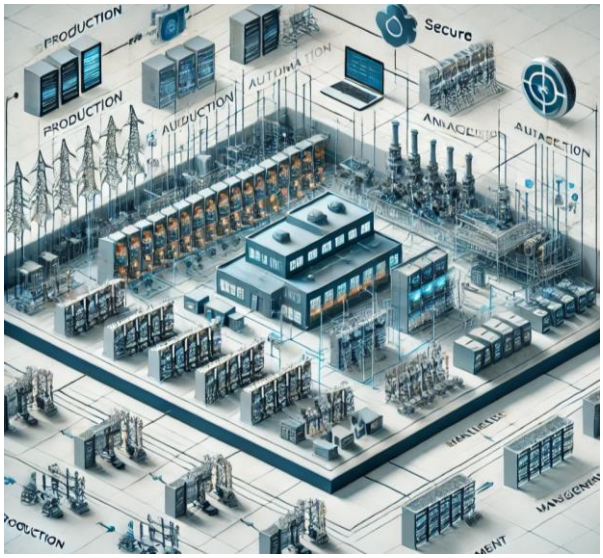
Controlware OT-Architekturdesign: sicheres und resilientes Planen von OT-Betriebsnetzen

Grundlagen und Zielsetzungen der OT-Architektur-Planung

Moderne industrielle Betriebe sind auf die Digitalisierung und Vernetzung angewiesen, um die Effizienz und Produktivität zu steigern. Traditionell getrennte Systeme für Produktionssteuerung und -überwachung (OT) und klassische IT-Infrastrukturen verschmelzen zunehmend. Allerdings werden OT-Netzwerke mit anderen Anforderungen konfrontiert als klassische IT-Netzwerke:

- **Echtzeitfähigkeit:** Prozesse müssen ohne Verzögerung ablaufen, da kleinste Latenzen die Produktion beeinflussen können.
- **Verfügbarkeit:** Minimale Ausfallzeiten sind entscheidend, da OT-Systeme häufig kontinuierlich in Betrieb sind.
- **Sicherheit:** Auch OT-Systeme sind potenzielle Ziele für Cyberangriffe, daher müssen diese Netzwerke besonders geschützt werden.

Die Zielsetzung der OT-Architekturplanung besteht darin, ein OT-Betriebsnetz zu schaffen, das diese Anforderungen erfüllt und gleichzeitig flexibel für zukünftige Erweiterungen ist − und auch technologische Fortschritte berücksichtigen kann.



Symbolbild für eine Betriebsnetz-Architektur

Herausforderungen bei der Planung von OT-Betriebsnetzen

Die Planung von OT-Betriebsnetzen birgt zahlreiche Herausforderungen. Da OT-Netzwerke oft für andere Zwecke als klassische IT-Netzwerke konzipiert sind, weisen sie auch andere Angriffsvektoren auf, die für potenzielle Angreifer attraktiv sein können. Viele Lagacy-OT-Systeme, die ursprünglich isoliert betrieben wurden, sind nicht für den sicheren Einsatz in vernetzten Umgebungen ausgelegt und benötigen angepasste Sicherheitsvorkehrungen.
In OT-Umgebungen werden hohe Anforderungen an Latenz und Netzwerk-Performance gestellt. In der Regel weichen diese Anforderungen oftmals stark von klassischen Office- oder Enterprise-Infrastrukturen ab und müssen gezielt berücksichtigt werden. Beispielsweise können Verzögerungen bei der Übertragung von Steuerungssignalen die Produktionsqualität und -sicherheit gefährden.

Die Integration herstellerspezifischer oder branchenspezifischer Protokolle erschwert zusätzlich die Kommunikation mit IT-Systemen. Zudem kann eine unzureichende Segmentierung unbefugten Geräten oder Nutzern den Zugriff auf kritische Bereiche des Produktionsnetzes ermöglichen, was erhebliche Sicherheits- und Stabilitätsprobleme nach sich ziehen kann.

Der Lösungsansatz: Planung des OT-Betriebsnetzes

Ohne Frage ist die Planung eines sicheren und widerstandsfähigen OT-Betriebsnetzes entscheidend, um die Verfügbarkeit und Stabilität industrieller Systeme zu gewährleisten. Der erste Schritt besteht darin, eine umfassende Netzwerksegmentierung vorzunehmen. Hierbei wird das Netzwerk in separate Bereiche unterteilt, die Produktionsprozesse von administrativen Systemen trennen. Diese Trennung dient als wichtige Sicherheitsmaßnahme, da sie den Datenverkehr kontrollierbarer macht und das Risiko von unerwünschten Zugriffen minimiert.

Darüber hinaus sind umfassende Schutzmechanismen notwendig, um die Sicherheit von OT-Netzwerken zu

gewährleisten. Dazu gehört eine gezielte Kontrolle des Datenflusses zwischen den Netzwerkbereichen, um unautorisierte Verbindungen zu verhindern. Verschlüsselte Verbindungen sorgen dafür, dass sensible Daten auch bei Zugriffen von außerhalb sicher übertragen werden. Eine konsequente Zugriffskontrolle stellt sicher, dass nur berechtigte Personen und Geräte Zugang zu kritischen Bereichen erhalten, wodurch das Risiko von Insider-Bedrohungen verringert wird.

Mit einem OT-SOC lassen sich Bedrohungen und Angriffe schneller erkennen. Somit ist eine schnelle Reaktion gewährleistet und Ihre OT-Umgebung wird möglichst unterbrechungsfrei in Betrieb bleiben.

Sprechen Sie uns dazu an!

Edge-Computing ist ebenfalls ein wesentlicher Bestandteil moderner OT-Architekturen, da die Latenzzeiten verringert und die Netzwerkleistung durch die Verarbeitung von Daten in der Nähe der Produktionsgeräte optimiert werden.

Eine modulare und skalierbare Struktur des Netzwerks sorgt dafür, dass das OT-Netzwerk flexibel auf sich verändernde Anforderungen reagieren kann, ohne umfangreiche Umstrukturierungen vornehmen zu müssen. So wird sichergestellt, dass sich zusätzliche Kapazitäten oder Funktionen problemlos integrieren lassen.

Eine enge Zusammenarbeit zwischen IT- und OT-Teams ist entscheidend, um eine robuste und sichere OT-Architektur zu schaffen. IT-Spezialisten bringen ihr Know-how in Sachen Netzwerksicherheit ein, während OT-Experten die Anforderungen der Produktionsprozesse verstehen. Eine gut abgestimmte Zusammenarbeit beider Bereiche ist die Grundlage, um den Anforderungen moderner Industrieumgebungen gerecht zu werden und das Unternehmen langfristig erfolgreich zu gestalten.

Wir stehen unseren Kunden in folgenden Situationen zur Seite:

- Design eines **vollständig neuen** Betriebsnetzes
- **Optimierung** eines bestehenden Betriebsnetzes
- **Erweiterung** eines bestehenden Betriebsnetzes

Vorteile eines sorgfältig geplanten OT-Betriebsnetzes

Eine sorgfältig geplante OT-Architektur bietet zahlreiche Vorteile. Die Implementierung von Segmentierungen und Sicherheitsmaßnahmen reduziert das Risiko von Cyberangriffen erheblich und sorgt für eine erhöhte Stabilität der Produktionssysteme. Zudem wird das Risiko von Betriebsstörungen und ungeplanten Stillstandzeiten durch eine widerstandsfähige Netzwerkinfrastruktur minimiert. Eine gut strukturierte OT-Architektur ist nicht nur besser auf zukünftige industrielle Anforderungen vorbereitet, sondern lässt sich auch einfacher erweitern oder an neue technische Entwicklungen anpassen. Die Zusammenarbeit zwischen IT- und OT-Abteilungen schafft Mehrwerte durch Synergien.

Insgesamt bildet eine gut strukturierte OT-Architektur die Basis für ein stabiles, sicheres und skalierbares Betriebsnetz, das den hohen Anforderungen moderner Produktionsumgebungen gerecht wird.

Warum Controlware?

Die Controlware GmbH ist ein führender IT-Dienstleister und Managed Service Provider mit über 40 Jahren Erfahrung. Wir entwickeln, implementieren und betreiben umfassende IT- und OT-Lösungen für Cloud-, Data Center-, Enterprise- und industrielle Umgebungen. Mit unserem ISO 27001-zertifizierten Customer Service Center gewährleisten wir höchste Servicequalität.

Die Controlware Experten verfügen über fundiertes Know-how in der Gestaltung moderner Netzwerke, einschließlich IT- und OT-Sicherheitslösungen. Wir unterstützen Kunden aus unterschiedlichsten Branchen bei der Absicherung und Optimierung ihrer IT- und OT-Infrastrukturen. Dabei legen wir besonderen Fokus auf die Integration von IT- und OT-Systemen, um Stabilität und Sicherheit zu gewährleisten.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf: