SIEMENS

Gezielt mehr Sicherheit in der industriellen Automatisierung

Das umfassende Angebot zum Schutz Ihrer Anlagen

Industrial Security

siemens.de/industrialsecurity

Gefahrenpotenziale mit System minimieren

Mit der steigenden Verwendung von Ethernet-Verbindungen bis in die Feldebene hinein gewinnen in der Industrie auch die damit verbundenen Sicherheitsfragen mehr und mehr an Bedeutung. Denn offene Kommunikation und eine zunehmende Vernetzung von Produktionssystemen bergen nicht nur enorme Chancen, sondern ebenso große Risiken. Um eine Industrieanlage unter dem Aspekt der IT-Sicherheit umfassend vor Angriffen zu schützen, müssen entsprechende Maßnahmen getroffen werden. Siemens unterstützt Sie dabei, diese Maßnahmen gezielt umzusetzen – im Rahmen unseres durchgängigen Angebotes für Industrial Security.

Security Services für Systeme und Lösungen

Industrial Security lässt sich nicht durch Produkte und Systeme allein erreichen. Als Partner der Industrie unterstützen wir Sie deshalb umfassend auf diesem Gebiet – von den ersten Planungsschritten über die Implementierung und den Betrieb einer maßgeschneiderten Sicherheitslösung, bis hin zu deren Modernisierung. Unsere professionellen Consulting-Dienstleistungen umfassen beispielsweise:

- Auf- und Ausbau von Know-how in **Workshops und Trainings**
- Analyse von **Schwachstellen**
- Zusammenstellung von **Whitelisting- und Firewall-Paketen**
- Konzeption **kundenspezifischer** Security-Lösungen

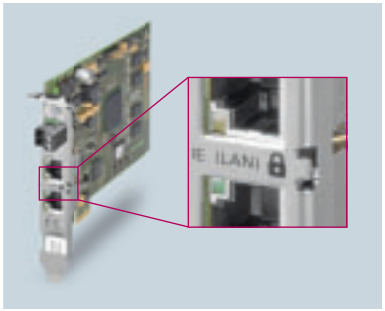
Integrierte Security in PCs und Steuerungen

Ganz im Sinne von Totally Integrated Automation, unserer offenen Systemarchitektur für die durchgängige Automatisierung, bieten wir Ihnen durchdachte Konzepte für die Sicherheit von PCs und Steuerungen.

- Benutzerverwaltung und rollenbasierte Zugriffskontrolle mit **SIMATIC® Logon** – für SIMATIC Engineering- und Runtime-Systeme
- Know-how-Schutz durch Verschlüsselung des Anwenderprogramms für **SIMATIC Controller**
- Whitelisting für den sicheren Betrieb unseres SCADA-Systems **SIMATIC WinCC** und unseres **Prozessleitsystems SIMATIC PCS 7**
- Virenscanner für PCs







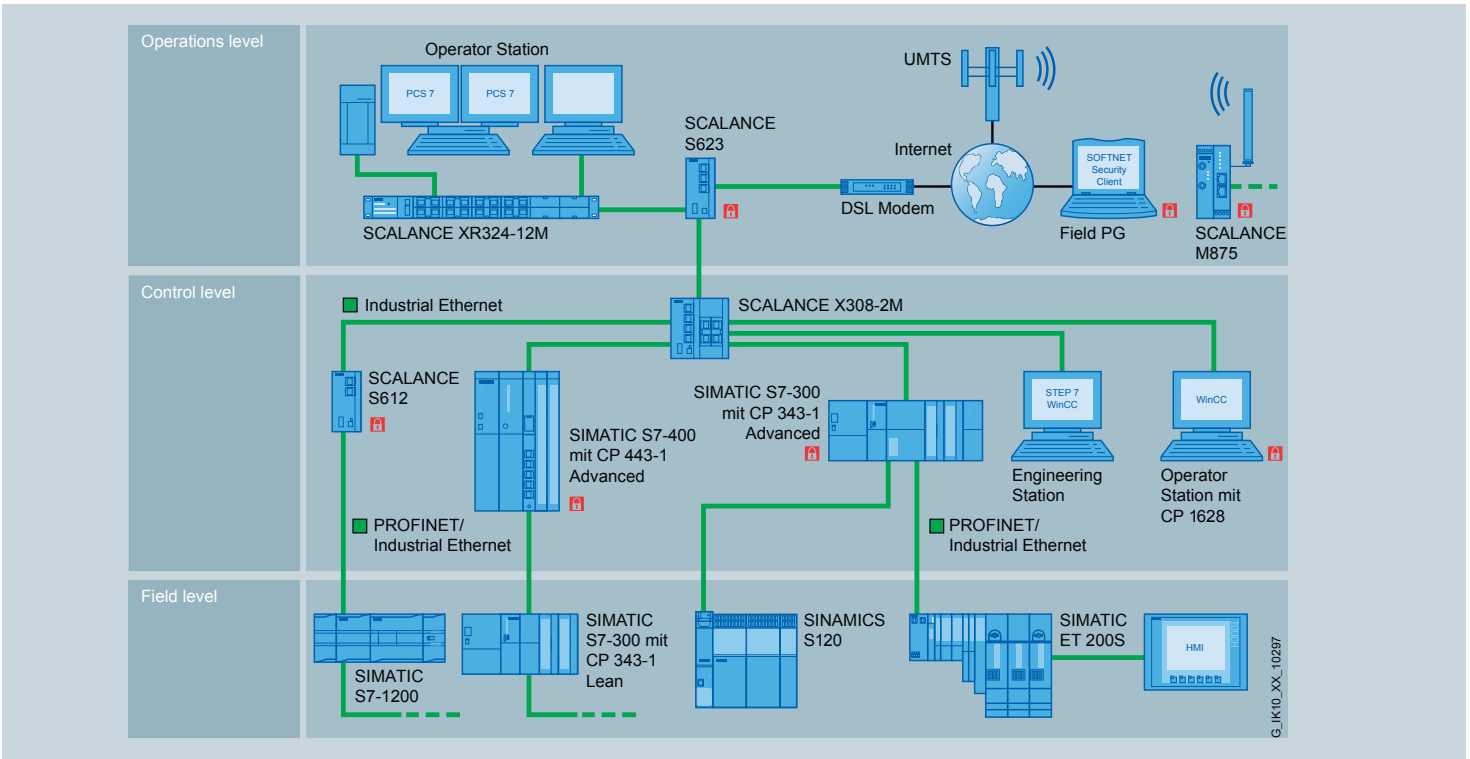
Neue Security-Produkte für Netzwerk und Kommunikation

Industrielle Kommunikation ist ein Schlüsselfaktor für den Schutz Ihres Unternehmens – um das Risiko einer Attacke zu minimieren. Aus diesem Grund bieten wir Ihnen Security-Module und Software sowie Komponenten mit Security Integrated für die Realisierung des Zellenschutzkonzepts.

- Security-Module SCALANCE S, z. B. S623 mit zusätzlichem DMZ-Port (Demilitarized Zone), der einen separaten und bei Bedarf eingeschränkten Netzwerkzugang für Servicezwecke eröffnet, z. B. für die Fernwartung über Internet.
- Die Software SOFTNET Security Client ermöglicht über Internet oder ein firmeninternes Netzwerk den Zugriff auf Automatisierungszellen oder PCs, die durch SCALANCE S oder eine Komponente mit Security Integrated geschützt sind.

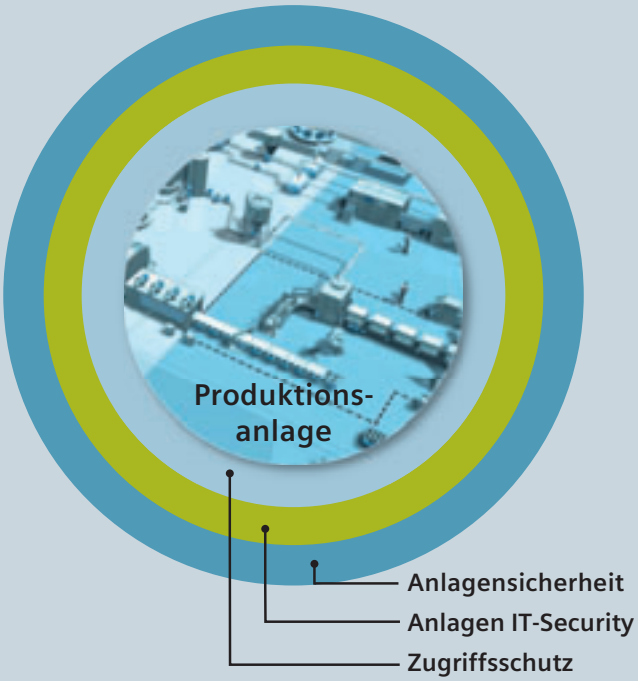
Security Integrated

- Schutz von Steuerungen vom Typ SIMATIC S7-300 und S7-400 durch Kommunikationsprozessoren CP 343-1 Advanced und CP 443-1 Advanced, die in ihrer neuen Version sowohl Firewall- als auch VPN-Funktionen (Virtual Private Network) beinhalten.
- Über den Kommunikationsprozessor CP 1628 werden Industrie-PCs durch Firewall und VPN geschützt – für eine sichere Kommunikation ohne Spezialeinstellungen des Betriebssystems. Auf diesem Wege lassen sich mit der Baugruppe ausgestattete Rechner mit geschützten Zellen verbinden.
- UMTS-Router SCALANCE M875 für einen sicheren Zugriff auf Anlagenteile über das UMTS-Mobilfunknetz.



Zellenschutzkonzept

Hierbei wird ein Anlagennetzwerk in einzelne geschützte Automatisierungszellen segmentiert, innerhalb derer alle Geräte sicher untereinander kommunizieren können. Die Anbindung der einzelnen Zellen an das Gesamtnetzwerk erfolgt gesichert per VPN und Firewall. Der Zellenschutz reduziert die Störungsanfälligkeit der gesamten Produktionsanlage und erhöht damit deren Verfügbarkeit. Zur Realisierung können SCALANCE S sowie die Komponenten mit Security Integrated eingesetzt werden.



Nur Gesamtlösungen bieten maximalen Schutz

Ob es um Erfindungen, Patente, Rezepturen oder anderes geistiges Eigentum geht: Für Ihren Unternehmenserfolg ist es von zentraler Bedeutung, dass Sie bestehendes Know-how effizient und nachhaltig vor Spionage schützen. Zudem müssen Sie jede unerlaubte Manipulation an Ihren Automatisierungsprozessen von vornherein ausschließen, da nur so Integritätsschutz gewährleistet ist. Ein weiteres wichtiges Thema: der zuverlässige Schutz vor Sabotage, also das Verhindern von Störungen in Ihren Produktionsprozessen – beispielsweise Anlagenstillstände durch einen Virusbefall. Unsere Antwort auf diese vielfältigen Bedrohungsszenarien: Wir betrachten Industrial Security als Ganzes und konzipieren Gesamtlösungen, die Ihren Anlagen ein Höchstmaß an Schutz bieten.

Whitelisting
Ob Personen, Unternehmen oder Programme: Eine Weiße Liste – oder auch Positivliste – bezeichnet eine Sammlung gleicher Elemente, die als vertrauenswürdig eingestuft werden. Whitelisting für PCs sorgt dafür, dass nur erwünschte Programme ausgeführt werden können.

Eckpunkte für effiziente Industrial Security-Lösungen

Bei der Planung und Realisierung effizienter Industrial Security-Lösungen müssen folgende fünf Ansatzpunkte berücksichtigt werden:

Industrial Security Konzept

Implementierung eines zweckmäßigen übergreifenden **Sicherheitsmanagements** hinsichtlich der Technologie sowie der Engineering- und Fertigungsprozesse.

Die **Schnittstellen** zu Office-IT und Internet/Intranet unterliegen klaren Vorschriften – und werden entsprechend überwacht.

Schutz **PC-basierter Systeme** (HMI, Engineering und PC-basierte Steuerungen) durch Antivirus-Software, Whitelisting und integrierte Security-Mechanismen.

Schutz der **Steuerungsebene**
- durch bereits in Automatisierungs- und Antriebskomponenten integrierte Sicherheitsfunktionen, die automatisch aktiv sind – z. B. IP-Hardening
- durch Sicherheitsfunktionen, die durch den Programmierer aktiviert werden müssen – z. B. Einrichten von Zugangspasswörtern

Überwachung der gesamten **Kommunikation** mit Systemen zur Eindringlingserkennung und intelligente Unterteilung des Netzwerks mithilfe von Firewalls.

Das Industrial Security Konzept basiert auf fünf Kernelementen zum Schutz industrieller Anlagen auf allen drei Ebenen.

Für weitere Informationen zu gezielten Maßnahmen gegen jedes denkbare Bedrohungsszenario wenden Sie sich bitte einfach an die Experten unseres Consulting-Teams:

industrialsecurity.i@siemens.com

Siemens AG
Industry Sector
Industry Automation
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Änderungen vorbehalten 11/11
Bestell-Nr.: E20001-A1020-P200
Dispostelle 06303
SCHÖ/36244 MI.AS.IS.52.2.01 SB 11110.5
Gedruckt in Deutschland