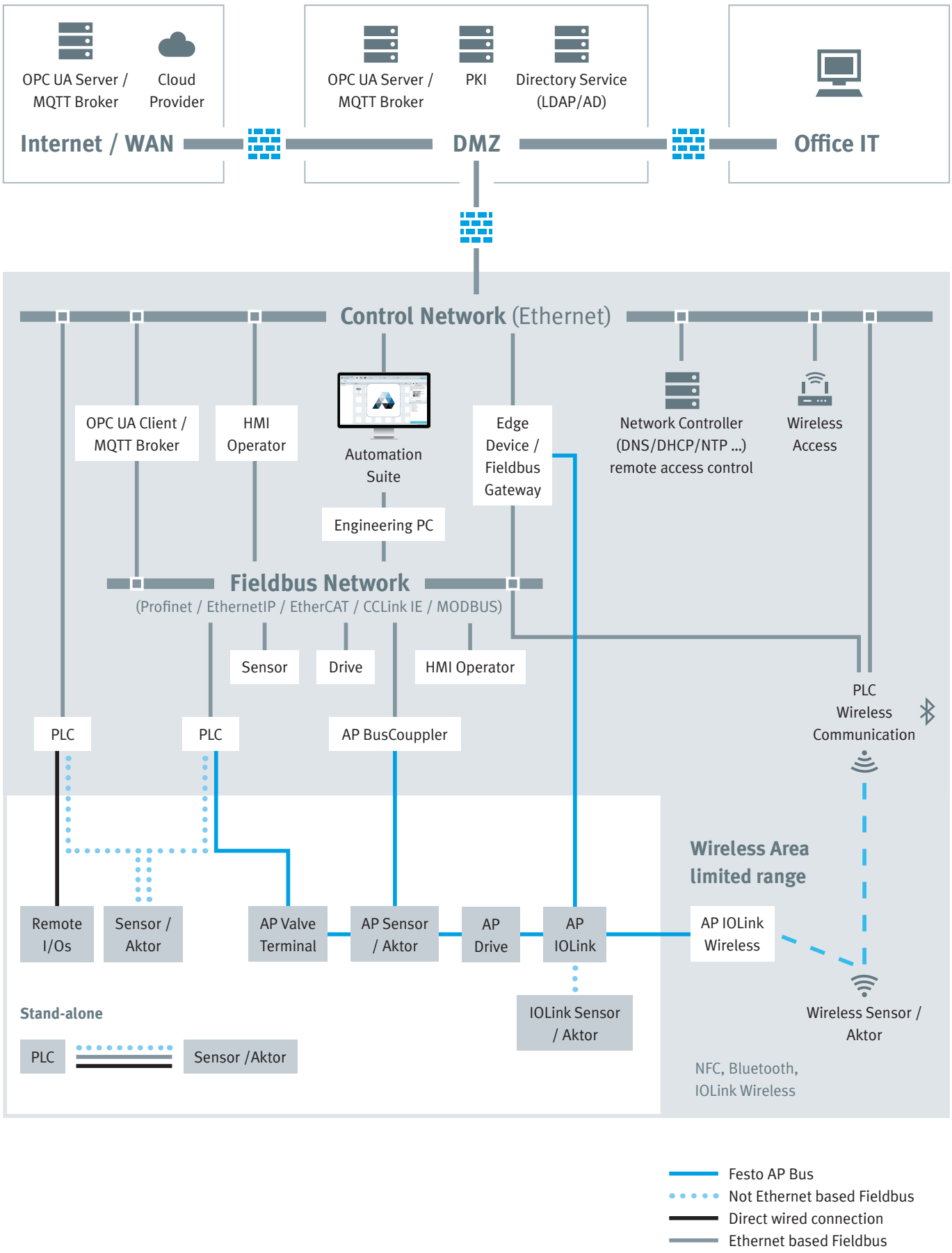
Beispielsweise könnte man der Meinung sein, dass eine Abtrennung des Netzwerks durch eine Firewall ausreichenden Schutz vor unberechtigtem Zugriff gewährleistet. Die Defense-in-Depth Strategie sieht nun vor, dass man noch weitere zusätzliche Maßnahmen ergreift, um dem Angreifer den unberechtigten Zugriff zu erschweren. Dies könnte z. B. durch die Nutzung des User Managements für die Codesys-Applikation gemacht werden (d.h. es gibt nun eine zusätzliche Hürde, falls die Abtrennung des Netzwerks durch einen Angreifer überwunden wurde).

Beispiele für mögliche Maßnahmen im Rahmen der Defense-in-Depth-Strategie finden Sie in **Kapitel 6** Maßnahmen.

© Copyright 2023, Festo SE & Co. KG

3. Einsatzzweck und Einsatzumgebungen

3.1 Typische Einsatzumgebung



© Copyright 2023, Festo SE & Co. KG

Festo Steuerungsprodukte sind für die Verwendung in der Industriellen Automation vorgesehen und wurden zum jeweiligen Stand der Technik entwickelt.

Festo Steuerungen sind für den Einsatz in abgeschotteten (Industrie) Netzwerken konzipiert und entwickelt. Bei unzureichender Abschottung des Netzwerks können unberechtigte Zugriffe auf das Produkt Schäden oder Fehlfunktionen verursachen.

Festo geht bei der Betrachtung von sicherheitsrelevanten Themen von den Rahmenbedingungen aus, die solche Umgebungen darstellen.

3.2 Funktionalitäten

Die verwendeten Funktionalitäten wie

- Kommunikationsprotokolle,
- Backupfähigkeiten,
- Updatefähigkeit
- Passwortschutz

wurden nach dem Stand der Technik zum Zeitpunkt der Markteinführung entwickelt und ausgewählt. Der Fokus liegt hier auf rascher Einsatzbereitschaft, Wartbarkeit, Offenheit der Kommunikation, breiter Einsatzfähigkeit (beispielsweise rascher Möglichkeit ein Backup einzuspielen auf ein Ersatzgerät) und Benutzerkomfort.

© Copyright 2023, Festo SE & Co. KG

4. Advisories / Vulnerabilities

Festo stellt Informationen über Schwachstellen bereit und bietet Möglichkeiten zur Kontaktaufnahme durch die Security Community.

4.1 Festo PSIRT

Das Festo Product Security Incident Response Team (PSIRT) ist das zentrale Team der Festo SE & Co. KG, das die Prüfung und Offenlegung von Sicherheitsschwachstellen managt. Alle Meldungen über mögliche Schwachstellen oder andere Sicherheitsvorfälle im Zusammenhang mit Festo Produkten können an das Festo PSIRT weitergeleitet werden. Das Festo PSIRT-Team koordiniert und pflegt die Kommunikation mit allen Beteiligten, intern und extern, um auf identifizierte Sicherheitsprobleme angemessen reagieren zu können.

Mehr Informationen unter: **PSIRT**

4.2 Security Advisories

Das Festo PSIRT untersucht alle Meldungen zu Sicherheitsproblemen und veröffentlicht Security Advisories zu validierten Sicherheitsschwachstellen, welche Produkte von Festo direkt betreffen und entweder ein Softwareupdate, -upgrade oder eine andere kundenseitige Aktion erfordern. Als Teil der kontinuierlichen Bemühungen, Betreiber bei der Adressierung von Sicherheitsrisiken und bei dem geschützten Betrieb von Systemen zu unterstützen, veröffentlicht das Festo PSIRT Informationen, welche für Betreiber zur Bewertung der Auswirkungen einer Sicherheitsschwachstelle notwendig sind.

Schwachstellen von Produkten bei Festo und neue oder aktualisierte Security Advisories veröffentlichen wir auf unserer Partnerplattform CERT@VDE unter: **http://www.festo.com/vde-festo-advisories**

Ebenso veröffentlicht Festo die Security Advisories in Form einer Application Note im Support Portal unter: **http://www.festo.com/festo-advisories**

© Copyright 2023, Festo SE & Co. KG

5. Risiken

Einer der Hauptaspekte der Risikobetrachtung ist, dass unterschiedliche Applikationen unterschiedliche Schutzbedürfnisse haben. Eine der wesentlichen Aufgaben ist es nun, im Zug der Risikoanalyse eben diese Schutzbedürfnisse zu bestimmen.

Die drei oben genannten Schutzziele (Confidentiality, Integrity, Availability) sind applikationsspezifisch und daher individuell im Rahmen einer Bedrohungs- und Risikoanalyse produkt- bzw. kundenseitig zu bestimmen.

Praktische Tipps zur Vorgangsweise können sein:

- Heranziehen eines Katalogs zur systematischen Bestimmung von Bedrohungen und Risiken (z. B. **Mitre ATT&CK**)
- Bewertung dieser Bedrohungen und Risiken für den jeweiligen Einsatzbereich durch Erstellung einer Risikomatrix (Bedrohung, Wahrscheinlichkeit, Konsequenz, Impact). Methoden dazu sind die STRIDE, Attack Tree, PASTA oder ähnliche **Ansätze**.

Am Ende der Bedrohungs- und Risikoanalyse wurden die größten Risiken identifiziert und infolge ist es nötig, Maßnahmen zu deren Verhinderung oder Abschwächung zu treffen (siehe **Kapitel 6** Maßnahmen).

Insgesamt werden dann damit alle Risiken so weit gesenkt, dass nur mehr ein akzeptables Restrisiko übrig bleibt, das dann bewusst in Kauf genommen wird.

Gegebenenfalls ist es im Bedarfsfall empfehlenswert, auch externe Dienstleistungen dazu in Anspruch zu nehmen.

© Copyright 2023, Festo SE & Co. KG

6. Maßnahmen

Dieses Kapitel beschreibt mögliche Maßnahmen, die ergriffen werden können, um Cyber-Security-Risiken möglichst gering zu halten.

6.1 Physischer Zugriffsschutz

Um physischen Zugriffsschutz zu gewährleisten, sollte das Produkt wenn immer möglich in geschützten Bereichen montiert werden, beispielsweise in einem abgeschlossenen Schaltschrank. Es sollte auch darauf geachtet werden, dass physischer Zugriff auch auf Schnittstellen (z. B. Netzwerkschnittstellen, USB) und Bedienelemente (z. B. DIP-Schalter) durch Unberechtigte verhindert wird.

6.2 Digitaler Zugriffsschutz

Es muss sichergestellt werden, dass nur ein eingeschränkter Nutzerkreis mit berechtigtem Interesse zum digitalen Zugriff auf das Gerät berechtigt ist.

Es ist empfehlenswert einen Prozess für die Verwaltung der Zugriffsrechte zu etablieren. Damit kann sichergestellt werden, dass Veränderungen in der Nutzerstruktur entsprechend abgebildet werden.

Der digitale Zugriffsschutz gliedert sich meist in mehrere Ebenen wie Netzwerkschutz, Passwortschutz etc.

6.3 Upgrade der Firmware / Einspielen von Patches

Festo liefert ein Gerät mit der zum Fertigungszeitpunkt aktuellen Softwareversion. Nur die aktuelle Softwareversion bietet den bestmöglichen Schutz, um Sicherheitsrisiken zu minimieren. Festo veröffentlich in regelmäßigen Abständen neue Softwareupdates und stellt diese den Kunden zum Download zur Verfügung.

Der Einsatz einer nicht aktuellen Firmwareversion (z.B. durch Downgrade) kann zu Sicherheitsrisiken führen und wird von Festo nicht empfohlen! Entsteht ein Sicherheitsproblem durch die Verwendung einer nicht aktuellen Software, kann Festo hierfür keine Garantie geben bzw. Haftung übernehmen.

© Copyright 2023, Festo SE & Co. KG

6.4 Sicherheit von aufgebrachten (SPS) Programmen

Festo Steuerungsprodukte sind frei programmierbare Geräte, um dem Kunden größtmögliche Flexibilität zu bieten. Damit einher geht, dass der Kunde die Verantwortung für die eigen erstellten Programme und deren Funktionen trägt.

Empfehlungen:

- Achtung bei der Verwendung von Code aus unbekannten Quellen
- Erstellte Programme sollten passend zu ihrer Funktion getestet werden. Dies kann beispielsweise durch einen Pentest oder durch Tests mit Experten erfolgen.
- Bei Kommunikation mit Cloud-Diensten sollte auf die Verwendung sicherer Protokolle geachtet werden. Beispielsweise sollte HTTPS statt HTTP verwendet werden.
- Bei der Erstellung von CODESYS-Programmen sollten die Codesys Best Practices bzw. **Whitepaper** beachtet werden.

6.5 Sicherheit von aufgebrachten Konfigurationen

Die Konfiguration eines Produktes ist schützenswert. Der Schutzbedarf der Konfiguration ist abhängig von Einsatzzweck und Einsatzumgebung. Manipulation der Konfiguration eines Produkts kann Auswirkungen auf den korrekten Betrieb haben.
Der Zugriff auf Konfigurationen sollte daher eingeschränkt sein und nur von autorisierten Nutzern durchgeführt werden können.

Konfigurationen können in Backups enthalten sein, dies sollte in einer Sicherheitsstrategie berücksichtigt werden. (siehe **Abschnitt 6.8**)

Welche Konfigurationsmöglichkeiten ein Produkt bietet, ist im jeweiligen Produkthandbuch beschrieben.

6.6 Passwörter

Passwörter und Passwortschutzmechanismen dienen dazu ein Gerät oder eine Funktionalität vor unberechtigtem Zugriff zu schützen.

Es sollte geprüft werden, ob alle möglichen Passwortschutzfunktionalitäten aktiviert sind und aktivieren Sie diese gegebenenfalls. Beispielsweise bietet Codesys die Möglichkeit das Projekt mit einem Passwortschutz zu versehen.

Default Passwörter sollten, wenn möglich bei Inbetriebnahme geändert werden. Sichere Passwörter sollten den aktuellen State-of-the-Art Anforderungen entsprechen, beispielsweise kann man sich am BSI orientieren.

Es muss beachtet werden, dass bei Verlust des Passworts das Gerät auf Werkseinstellungen zurückgesetzt werden muss.

> Weitere Informationen zur Absicherung von Passwörtern finden Sie beim BSI unter:
> **http://www.festo.com/sichere-passwoerter**

© Copyright 2023, Festo SE & Co. KG

6.7 Netzwerkarchitektur / Netzwerksegmentierung

Es ist empfehlenswert das Netzwerk nach logischen Einheiten in Zonen mit eigenen Subnetzen zu gliedern. Zwischen diesen Zonen sollte jegliche Kommunikation unterbunden sein. Es sollten nur die tatsächlich notwendigen Kommunikationsbeziehungen (Conduits) erlaubt werden (z.B. durch das Öffnen von Ports auf der Firewall)

Es sollten sinnvolle Limits und Regeln für den Datendurchsatz der Firewalls konfiguriert werden, um bestimmte Arten von Denial-of-Service-Angriffen abzumildern.

Es ist empfehlenswert das Netzwerk zu überwachen (z.B. mit Hilfe eines Intrusion Detection System (IDS)). Die Überwachungsregeln sollten regelmäßig überprüft und angepasst werden.

Externer Zugriff auf Systeme sollte überwacht und eingeschränkt werden. Dies kann z.B. durch die Verwedung von Jumphosts realisiert werden.

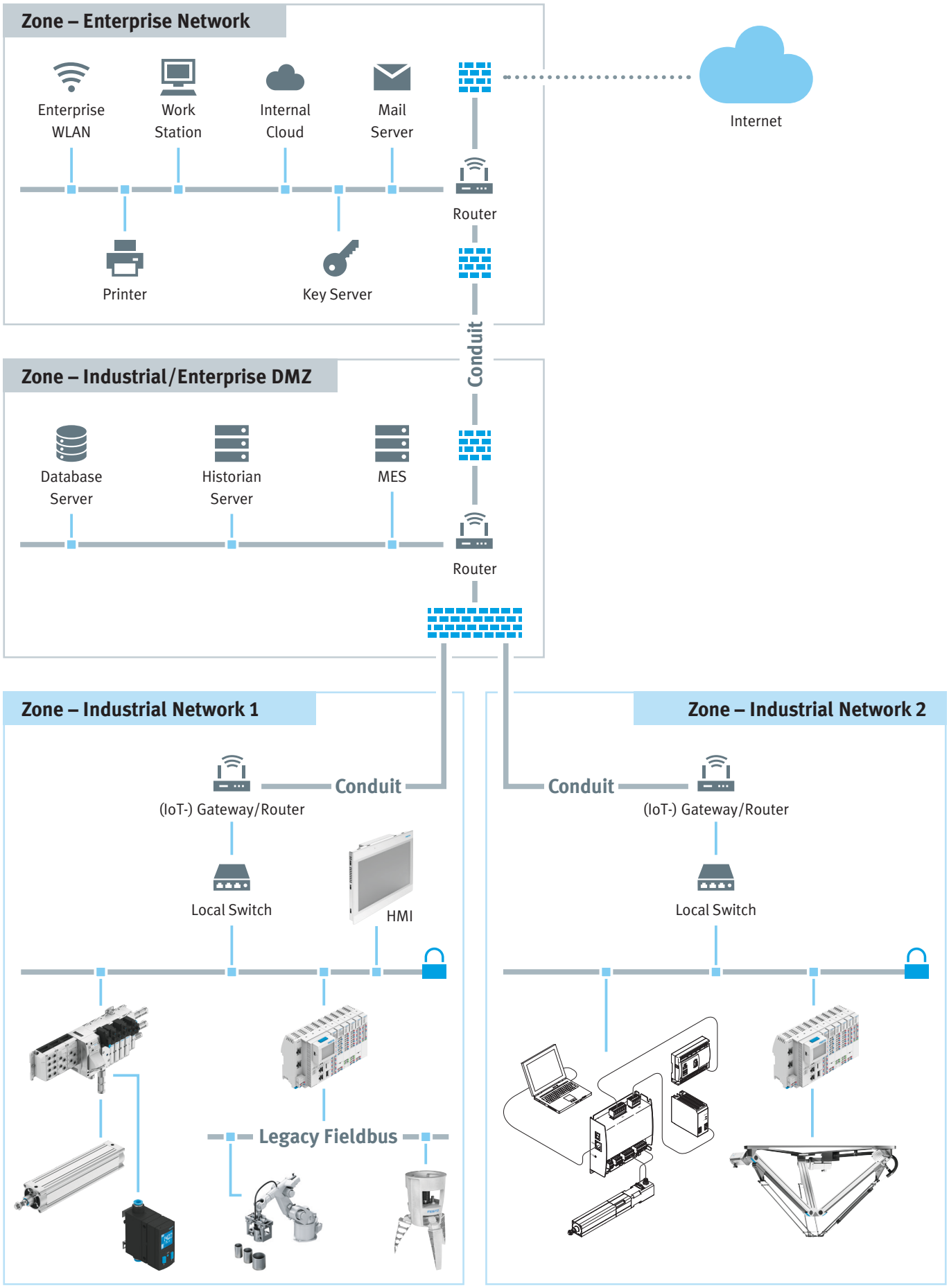
Beispielsweise wäre es denkbar, jeweils Subnetze für Maschinenzelle, Fabrikhalle und den gesamten Produktionsbereich zu definieren.

Eine Orientierung hierzu gibt auch die Normenreihe IEC62443.

> Weitere Informationen und Empfehlungen können Sie aus dem ZVEI Whitepaper entnehmen unter: **http://www.festo.com/white-paper-teil-2-integritaet-in-produktion**

© Copyright 2023, Festo SE & Co. KG

Zonenkonzept



© Copyright 2023, Festo SE & Co. KG

6.7.1 Ethernet-Ports und Kommunikationsbeziehungen

Festo Produkte verwenden unterschiedlichste Protokolle, um ihre Funktionalitäten bereitzustellen.

Bei Festo häufig verwendete Protokolle:

Protokoll	Port	Beschreibung
Festo FGMC	10002 (Multicast-Gruppe: 239.255.002.003)	Multicast-Suchprotokoll von Festo (Festo Generic Multicast)
Festo WAY	Layer 3 Protokoll	Festo Broadcast (Where Are You)
Festo CI	991 (UDP)	Command Interpreter
Festo ENGP/ENGT	7507 (tcp) / 7508 (tcp)	Festo Engineering Protocol
HTTP	80	Hyper text transfer Protokoll zur Darstellung von Webvisualisierungen
Codesys Engineering Interface	1740 – 17431 (UDP) 11740 (TCP) 1217 (TCP)	Kommunikation zwischen Codesys Runtime und Engineering

Des weiteren verwenden Festo Produkte Standard-Protokolle, die nötig sind, um TCP/IP-Kommunikation zur ermöglichen (z.B. DHCP, ICMP etc). Es kommen weiterhin je nach Produkt spezifische Protokolle zum Einsatz, um spezialisierte Funktionalitäten zu ermöglichen (z.B. Profinet, EtherCAT etc.).
Welche Protokolle in einem Produkt verwendet werden, entnehmen Sie bitte der jeweiligen Produktdokumentation.

6.7.2 Weitere digitale physische Schnittstellen

Die weiteren physischen Schnittstellen wie z. B. SD-Karte, CAN, IOL, USB sind über physischen Zugangsschutz abzusichern.

6.8 Backup / Restore

Das Anlegen eines Backups ist essentiell wichtig, um eine schnelle Wiederherstellung im Katastrophenfall zu ermöglichen.
Ein regelmäßiges Testen der Prozeduren für den Wiederherstellungsfall wird empfohlen.

Beim Backup ist sicherzustellen, dass der Zugriff auf das Backup nur durch autorisierte und geschulte Personen erfolgt. Das Backup sollte sicher abgelegt werden (z.B. auf Air-Gapped-Systemen oder Off-Site).

Bei Restore muss überprüft werden, dass das richtige am richtigen Ort wiederhergestellt wird.

Das Backup eines Produkts umfasst üblicherweise die Konfiguration (z.B Netzwerkkonfigurtati on,Passwörter, Parmeter, etc.) und Anwendungsdaten (z.B. PLC Projekt, Persistente Daten).

Festo bietet verschiede Möglichkeiten Backups zu erstellen und wiederherzustellen. Hierzu stehen Software Tools wie die Festo Automation Suite oder das Festo Field Device Tool zur Verfügung.

© Copyright 2023, Festo SE & Co. KG

6.9 Außerbetriebnahme

Zum Schutz der auf dem Produkt befindlichen Daten ist bei Außerbetriebnahme das zurücksetzen auf Werkseinstellungen und das Löschen von Information, wenn möglich, durchzuführen. Eine Beschreibung hierzu ist dem jeweiligen Produkt Handbuch zu entnehmen.

Sollte der Schutzbedarf für die im Produkt gespeicherten Daten hoch sein, sollte man sich zusätzlich an einen Entsorger wenden, der die elektronischen Informationen sicher entwertet.

6.10 Servicefall

Im Servicefall sollte ebenfalls auf die Sicherheit der Daten geachtet werden.

6.10.1 Remote Support

Empfehlung für einen sicheren remote Zugriff für den Support sind:

- Den Remote Zugriff sicher gestalten (z.B. VPN, Jump-Host) und die Vertraulichkeit der Kommunikation im Netzwerken sicherstellen.
- Setzen eines Accounts für den Support, Vermeidung von offenlegen eigener Security Credentials wie Passwörter.
- Entfernen des Support Accounts nach Beendigung der Servicetätigkeit.

6.10.2 Support bei Festo – Reklamationen

Vor Rücksendung des Produkts in einem Support- oder Reklamationsfall sollten folgende Punkte beachtet werden:

- Setzen eines Accounts für den Festo Support, Vermeidung von offenlegen eigener Security Credentials wie Passwörter.
- Entfernen vorab von sicherheitsrelevanten Daten
- Entfernen des Support Accounts bei Wiederinbetriebnahme.

Veröffentlicht durch:
Festo AG & Co. KG

process@festo.com
→ **www.festo.com/process**

Ihr persönlicher Ansprechpartner:
Dr. Wolfgang Rieger
Wolfgang.Rieger@festo.com

→ **Feedback zum Datei**

© Copyright 2023, Festo SE & Co. KG