KRIKO Engineering GmbH

Automation, Drives & Industrial IT

# HÖCHSTE ZEIT FÜR OT-SICHERHEIT

## NETZWERKSEGMENTIERUNG FÜR EINE SICHERE BETRIEBSTECHNIK

Fast täglich zieren solche Schlagzeilen über Cyberattacken die Medien. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet die Bedrohung der Cybersicherheit im Jahr 2023 als „so hoch wie nie zuvor". Auch produzierende Unternehmen bleiben nicht von Cyberkriminalität verschont. Um das zu verhindern, hilft ein Blick auf die OT-Sicherheit.

***01.09.2024:*** *Cyberangriff auf Deutsche Flugsicherung*
***14.04.2023:*** *Cyberangriff auf Rheinmetall*
***06.02.2023:*** *Globale Hackerwelle trifft Deutschland*

### IEC 62443 und Defense in Depth

Die Normenreihe IEC 62443 wird aktuell als Industriestandard zur Cybersecurity gesehen. Zum Schutz einer Anlage werden über das mehrschichtige Grundkonzept „Defense in Depth" die drei zentralen Zonen zum Schutz einer Industrieanlage definiert:

- Anlagensicherheit
- Netzwerksicherheit
- Systemintegrität

Hier fokussieren wir uns auf die Netzwerksicherheit, die sich stark auf die zugrundeliegende Segmentierung definiert.

### RISIKEN IM BESTAND DURCH GEWACHSENE STRUKTUREN

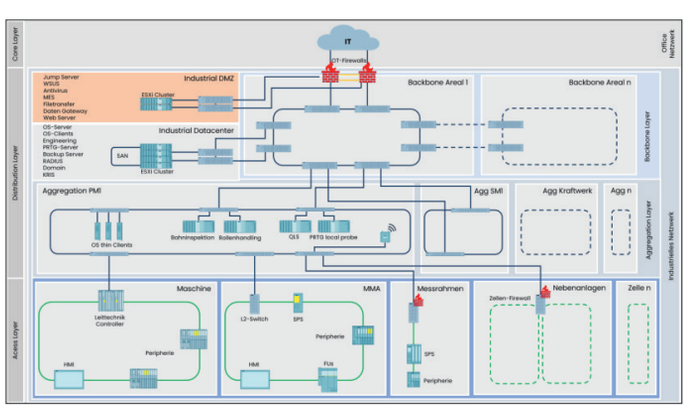
Der erste Schritt zur Sicherung der Anlagentechnik liegt in der Überprüfung der Netzarchitektur. Hierbei wird zuerst über eine Bestandsaufnahme die logische und physikalische Netzaufteilung betrachtet. Oft finden sich hier historisch gewachsene Strukturen. Die folgenden Sicherheitsrisiken können zu Tage treten:

- Keine klare Trennung zwischen IT und OT
- Keine Kanalisierung des IT-Zugangs, mehrere Zugänge von IT zu OT
- Keine Segmentierung und Zellenbildung von Teilanlagen
- Direkte Verbindungen von Geräten der IT zur OT und umgekehrt
- Direkte Verbindung von Netzwerken unterschiedlicher Sicherheitsklassen durch Multihoming

Diese konzeptionellen Sicherheitsrisiken erleichtern Viren und Schadsoftware aus der IT den Zugang zur Produktion. Noch kritischer ist jedoch, dass sich Viren im Schadfall über viele Netzwerke, Anlagenteile, Maschinen und sogar Standorte ausbreiten können. Die Segmentierung schränkt nicht nötigen funktionsübergreifenden Netzwerk-Traffic ein. Notwendiger funktionsübergreifender Datenaustausch wird streng reglementiert, überwacht und steht nur denjenigen Endgeräten zur Verfügung, die die Information tatsächlich benötigen. Dies gewährleistet eine bestmögliche Sicherheit und Performance des Netzwerks und damit der gesamten Anlagentechnik.

### NETZWERKSEGMENTIERUNG IN DER PRAXIS

Die hier dargestellte Netzwerkkonfiguration zeigt die bespielhafte Netzwerksegmentierung einer modernen Papierfabrik. Bei der Konzeptionierung der Netzarchitektur wurden die Systemanforderungen der IEC 62443-3-3 berücksichtigt. Das OT-Netzwerk wird horizontal und vertikal segmentiert. Die vertikale Segmentierung ist in Access, Distribution und Core Layer unterteilt, wobei der Distribution Layer ab mittelgroßen Netzarchitekturen wiederum in die Bereiche Aggregation und Backbone unterteilt werden kann.




Diese Art der Segmentierung führt zu deutlich weniger Verbindungen einzelner Geräte untereinander und reduziert die Komplexität des Netzwerks. Der Core Layer stellt den bevorzugten Anschluss des OT-Netzwerks auf der Seite des Unternehmensnetzwerks dar und gehört üblicherweise nicht zum Verantwortungsbereich der Betriebstechnik.

### ACCESS LAYER

Auf Zugriffs- oder Zellebene werden die Bestandteile einzelner Maschinen- und Anlagenteile vernetzt. Hier sind die klassischen Feldbus-Netzwerke je nach Redundanzanforderungen in Ring-/ Linien und Baumstrukturen vorzufinden. Die IEC 62443-3-3 fordert eine logische und physikalische Trennung von kritischen zu nicht kritischen automatisierungstechnischen Netzen. Diese Isolierung wird über die Bildung von Zellen organisiert. Der ein- und ausgehende Datenstrom der Zelle, kann zusätzlich durch eine Zellen-Firewall kontrolliert werden.

### AGGREGATION LAYER

Der Hauptzweck der Aggregationsebene liegt im Herstellen einer Verbindung der Zugriffsebene zum Backbone, was hohe Datenraten der eingesetzten Switche bedingt. Zusätzlich können hier diejenigen physikalischen Server, Clients, WLAN Access Points etc. angeschlossen sein, die nur dem jeweiligen Anlagenbereich zuzuordnen sind. Auf dieser Ebene empfiehlt es sich, VLANs für die logische Segmentierung bestimmter Funktionen wie Terminal-, Anlagen- und Managementbus sowie zur Anbindung einzelner isolierten Zellen zu nutzen. Dies bedingt den Einsatz von Layer-2 Switchen.

### Kriterien zur Bildung von Zellen:

- **Funktionale Beziehung:** Mehrere Maschinen derselben Produktionslinie können eine Zelle bilden
- **Echtzeitbedürfnisse:** Bei hohen Anforderungen an Latenz oder Taktsynchronität zwischen automatisierungstechnischen Komponenten, müssen sich diese Komponenten in derselben Zelle befinden
- **Funktionale Sicherheit:** Kritische Anwendungen im Sinne der funktionalen Sicherheit, die zu Schaden von Personal oder Maschinen führen können, erfordern eine Trennung zu anderen nicht-kritischen Anwendungen
- **Risiko:** Geräte, die als kritisch im Sinne der IT-Sicherheit angesehen werden (bspw. Rechner mit veralteten Betriebssystemen) können in dieselbe Zelle gruppiert werden, um ein- und ausgehende Datenströme kontrollieren zu können.

### BACKBONE LAYER

Der Backbone ist der zentrale Verbindungspunkt des Netzwerks. Die Netzwerkgeräte in dieser Ebene stellen die Verbindungen der Aggregationsebenen zu den Hosts des Datacenters und der DMZ und von dort aus zur IT her. Es werden hoch performante Netzwerkgeräte, sowie Next Generation Firewalls zur Koordinierung und Prüfung des Datenverkehrs eingesetzt.

### INDUSTRIAL DATACENTER

In diesem Netzwerkbereich befinden sich die Hosts zur Bereitstellung aller Anwendungen und Dienste, die ausschließlich im OT-Netzwerk genutzt werden und keine direkte Verbindung zur IT benötigen. Hierzu gehören virtualisierte Leittechnik-Server, Engineering-Server, Netzwerkmanagement, Backupsysteme, Betriebsdatenerfassung und RADIUS. Wird für den OT-Bereich eine von der IT unabhängige Domäne genutzt, können die Domain-Controller auch hier gehostet sein.

### INDUSTRIAL DMZ

Alle Systeme, die eine direkte Verbindung zur IT oder ins Internet benötigen, werden in einem physikalisch und logisch isolierten Netzwerksegment, der demilitarisierten Zone (DMZ) gehostet. Hierzu gehören Jump Server für Remote-Zugriffe, Windows Update Services, Antiviren-Server, MES, Filetransfer, Datengateway-Server oder Webdienste.
Eine DMZ kann auf zwei Arten erstellt werden:

- An einer einzelnen (redundanten) Firewall werden separate physikalische Ports genutzt, an denen die DMZ errichtet wird. Der Traffic von und zur DMZ wird von der Firewall überwacht.
- Noch sicherer ist es, zwei physikalisch getrennte (redundante) Firewalls zu nutzen, eine auf DMZ-Seite und eine auf der OT-Seite:

Wir empfehlen generell den Einsatz redundanter Firewalls, um die Netzverfügbarkeit auch im Fehlerfall oder bei Firmwareupdates zu gewährleisten.
Das DMZ-Konzept ist die logische Folge einiger Systemanforderungen der IEC 62443-3-3, insbesondere der SR5.1 RE 2 „Das Automatisierungssystem muss die Fähigkeit bieten, ohne eine Verbindung zu nicht automatisierungstechnischen Netzen Netzdienste bereitzustellen in automatisierungstechnischen Netzen […].“

### KRIKO ALS PARTNER FÜR INDUSTRIAL IT

Netzwerksegmentierung ist der Schlüssel zu einer sichereren Betriebssicherheit. Sie ist jedoch nur ein Teil eines ganzen OT-Sicherheitskonzeptes. Wir unterstützen SIe gerne bei der Erstellung Ihres individuellen Sicherheitskonzeptes.

## ANSPRECHPARTNER

**Felix Steinkuhl**
Automatisierungstechnik und Informationstechnik
+49 761 40078 45
felix.steinkuhl@kriko.com

**Deutschland**
Merzhauser Str. 120
79100 Freiburg im Breisgau
Tel. +49 761 40078 0

**Schweiz**
Riehenring 175
4058 Basel
Tel. +41 61 68324 80