SIEMENS

Industrial Security

Netzwerksicherheit

Broschüre

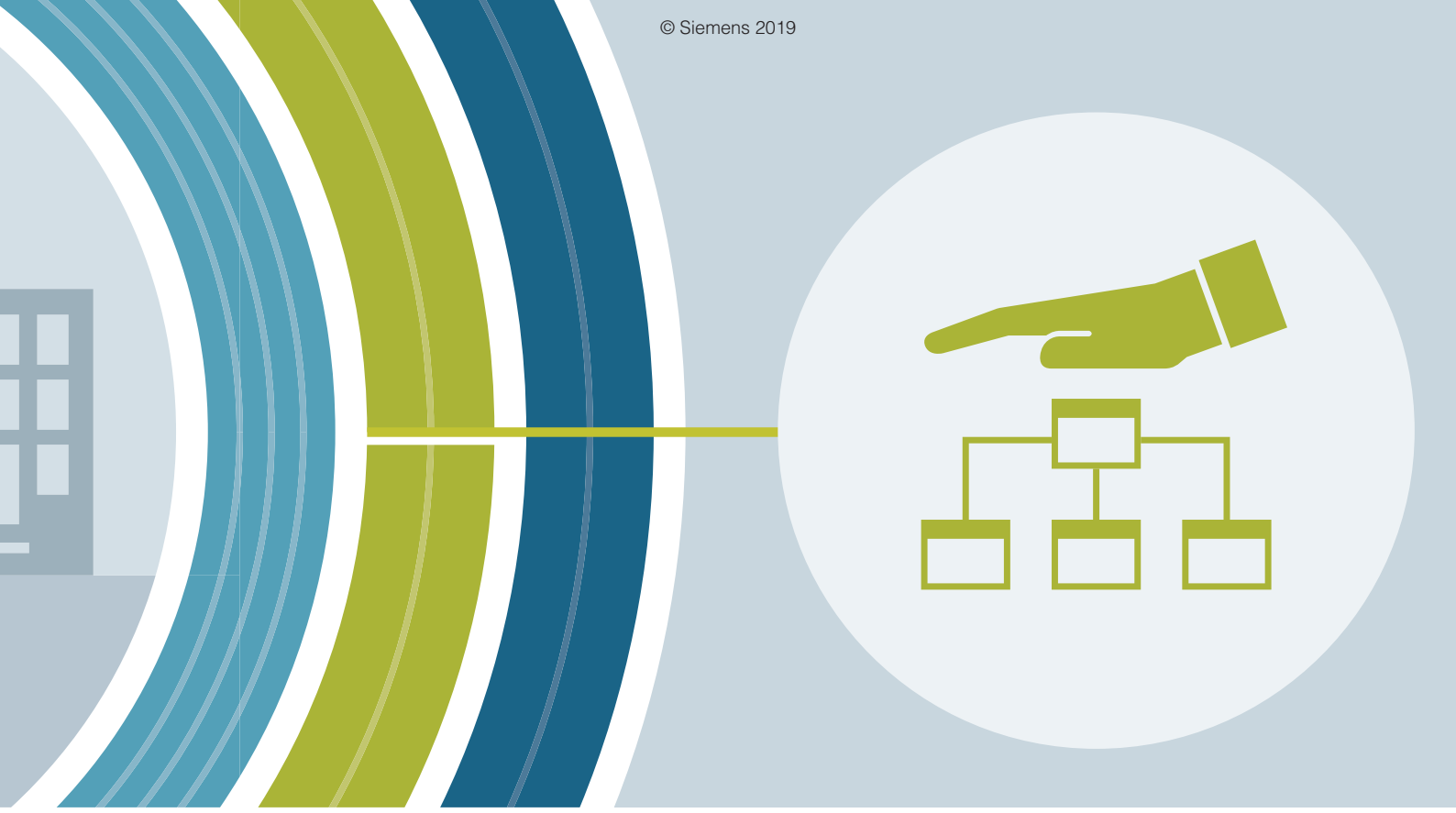
Ausgabe 11/2019

siemens.de/netzwerksicherheit

**Das Internet wirkt als enormer Beschleuniger von Geschäftsprozessen und revolutioniert das globale Geschäftsgeschehen.
Man kann den dadurch bewirkten Umbruch in der produzierenden Industrie auch als Revolution – die 4. industrielle Revolution – bezeichnen. Industrie 4.0 betrifft alle Aspekte des industriellen Wertschöpfungsprozesses, wobei industrielle Kommunikation und Security wesentliche Aspekte sind.**

Entscheidend dabei ist, dass angesichts der Digitalisierung und der immer stärkeren Vernetzung von Maschinen und Anlagen auch stets der Datensicherheit Rechnung getragen wird. Der Einsatz exakt auf die Industrie zugeschnittener Industrial Security-Lösungen ist deshalb von elementarer Bedeutung – und sollte untrennbar mit der industriellen Kommunikation verknüpft sein.

Durch die stetig steigende Anzahl konvergenter Netzwerke in Unternehmen und der immer häufiger werdenden Cyberangriffen gewinnt auch das Thema Cybersecurity kontinuierlich an Bedeutung und ist bereits seit Längerem Gegenstand der Standardisierungsbemühungen internationaler Gremien, wie der Internationalen Elektrotechnischen Kommission - IEC.
Darüber hinaus wird Security auch auf nationaler Ebene durch Gesetze und Vorgaben reguliert, die insbesondere kritische Infrastrukturen adressieren, um dort den gestiegenen Sicherheitsanforderungen Rechnung zu tragen. Beispiele hierfür sind das bundesdeutsche IT-Sicherheitsgesetz, die ANSSI-Zertifizierung in Frankreich oder NERC CIP in den USA und viele weitere. Dank dieser Standards und Vorgaben können letztlich die enormen Chancen genutzt werden, die eine offene Kommunikation und eine zunehmende Vernetzung von Produktionssystemen mit sich bringen, wobei aber auch die einhergehenden, großen Risiken entsprechend adressiert werden. Siemens unterstützt Sie dabei, Ihre Industrieanlage im Rahmen eines durchgängigen Angebotes für Industrial Security adäquat vor Cyberangriffen zu schützen.



Inhalt

Industrial Security

Ein Blick auf die Bedrohungslage

Nr.	Bedrohung	Erläuterung
1	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Der Einsatz von Wechseldatenträgern und mobilen IT-Komponenten externer Mitarbeiter stellt stets eine große Gefahr bzgl. Malware-Infektionen dar. Die Auswirkungen von Schadsoftware hingegen sind den Mitarbeitern häufig nicht bewusst.
2	Infektion mit Schadsoftware über Internet und Intranet	In Unternehmensnetzwerken genutzte Standartkomponenten (z. B. Betriebssysteme, Datenbanken, Browser oder E-Mail Clients) enthalten zumeist Schwachstellen, die ein Angreifer zum Eindringen in das Firmennetzwerk nutzen kann. Aus dem infiltrierten Intranet oder Office-Netzwerk heraus, kann sich der Angreifer häufig direkt oder mit einem Folgeangriff in das Produktionsnetzwerk vorarbeiten.
3	Menschliches Fehlverhalten und Sabotage	Vorsätzliche Handlungen - ganz gleich ob durch interne oder externe Täter - sind eine massive Bedrohung für sämtliche Schutzziele Die Sicherheit kann niemals ausschließlich durch technische Maßnahmen gewährleistet werden, sondern bedarf immer gelebter organisatorischer Regelungen.
4	Kompromittierung von Extranet und Cloud-Komponenten	Outsourcing von IT-Komponenten in Cloud-Lösungen führt dazu, dass Anlagenbetreiber teilweise nur noch eine sehr eingeschränkte Kontrolle über die Sicherheit dieser Komponenten und die damit verbundene Möglichkeiten einer Kompromittierung haben. Die Komponenten selbst können jedoch unmittelbar mit der lokalen Produktion vernetzt sein.
5	Social Engineering und Phishing	Social Engineering ist eine Methode, um durch meist nicht-technische Handlungen und durch Ausnutzung menschlicher Eigenschaften wie z. B. Neugier, Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität unberechtigt Zugang zu Informationen oder IT-Systemen zu erlangen. Ein klassisches Beispiel hierfür sind betrügerische E-Mails, sogenannte Phishing-Mails, die dazu verleiten manipulierte Links oder Anhänge mit Schadsoftware zu öffnen.
6	(D)DoS Angriffe	Durch (Distributed) Denial of Service Angriffe können sowohl drahtgebundene als auch drahtlose Netzwerkverbindungen sowie benötigte Systemressourcen beeinträchtigt werden, wodurch Systeme zum Absturz gebracht werden können, z. B. um die Funktionsfähigkeit eines ICS zu stören.
7	Internet-verbundene Steuerungskomponenten	ICS-Komponenten werden entgegen den Empfehlungen der Hersteller direkt mit dem Internet verbunden verfügen jedoch oft nicht über ein hinreichendes Sicherheitsniveau und Sicherheitsmechanismen.
8	Einbruch über Fernwartungszugänge	In ICS-Installationen sind externe Zugänge für Wartungszwecke weit verbreitet. Dabei existieren oft Default-Zugänge mit Standard- oder fest kodierten Passwörtern. Über die Wartungszugänge für bestimmte Systeme die häufig von Herstellern und externen Dienstleistern genutzt werden, sind auch weitere Systeme zu erreichen.
9	Technisches Fehlverhalten und höhere Gewalt	Ausfälle durch extreme Umwelteinflüsse oder technische Defekte sind immer möglich – Risiko und Schadenspotential können hier lediglich minimiert werden.
10	Kompromittierung von Smartphones im Produktionsumfeld	Die Anzeige sowie die Veränderung von Betriebs- oder Produktionsparametern auf einem Smartphone oder Tablet wird im Produktionsumfeld immer häufiger eingesetzt. Ein Fernwartungszugang über ein Smartphone oder Tablet stellt einen Sonderfall dar und fügt zusätzliche Angriffsfläche hinzu.

Bedrohungen im Überblick

Quelle:
Basierend auf BSI-CS 005 | Version 1.30 vom 01.01.2019
Hinweis:
Die Auflistung der Bedrohungen ist in enger Zusammenarbeit zwischen BSI und Vertretern der Wirtschaft entstanden.
Mit den BSI-Analysen veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) Statistiken und Berichte zu aktuellen Themen der Cybersecurity.

Defense in Depth

Netzwerksicherheit als zentraler Bestandteil des Industrial Security-Konzeptes von Siemens

Mit Defense in Depth bietet Siemens ein vielschichtiges Konzept, das Ihre Anlage sowohl rundum als auch in die Tiefe schützt. Das Konzept basiert auf Anlagensicherheit, Netzwerksicherheit und Systemintegrität – nach den Empfehlungen der IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung.

Anlagensicherheit

Anlagensicherheit sichert mit verschiedenen Methoden den physischen Zugang von Personen zu kritischen Komponenten. Dies beginnt mit dem klassischen Gebäudezutritt und reicht bis zur Sicherung sensibler Bereiche mittels Codekarten. Umfassendes Security Monitoring führt zu Transparenz über den Security-Status von Produktionsstätten. Dank kontinuierlicher Analysen und Korrelationen von bereits vorhandenen Daten sowie durch den Abgleich dieser mit Bedrohungsindikatoren können Security-relevante Ereignisse erkannt und nach Risikofaktoren klassifiziert werden. Auf dieser Basis und durch regelmäßige Statusberichte erhalten Betreiber eine Übersicht über den aktuellen Sicherheitsstatus der Produktionsstätte, was eine schnelle Reaktion im Bedrohungsfall ermöglicht.

Netzwerksicherheit

Netzwerksicherheit bedeutet Schutz von Automatisierungsnetzwerken vor unbefugten Zugriffen. Dies beinhaltet die Kontrolle aller Schnittstellen wie z. B. zwischen Büro- und Anlagennetzwerk oder der Fernwartungszugänge zum Internet und kann mittels Firewalls und gegebenenfalls durch den Aufbau einer DMZ (demilitarisierte Zone = sicherheitstechnisch abgeschirmte Zone) erfolgen. Die DMZ dient zur Bereitstellung von Daten für andere Netzwerke, ohne direkten Zugang zum Automatisierungsnetzwerk zu gewähren. Die sicherheitstechnische Segmentierung des Anlagennetzwerks in einzelne geschützte Automatisierungszellen, dient der Risikominimierung und Erhöhung der Sicherheit. Die Aufteilung der Zellen und Zuordnung der Geräte erfolgt nach Kommunikations- und Schutzbedarf. Die Datenübertragung kann mittels Virtual Private Network (VPN) verschlüsselt und so vor Datenspionage und Manipulation geschützt werden. Die Kommunikationsteilnehmer werden sicher authentifiziert. Mit Industrial Security Appliances SCALANCE S, Industrie-Routern SCALANCE M oder Security Kommunikationsprozessoren für SIMATIC können Automatisierungsnetzwerke, Automatisierungssysteme und die industrielle Kommunikation gesichert werden.

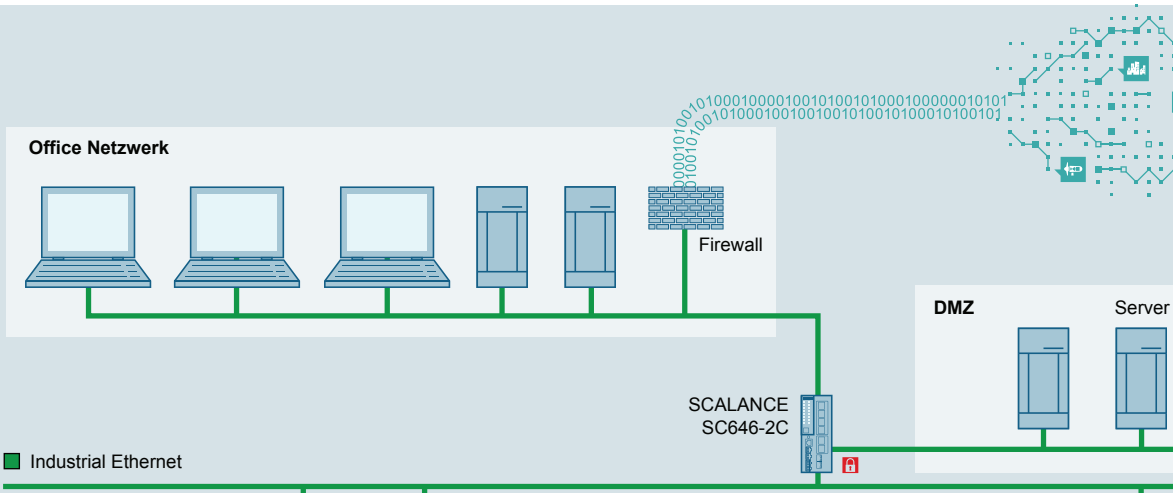
Systemintegrität

Die dritte tragende Säule von Defense in Depth ist die Sicherung der Systemintegrität. Hierbei steht im Mittelpunkt, Automatisierungssysteme und Steuerungskomponenten wie SIMATIC S7-1200 und S7-1500 sowie SCADA und HMI-Systeme gegen unbefugte Zugriffe zu schützen oder spezielle Anforderungen wie Know-how-Schutz zu erfüllen. Weiterhin geht es um die Authentifizierung von Benutzern, um Zugriffs- und Änderungsberechtigungen sowie um die Systemhärtung, also die Robustheit der Komponenten gegen mögliche Angriffe.

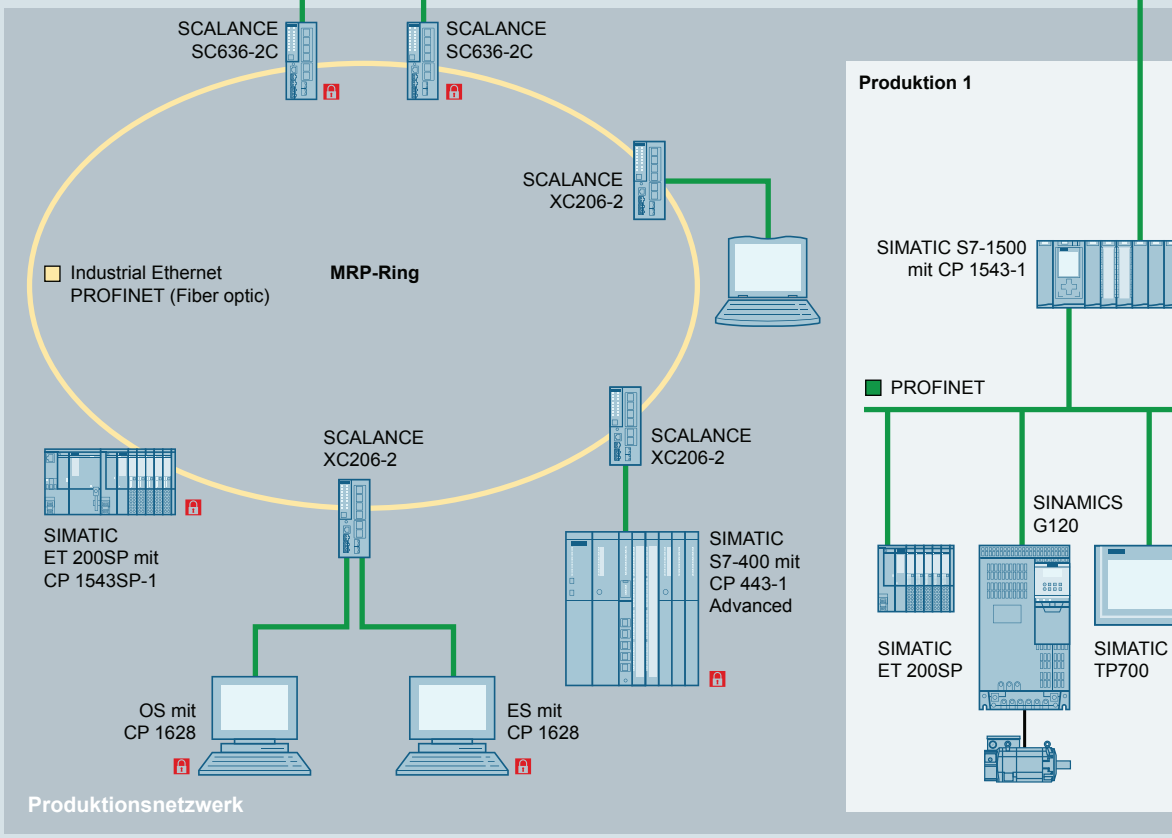
Industrial Security im Überblick

Anlagensicherheit

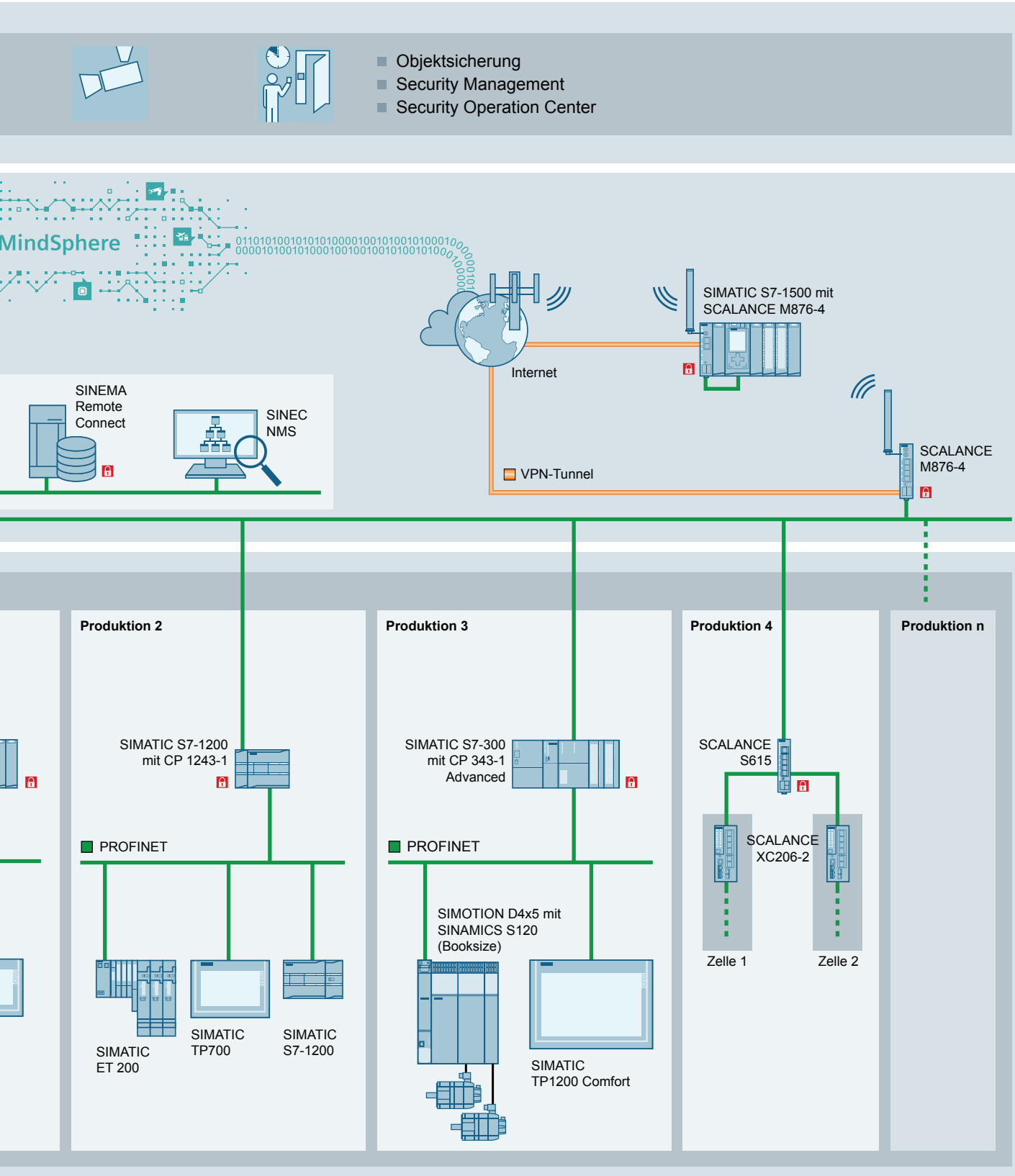
Netzwerksicherheit



Systemintegrität



Gesicherte Kommunikation, Netzwerkzugangsschutz und Netzwerksegmentierung mit Security Integrated-Komponenten



Industrial Security – Mehr als nur Produktfunktionen

Um ebenfalls einen weiteren Schritt in eine sichere digitale Welt zu machen hat Siemens nicht nur als erstes Unternehmen eine auf IEC 62443-4-1 basierende TÜV SÜD-Zertifizierung für den übergreifenden Entwicklungsprozess in der Automatisierungs- und Antriebstechnik erhalten, sondern ist auch Initiator der sogenannten „Charter of Trust".

Anhand von 10 Grundprinzipien stellen sich die Mitglieder der „Charter of Trust" selbst den drei Zielen, die Daten von Einzelnen und Unternehmen zu schützen, Menschen, Unternehmen und Infrastrukturen vor Schaden zu bewahren und ein zuverlässiges Fundament zu schaffen, in dem das Vertrauen in eine vernetzte digitale Welt verankert wird und auf dem es wachsen kann.

Industrial Security als Teil von Totally Integrated Automation

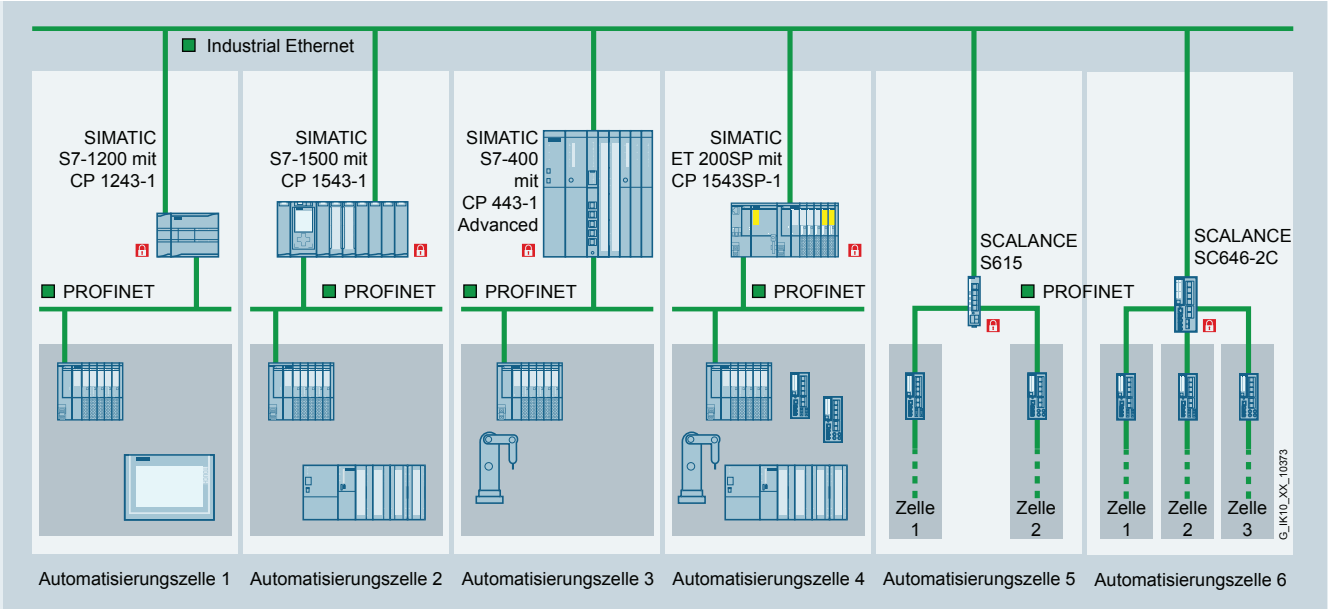
Totally Integrated Automation:
Effizientes Zusammenwirken aller Automatisierungskomponenten

Mit industrietauglichen und im TIA Portal integrierten Securityprodukten für Netzwerksicherheit und Systemintegrität lässt sich Ihre Automatisierungslösung effizient absichern und das Security-Konzept Defense in Depth zum Schutz industrieller Anlagen und Automatisierungssysteme umsetzen.

Alle Industrial Security Appliances und Remote Networks Komponenten sind im TIA-Portal integriert und können dort konfiguriert werden. Neben einer zentralen Benutzerverwaltung durch die TIA Portal Option UMC werden zudem die Firewall-Regeln für die Security Kommunikationsprozessoren automatisch über TIA Portal vergeben.

Netzwerksicherheit

Zellenschutzkonzept



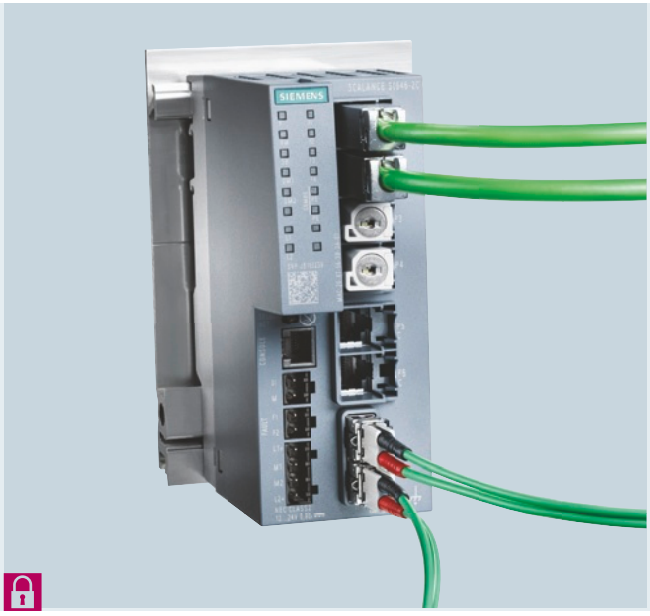
Gesicherte Kommunikation zwischen Komponenten mit Security Integrated in getrennten Automatisierungszellen

Industrielle Kommunikation ist ein Schlüsselfaktor für den Unternehmenserfolg – solange das Netzwerk geschützt ist. Als Partner bietet Siemens seinen Kunden zur Realisierung des Zellenschutzkonzeptes deshalb Komponenten mit Security Integrated, die neben ihren Kommunikationsfunktionen auch spezielle Security-Funktionen wie Firewall und VPN integriert haben.

Cybersecurity - umfassende Sicherheitsmechanismen
Siemens hilft seinen Kunden, vom technologischen Fortschritt zu profitieren und gleichzeitig Risiken in Bereichen wie Cybersecurity möglichst gering zu halten. Die Implementierung einer Sicherheitslösung verläuft nur dann optimal, wenn sie kontinuierlich an neue Bedrohungen angepasst wird. Unter Berücksichtigung dieses Umstands, bieten Siemens-Produkte, -Lösungen und -Services für Cybersecurity bewährten Schutz in Industrieanlagen, Automatisierungssystemen sowie in industriellen Netzwerken.

Zellenschutzkonzept
Beim Zellenschutzkonzept wird ein Anlagennetzwerk in einzelne geschützte Automatisierungszellen segmentiert, innerhalb derer alle Geräte gesichert untereinander kommunizieren können. Die Anbindung der einzelnen Zellen an das Anlagennetzwerk erfolgt gesichert mit VPN und Firewall. Der Zellenschutz reduziert die Störungsanfälligkeit der gesamten Produktionsanlage und erhöht damit deren Verfügbarkeit. Zur Realisierung können Security Integrated-Produkte wie Industrial Security Appliances SCALANCE S, Industrie-Router SCALANCE M oder Security Kommunikationsprozessoren eingesetzt werden.

Industrial Security Appliance SCALANCE S



Die SCALANCE S Industrial Security Appliances dienen dem Schutz von Geräten und Netzwerken in der diskreten Fertigung sowie der Prozessindustrie und sichern die industrielle Kommunikation mit Mechnismen wie Stateful Inspection Firewall sowie Virtual Private Networks (VPN). Die für industrienahe Applikationen geeigneten Geräte sind je nach Anforderung in unterschiedlichen Portausprägungen (2 bis 6 Ports) und Funktionsumfang (Firewall oder Firewall + VPN) verfügbar. Alle Varianten ermöglichen die Konfiguration über Web Based Management (WBM), Command Line Interface (CLI) , Simple Network Management Protocol (SNMP), Netzwerkmanagement SINEC NMS sowie TIA Portal.

Alle Industrial Security Appliances unterstützen:

- Benutzerspezifische Firewall
- Network Address Translation (NAT), Network Address Port Translation (NAPT) zur Kommunikation zu Serienmaschinen, die über identische IP-Adressbänder verfügen
- Autokonfigurations-Schnittstelle zur einfachen Projektierung einer Verbindung zu SINEMA Remote Connect
- Digitaler Eingang (DI) zum Anschluss eines Schlüsselschalters für den kontrollierten Aufbau einer Tunnelverbindung
- Einfacher Gerätetausch mit C-PLUG
- Redundanz-Mechanismen durch VRRPv3

Erfahren Sie mehr zu Industrial Security Appliances unter:
siemens.de/scalance-s
Weitere Informationen zu SINEMA Remote Connect auf Seite 18.

Industrial Firewall Appliances

SCALANCE SC632-2C und SCALANCE SC636-2C

- Firewall-Performance ca. 600 Mbit/s
- gesicherter Zugang zwischen getrennten Netzwerksegmenten durch Bridge-Firewall
- Anschluss über 10/100/1000 Mbit/s Ports sowie Fiber Optic für große Distanzen (bis zu 200 km)
- Konsolen-Port für den direkten Zugriff über Programmiergerät
- gesicherte, redundante MRP/HRP-Anbindung bei SCALANCE SC636-2C

Industrial VPN Appliances

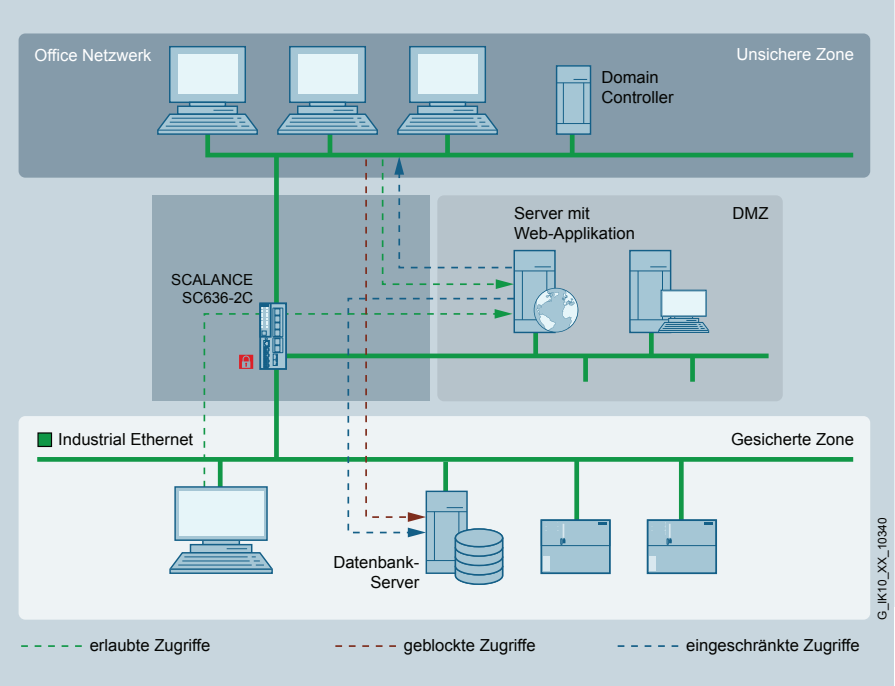
SCALANCE S615

- Firewall-Performance ca. 100 Mbit/s
- Verwaltung von bis zu 20 VPN Verbindungen mit einer Datenrate von bis zu 35 Mbit/s
- Anschluss über 10/100 Mbit/s Ports

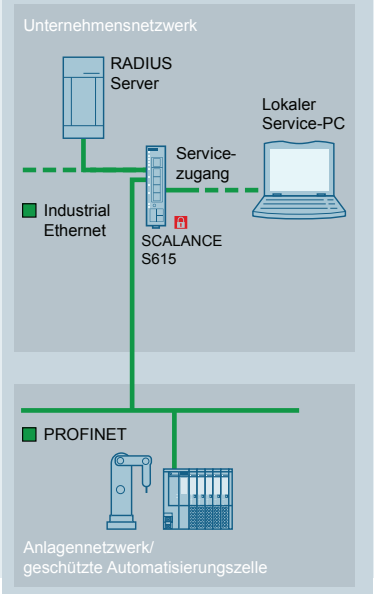
SCALANCE SC642-2C und SCALANCE SC646-2C

- Firewall-Performance ca. 600 Mbit/s
- gesicherter Zugang zwischen getrennten Netzwerksegmenten durch Bridge-Firewall
- Verwaltung von bis zu 200 VPN Verbindungen mit einer Datenrate von bis zu 120 Mbit/s
- Anschluss über 10/100/1000 Mbit/s Ports sowie Fiber Optic für große Distanzen (bis zu 200 km)
- Konsolen-Port für den direkten Zugriff über Programmiergerät
- gesicherte, redundante MRP/HRP-Anbindung bei SCALANCE SC646-2C

Anwendungsbeispiel
Netzwerkzugangsschutz mit DMZ



Netzwerksicherheit als zentraler Bestandteil des Industrial Security-Konzeptes von Siemens



Anschluss eines lokalen Service-PCs über SCALANCE S615

Aufgabenstellung
Netzwerkteilnehmer oder Server (z. B. MES-Server) sollen sowohl aus dem gesicherten wie aus dem ungesicherten Netzwerk erreichbar sein, ohne dass eine direkte Verbindung zwischen den Netzwerken besteht.

Lösung
Eine DMZ kann mithilfe eines SCALANCE SC636-2C eingerichtet werden. In dieser DMZ können die Server platziert werden.

Vorteile auf einen Blick

- Erhöhung der Sicherheit durch Datenaustausch über DMZ und Vermeidung des direkten Zugriffs auf das Automatisierungsnetzwerk
- Schutz von Automatisierungsnetzwerken vor unbefugten Zugriffen bereits an den Netzwerkgrenzen

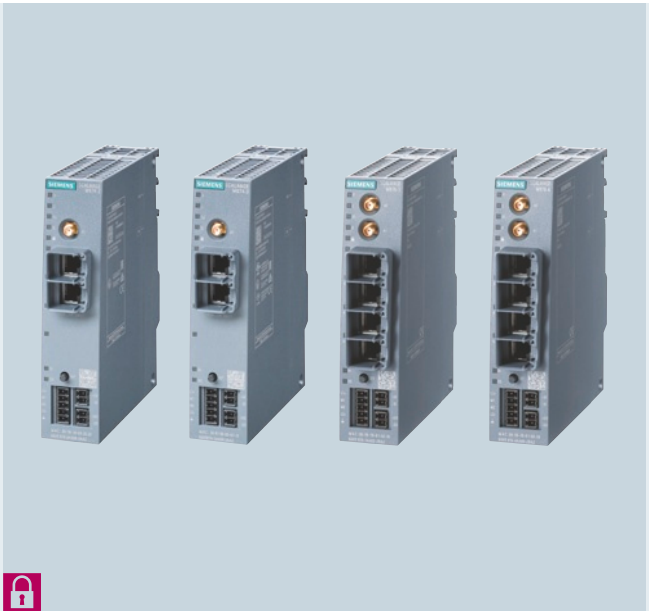
Aufgabenstellung
Die lokalen Netzwerkzugänge sollen gegen unbefugte Zugriffe gesichert werden und Berechtigte Zugriffsrechte nur gemäß ihrer Rollen erhalten.

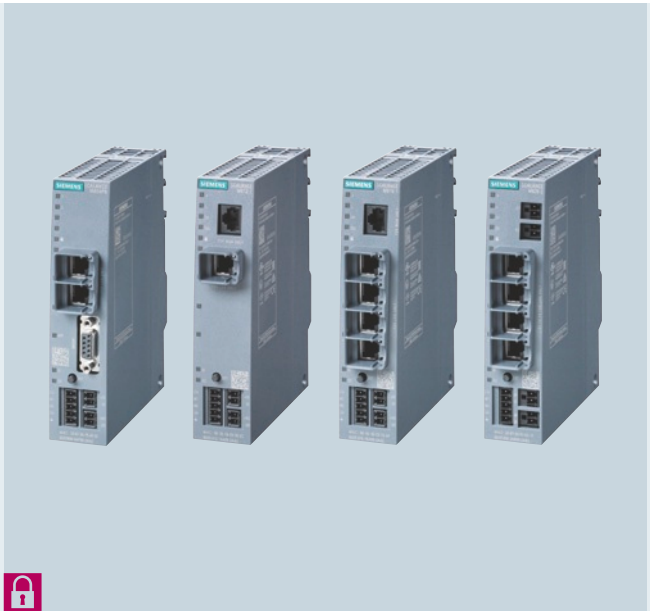
Lösung
Der als DMZ-Port definierte Port der Industrial Security Appliance (in diesem Fall der des SCALANCE S615) ist der einzige lokal zugängliche Port. Die Industrial Security Appliance ist mit dem Anlagennetzwerk und einer unterlagerten Automatisierungszelle verbunden.
Für jeden Anwender werden benutzerspezifische Firewall-Regeln erstellt. Um Zugang zum Netzwerk zu erlangen, muss sich der Anwender auf dem SCALANCE S mit Kennung und Passwort einloggen.

Vorteile auf einen Blick

- Sicherung der lokalen Netzwerkzugänge
- Flexible und anwenderspezifische Zugriffsrechte
- Zentrale Authentifizierung mittels RADIUS möglich

Anwendungsbeispiel
Industrie-Router SCALANCE M





Das SCALANCE M-Portfolio besteht aus Routern für Applikation für Industrial Remote Communication, wie Telecontrol und Teleservice. Die integrierten Security-Funktionen Firewall und VPN (IPsec; OpenVPN als Client und zur Anbindung an SINEMA Remote Connect) schützen vor unbefugten Zugriffen und sichern die Datenübertragung.

Drahtlose Anbindung an Remote Networks
Die drahtlosen SCALANCE M-Router nutzen die weltweit verfügbaren, öffentlichen Mobilfunknetze (2G, 3G, 4G) zur Datenübertragung.

SCALANCE M874-2 unterstützt die GSM Datendienste GPRS (General Packet Radio Service) und EDGE (Enhanced Data Rates for GSM Evolution).

SCALANCE M874-3 unterstützt den UMTS Datendienst HSPA+ (High Speed Packet Access) und ermöglicht dadurch hohe Übertragungsraten von bis zu 14,4 Mbit/s im Downlink und bis zu 5,76 Mbit/s im Uplink.

SCALANCE M876-3 unterstützt Dual Band CDMA2000 und den UMTS Datendienst HSPA+. Damit ermöglicht das Gerät hohe Übertragungsraten im Downlink von bis zu 14,4 Mbit/s und im Uplink von bis zu 5,76 Mbit/s.

SCALANCE M876-4 unterstützt LTE (Long Term Evolution) und ermöglicht hohe Übertragungsraten im Downlink von bis zu 100 Mbit/s und bis zu 50 Mbit/s im Uplink.

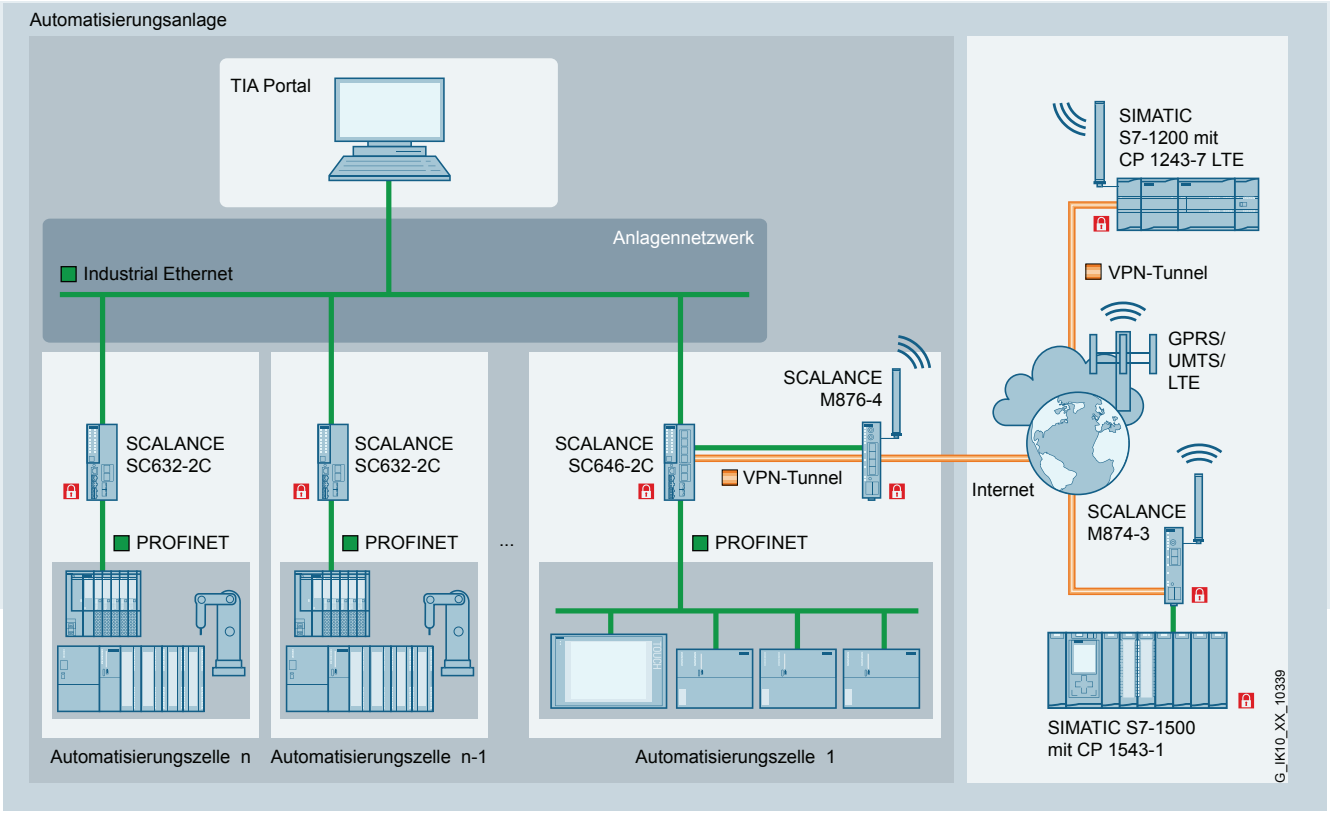
Drahtgebundene Anbindung an Remote Networks
Die drahtgebundenen Router der SCALANCE M-Produktfamilie unterstützen die kostengünstige und gesicherte Anbindung von Ethernet-basierten Subnetzen und Automatisierungsgeräten. Die Anbindung kann über bestehende Zwei- oder Mehrdrahtleitungen oder über kabelgebundene Telefon- bzw. DSL-Netze erfolgen. Auch die Anbindung von PROFIBUS-Anlagen ist ohne zusätzliche Adapter oder Software möglich.

SCALANCE M804PB unterstützt PROFIBUS/ MPI. Damit ermöglicht das Gerät den gesicherten Fernzugriff auf Bestandsanlagen. Es können Übertragungsraten von bis zu 12 Mbit/s erzielt werden.

SCALANCE M812-1 und SCALANCE M816-1 sind DSL-Router für die Anbindung an kabelgebundene Telefon- bzw. DSL-Netze, die ADSL2+ (Asynchronous Digital Subscriber Line) unterstützen. Damit ermöglichen die Geräte hohe Übertragungsraten von bis zu 25 Mbit/s im Downlink und bis zu 1,4 Mbit/s im Uplink).

SCALANCE M826-2 ist ein SHDSL-Modem für die Anbindung über bestehende Zwei- oder Mehrdrahtleitungen und unterstützt den ITU-T-Standard G.991.2. Damit ermöglicht das Gerät hohe symmetrische Übertragungsraten von bis zu 15,3 Mbit/s pro Adernpaar.

Anwendungsbeispiel
Gesicherte Fernwartung mit SCALANCE M und SCALANCE S



Gesicherter Fernzugriff ohne direkte Verbindung zum Automatisierungsnetzwerk mit Industrial Security-Komponenten

Aufgabenstellung
Ein Systemintegrator möchte für Servicezwecke gesichert über Internet auf seine Maschine oder einen Anlagenteil beim Endanwender zugreifen. Er soll jedoch keinen Zugriff auf das Anlagennetzwerk bekommen und auch nur auf bestimmte Geräte Zugriff haben. Zudem soll eine gesicherte Verbindung von der Anlage zu einer abgesetzten Station über mobile Netze (z. B. UMTS oder LTE) aufgebaut werden.

Lösung
Ausgangspunkte für die Verbindung des Systemintegrators sind die VPN Clients (hier CP 1243-7 LTE, SCALANCE M874-3) mit dem Endpunkt: SCALANCE SC646-2C als VPN Server in der Automatisierungsanlage.

Vorteile auf einen Blick

- Gesicherte Fernzugriffe über Internet oder mobile Netze wie UMTS oder LTE durch Sicherung der Datenübertragung mit VPN (IPsec)
- Einschränkung der Zugriffsmöglichkeiten mit integrierter Firewall-Funktion
- Gesicherter Fernzugriff auf Anlagenteile ohne direkten Zugang zum Anlagennetzwerk mit Firewall SCALANCE SC646-2C

Aufgabenstellung
Der Zugriff des Systemintegrators auf seine Maschine soll für einzelne Endgeräte und Dienste personen- und rollenabhängig freigegeben werden.

Lösung
Benutzerspezifische Firewall-Regeln können mit personalisierten Benutzerdaten temporär für die Dauer des Serviceeinsatzes an den Industrial Security Appliances SCALANCE S aktiviert werden.

Vorteile auf einen Blick

- Verringertes Security-Risiko bei Service und Wartung
- Kontrollierter und protokollierter Gerätezugriff
- Personen- und protokollabhängige Zugriffskontrolle auf Endsysteme einer Netzwerkzelle

Security Kommunikationsprozessoren für Basic Controller, Advanced Controller und Distributed Controller

Security Kommunikationsprozessoren schützen Steuerungen mit integrierter Firewall und VPN vor Datenmanipulation und Spionage.

Für SIMATIC Basic Controller
CP 1243-1, CP 1243-7 LTE und CP 1243-8 IRC
Die Kommunikationsprozessoren CP 1243-1 und CP 1243-7 LTE verbinden die Steuerung SIMATIC S7-1200 mit Ethernet-Netzwerken (CP 1243-1) bzw. Mobilfunknetzen (CP 1243-7 LTE). Der Kommunikationsprozessor CP 1243-8 IRC verbindet die Steuerung über die Fernwirkprotokolle SINAUT ST7, DNP3 und IEC 60870-5-104 mit einer Telecontrol Leitstelle. Mit den integrierten Sicherheitsfunktionen Firewall und VPN schützen die Kommunikationsprozessoren S7-1200-Stationen und unterlagerte Netzwerke vor unberechtigten Zugriffen, sowie die Datenübertragung durch Verschlüsselung gegen Manipulation und Spionage.

Vorteile auf einen Blick

Ein spezieller Vorteil der Security Kommunikationsprozessoren für SIMATIC Controller ist die automatische Erstellung von Firewall-Regeln bei der Projektierung mit dem TIA Portal.
Konfigurierte Kommunikationsverbindungen werden automatisch in der Firewall freigeschaltet, so dass der Konfigurationsaufwand und auch die Fehleranfälligkeit deutlich reduziert werden.

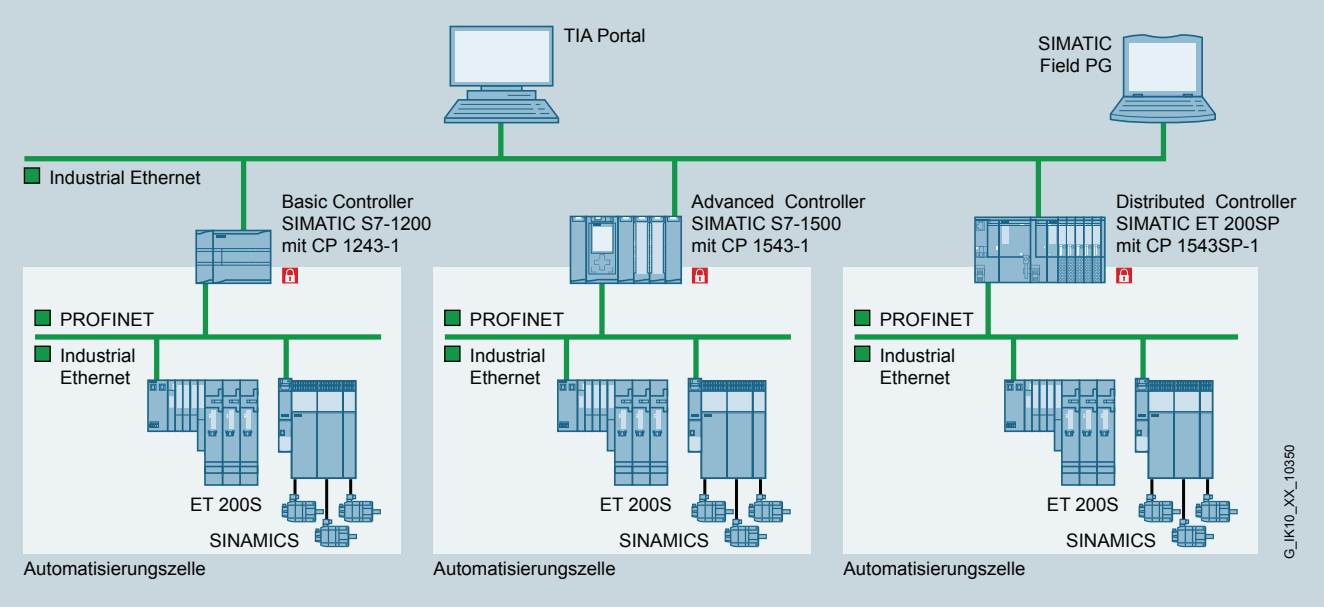
Für SIMATIC Advanced Controller Controller
CP 1543-1
Der Kommunikationsprozessor CP 1543-1 verbindet die Steuerung SIMATIC S7-1500 sicher mit Ethernet-Netzwerken. Mit den integrierten Sicherheitsfunktonen Firewall, VPN und Protokollen zur Datenverschlüsselung wie FTPS und SNMPv3 schützt der Kommunikationsprozessor S7-1500-Stationen und unterlagerte Netzwerke vor unberechtigten Zugriffen, sowie die Datenübertragung durch Verschlüsselung gegen Manipulation und Spionage. Zudem verfügt der CP über verschlüsselte E-Mail-Kommunikation über SMTPS (Port 587 und 25) und secure Open Communication über TCP/IP.

CP 1545-1
Der CP 1545-1 mit CloudConnect-Funktionalität ermöglicht einen einfachen und zuverlässigen Transfer aller Daten von SIMATIC S7-1500 zur MindSphere oder zu einer Cloud-Lösung, die das standardisierte Protokoll MQTT unterstützt, z. B. Microsoft Azure oder IBM Cloud. Durch die integrierte SPI-Firewall schützt der CP 1545-1 die SIMATIC S7-1500-Station dabei vor unberechtigten Zugriffen. Auch die Einbindung in eine IPv6-Infrastruktur ist möglich: Parallel zur Anbindung an Cloud-Anwendungen unterstützt der CP 1545-1 den Anschluss an weitere Automatisierungsgeräte, z. B. HMIs, über Industrial Ethernet mittels SIMATIC S7-Protokoll.

Für SIMATIC Distributed Controller
CP 1543SP-1
Mit dem Kommunikationsprozessor CP 1543SP-1 lässt sich der Distributed Controller ET 200SP flexibel um eine Industrial Ethernet Schnittstelle erweitern. Das ermöglicht den Aufbau identischer Maschinen mit gleichen IP-Adressen durch Netzwerktrennung. Er bietet zusätzlich erweiterte Security-Funktionen, wie die Verschlüsselung aller übertragenen Daten mittels VPN mit IPsec oder die Stateful Inspection Firewall für den sicheren Zugriff auf den Distributed Controller ET 200SP.

Anwendungsbeispiel

Netzwerksegmentierung mit Security Kommunikationsprozessoren



Segmentierung von Netzwerken und Schutz der Steuerungen SIMATIC S7-1200 mit CP 1243-1, der S7-1500 mit CP 1543-1 bzw. dem Distributed Controller ET 200SP mit CP 1543SP-1

Aufgabenstellung

Die Kommunikation zwischen Automatisierungsnetzwerk und unterlagerten Netzwerken an SIMATIC Controllern soll per Zugriffskontrolle gesichert werden.

Lösung

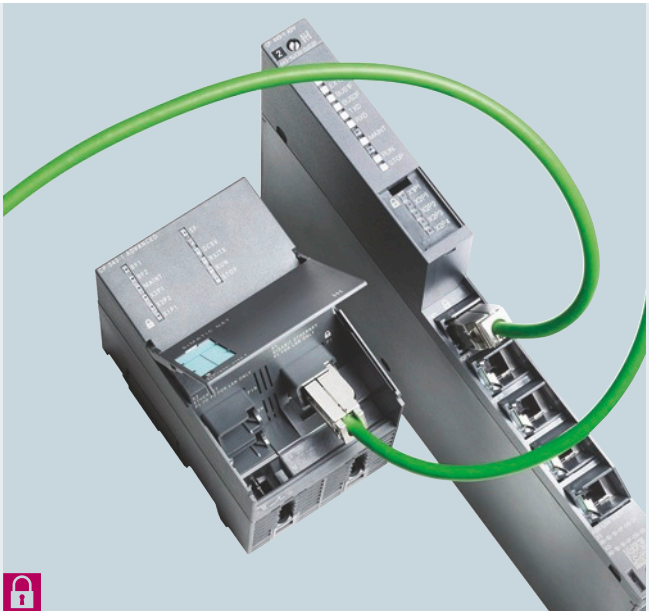
Die Kommunikationsprozessoren werden im Rack der jeweiligen Zielsysteme SIMATIC S7-1200, S7-1500, Distributed Controller ET 200SP vor den zu schützenden Automatisierungszellen platziert. Dadurch wird die Kommunikation von und zur SIMATIC CPU und unterlagerter Automatisierungszelle mithilfe von Firewall-Regeln auf die erlaubten Verbindungen eingeschränkt und bei Bedarf durch Aufbau von VPN-Tunneln gegen Manipulation oder Spionage geschützt.

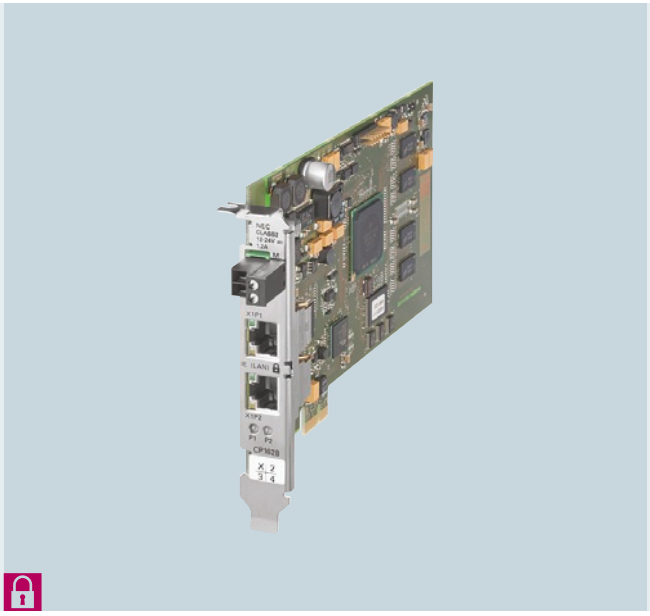
Vorteile auf einen Blick

- Gesicherter Anschluss der SIMATIC S7-1200, S7-1500 und Distributed Controller ET 200SP an Industrial Ethernet mittels integrierter Stateful Inspection Firewall und VPN
- Zusätzliche gesicherte Kommunikationsmöglichkeiten: File-Transfer und E-Mail
- Einsatz in einer IPv6-basierten Infrastruktur [1)]

[1)] gilt für CP 1543-1, CP 1543SP-1

Security Kommunikationsprozessoren für SIMATIC S7-300, S7-400 und PG/PC





CP 343-1 Advanced und CP 443-1 Advanced
Die Industrial Ethernet Kommunikationsprozessoren CP 343-1 Advanced und CP 443-1 Advanced für SIMATIC S7-300 bzw. S7-400 beinhalten neben den bekannten Kommunikationsfunktionen, einem integrierten Switch und Layer 3 Routing-Funktionalität, auch Security Integrated, d.h. eine Stateful Inspection Firewall und ein VPN Gateway zum Schutz der Steuerung und unterlagerten Geräte gegen Sicherheitsrisiken.

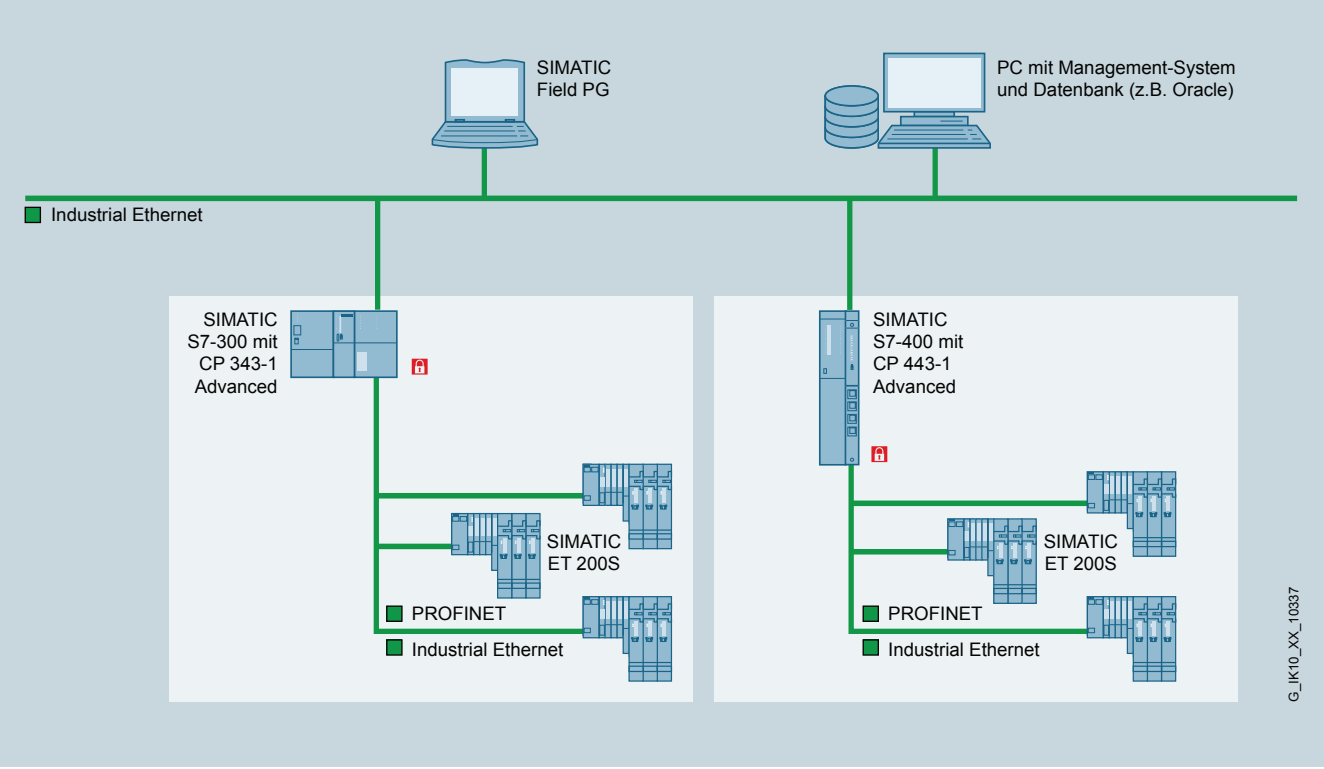
CP 1628
Über den Industrial Ethernet Kommunikationsprozessor CP 1628 werden Industrie-PCs durch Firewall und VPN geschützt – für eine gesicherte Kommunikation ohne Spezialeinstellungen des Betriebssystems. Auf diesem Wege lassen sich mit der Baugruppe ausgestattete Rechner mit geschützten Zellen verbinden. Der CP 1628 ermöglicht den Anschluss an Industrial Ethernet (10/100/1000 Mbit/s) für SIMATIC PG/PC und PCs mit PCI Express- Steckplatz. Weitere Feldgeräte sind über den integrierten Switch flexibel an Industrial Ethernet anschließbar. Der Kommunikationsprozessor beinhaltet neben Automatisierungsfunktionen auch Security Integrated, d.h. eine Stateful Inspection Firewall und ein VPN Gateway zum Schutz des PG/PC-Systems gegen Sicherheitsrisiken.

Vorteile auf einen Blick

Ein spezieller Vorteil der Security Kommunikationsprozessoren für SIMATIC Controller ist die automatische Erstellung von Firewall-Regeln bei der Projektierung mit dem TIA Portal.
Konfigurierte Kommunikationsverbindungen werden automatisch in der Firewall freigeschaltet, so dass der Konfigurationsaufwand und auch die Fehleranfälligkeit deutlich reduziert werden.

Anwendungsbeispiel

Netzwerksegmentierung mit Security Kommunikationsprozessoren



Segmentierung von Netzwerken und Schutz der Steuerungen SIMATIC S7-300 bzw. S7-400 mit CP 343-1 Advanced bzw. CP 443-1 Advanced

Aufgabenstellung
Die Kommunikation zwischen dem Verwaltungssystem auf Office-Ebene und unterlagerten Netzwerken der Automatisierungsebene soll per Zugriffskontrolle gesichert werden.

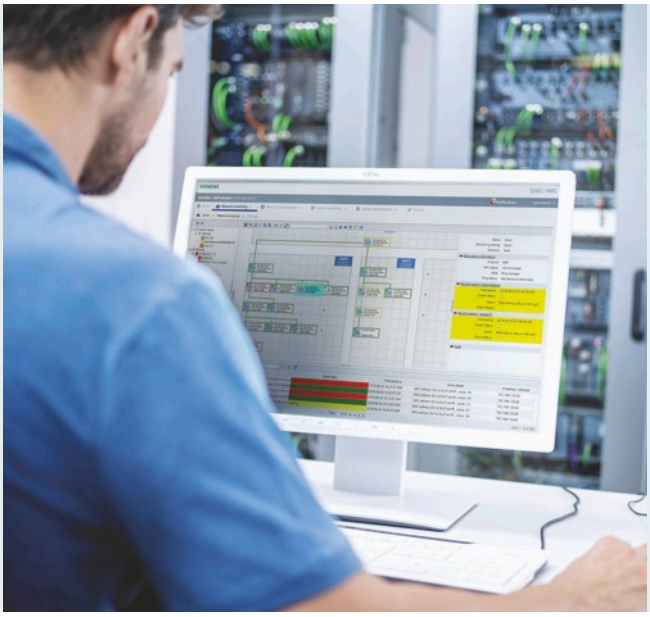
Lösung
CP 343-1 Advanced und CP 443-1 Advanced werden vor den zu schützenden Automatisierungszellen platziert. Dadurch wird die Kommunikation mithilfe von Firewall-Regeln auf die erlaubten Verbindungen eingeschränkt.

Vorteile auf einen Blick

- Firewall, VPN Gateway und CP in einem Gerät: die Advanced CPs bieten die integrierten Security Funktionen Firewall und VPN zur Realisierung einer geschützten Automatisierungszelle und Schutz der Datenübertragung.
- Durchgängigkeit bei der sicheren Kommunikation: Projektierung der CPs erfolgt einfach mit STEP 7 / TIA Portal; VPN-Tunnel können zwischen CPs untereinander oder zur Industrial Security Appliance SCALANCE S, der PC-Baugruppe CP 1628 und den Internet- und Mobilfunk-Routern SCALANCE M aufgebaut werden.

Alle Anwender von CP 343-1 Advanced und CP 443-1 Advanced erhalten Security Integrated und benötigen zur Projektierung der Sicherheit industrieller Anlagen keine separate Hardware oder spezielle Tools, außerhalb der SIMATIC S7.

Software für sichere Netzwerke



SINEMA Remote Connect
Die Managementplattform für Remote Networks erleichtert den Fernzugriff auf weitverteilte Maschinen und Anlagen. SINEMA Remote Connect sorgt dabei für die gesicherte Verwaltung von Tunnelverbindungen (VPN) zwischen der Zentrale, den Servicetechnikern und den installierten Anlagen. Ein direkter Zugriff auf das Firmennetzwerk, in dem die Anlage oder Maschine eingebunden ist, wird zunächst unterbunden. Der Servicetechniker und die zu wartende Maschine stellen getrennt voneinander eine Verbindung zum SINEMA Remote Connect Server her. Dort wird die Identität der Teilnehmer über Zertifikatsaustausch ermittelt, bevor der Zugriff auf die Maschine erfolgt.

Die Verbindung zum SINEMA Remote Connect kann über diverse Medien, wie Mobilfunk, DSL oder bestehende, private Netzwerkinfrastrukturen aufgebaut werden.

Mit dem Industrie-Router SCALANCE M804PB ist auch eine komfortable und kostengünstige direkte Anbindung bestehender Anlagen mit PROFIBUS/ MPI an SINEMA Remote Connect für einen gesicherten Fernzugriff möglich.

Netzwerk-Management-System SINEC NMS
Mit dem leistungsstarken und zukunftssicheren Netzwerk-Management-System (NMS) lassen sich branchenübergreifend Netzwerke bis zu mehreren Zehntausend Teilnehmern zentral, rund um die Uhr überwachen, verwalten und konfigurieren.

Das NMS ermöglicht dabei auch effizientes Security Management gemäß Richtlinie IEC 62443. So lassen sich z. B. der Zugang zum System und der Funktionsumfang aller Berechtigten über die Benutzerrollenverwaltung genau steuern.

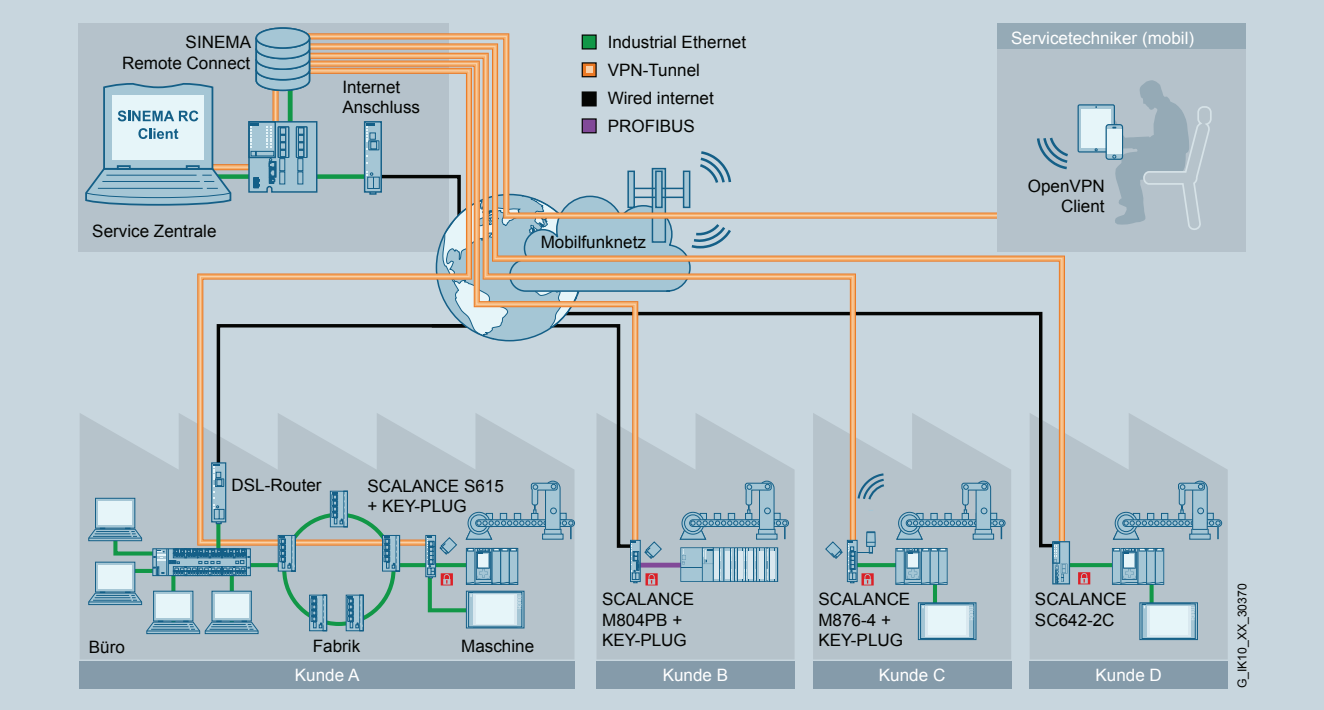
Systemsicherheit bietet das System u.a. durch verschlüsselte Datenkommunikation (über Zertifikate und Passwort) zwischen der zentralen SINEC NMS Control-Instanz und den im Netzwerk verteilten SINEC NMS Operations. Auch die Datenkommunikation zwischen SINEC NMS und den Infrastrukturkomponenten im Netzwerk kann verschlüsselt (SNMP V3) realisiert werden.

Außerdem bietet SINEC NMS eine lokale Dokumentationsfunktion über Audit Trails. So können Audit-Log-Einträge nachvollzogen werden, indem über einen Zeitstempel automatisch dokumentiert wird, welcher Benutzer wann welche Aktivitäten im System tätigt. Das ist auch für offizielle Prüfungen eine deutliche Zeit- und Aufwandsersparnis.

Zudem können Informationen über Syslog an eine zentrale Stelle weitergegeben werden, z. B. Audit-Logs, System-Ereignisse oder Netzwerk-Alarme. Darüber hinaus bietet SINEC NMS ein zentrales Firewall- und NAT-Management. Firewall-Komponenten (SCALANCE SC600/S615 und RUGGEDCOM RX1400/1500) können zentral konfiguriert werden. Die Erstellung der Firewall-Regeln erfolgt dabei über eine grafische Beschreibung der erlaubten Kommunikationsbeziehung im Netzwerk. Das System generiert daraufhin automatisch die gerätespezifischen Regeln. Es kann auch nur die NAT-Management-Funktion unabhängig von Firewall-Management oder umgekehrt genutzt werden.

Anwendungsbeispiel

Gesicherter Zugriff auf Anlagenteile mit SINEMA Remote Connect



Konfigurationsbeispiel SINEMA Remote Connect – Gesamtübersicht

Aufgabenstellung

Für Serienmaschinen und größere Anlagen mit identischen Subnetzen soll ein Fernzugriff für die Fernwartung ermöglicht werden. Besonders der Fernzugriff auf Sondermaschinen und sensible Bereiche erfordert eine zentrale Verwaltung der Verbindungen, die zur Erfassung der Zustands- und Wartungsdaten notwendig sind. Zusätzlich sollen die entsprechenden Router mit Routing / NAT Informationen einfach und komfortabel angelegt werden können.

Lösung

Die zentrale Verwaltung der Verbindungen zwischen Maschinen und Servicetechnikern erfolgt über die Managementplattform für Remote Networks - SINEMA Remote Connect.
SINEMA Remote Connect verwaltet sowohl die Nutzerrechte als auch die Zugriffsberechtigungen und sorgt dafür, dass nur befugtes Personal auf entfernte Maschinen zugreifen darf.

Typische Einsatzgebiete

- Anlagen- und Maschinenbau
- Energieverteilung / Unterstationen (Stadtwerke)
- Logistik / Hafenlogistik
- ITS / Verkehrsbetriebe
- Wasser / Abwasser (Stadtwerke, ...)

Vorteile auf einen Blick

- Hohe Transparenz und Sicherheit
- Lokales und zentrales Logging sämtlicher Aktivitäten
- zentrale Benutzerverwaltung
- Gesicherter und einfacher Zugriff auf Anlagenteile von jedem Punkt der Welt aus
- Optimale Anbindung von Maschinen auch mit identischen IP-Adressen in lokalen Subnetzwerken (NAT)
- Komfortable Verwaltung verschiedener Nutzer (Servicetechniker) durch Gruppenverwaltung , inkl. benutzerspezifischer Zugriffsrechte - auch auf eindeutige IP-Adressen im Subnetz (Dedicated Device Access)
- Schneller und müheloser Verbindungsaufbau dank Adressbuchfunktion
- Einfache Integration in Industrieanlagen
- Kein spezielles IT Know-how erforderlich dank einfachem Nutzerinterface mit Autokonfiguration für Endgeräte und SINEMA RC Client
- Sichere und komfortable Multifaktor-Authentifizierung mit Benutzername / Passwort und PKI Smartcard
- Betrieb in virtualisierter Umgebung möglich

Technische Daten

Industrial Security Appliances SCALANCE S

	Industrial Firewall Appliances		Industrial VPN Appliances		
Produkttyp-Bezeichnung	SCALANCE SC632-2C	SCALANCE SC636-2C	SCALANCE S615	SCALANCE SC642-2C	SCALANCE SC646-2C
Artikelnummer	6GK5632-2GS00-2AC2	6GK5636-2GS00-2AC2	6GK5615-0AA00-2AA2	6GK5642-2GS00-2AC2	6GK5646-2GS00-2AC2
Übertragungsrate					
Übertragungsrate	10/100/1000 Mbit/s	10/100/1000 Mbit/s	10/100 Mbit/s	10/100/1000 Mbit/s	10/100/1000 Mbit/s
Schnittstellen					
Elektrischer Anschluss	2x RJ45-Port	6x RJ45-Port	5x RJ45-Port	2x RJ45-Port	6x RJ45-Port
Optischer Anschluss	2x Combo-Port mit SFP	2x Combo-Port mit SFP	–	2x Combo-Port mit SFP	2x Combo-Port mit SFP
für Meldekontakt	1x 2-poliger Klemmenblock	1x 2-poliger Klemmenblock	–	1x 2-poliger Klemmenblock	1x 2-poliger Klemmenblock
für Spannungs-versorgung	1x 4-poliger Klemmenblock	1x 4-poliger Klemmenblock	1x 5-poliger Klemmenblock	1x 4-poliger Klemmenblock	1x 4-poliger Klemmenblock
Wechselmediums C-PLUG	Ja	Ja	Ja	Ja	Ja
Versorgungsspannung, Stromaufnahme, Verlustleistung					
Versorgungsspannung extern	DC 24 V	DC 24 V	DC 24 V	DC 24 V	DC 24 V
Bereich	DC 9,6 V ... 31,2 V	DC 9,6 V ... 31,2 V	DC 10,8 ... 28,2 V	DC 9,6 V ... 31,2 V	DC 9,6 V ... 31,2 V
Zulässige Umgebungsbedingungen					
Umgebungstemperatur während Betrieb [°C]	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C
Schutzart	IP20	IP20	IP20	IP20	IP20
Bauform					
Baugruppenformat	kompakt	kompakt	kompakt	kompakt	kompakt
Produktfunktion Security					
Ausführung Firewall	stateful inspection	stateful inspection	stateful inspection	stateful inspection	stateful inspection
Bridge-Firewall	Ja	Ja	Nein	Ja	Ja
Benutzerspezifische Firewall	Ja	Ja	Ja	Ja	Ja
Passwortschutz	Ja	Ja	Ja	Ja	Ja
Produktfunktion bei VPN-Verbindung	OpenVPN (als Client zu SINEMA RC)	OpenVPN (als Client zu SINEMA RC)	IPsec, OpenVPN (als Client zu SINEMA RC)	IPsec, OpenVPN (als Client zu SINEMA RC)	IPsec, OpenVPN (als Client zu SINEMA RC)
IPsec VPN Daten-durchsatz	–	–	35 Mbit/s	120 Mbit/s	120 Mbit/s
Anzahl der möglichen Verbindungen bei VPN-Verbindung	0	0	20	200	200
Firewall Datendurchsatz	600 Mbit/s	600 Mbit/s	100 Mbit/s	600 Mbit/s	600 Mbit/s
NAT/NAPT	Ja	Ja	Ja	Ja	Ja
VRRPv3-Kopplung	6	6	2	6	6
MRP-Client / HRP-Client	Nein	Ja	Nein	Nein	Ja

Industrie-Router SCALANCE M

Produkttyp-Bezeichnung	SCALANCE M drahlos	
	M874-2, M874-3	M876-3, M876-4
Artikelnummer	6GK5874-2AA00-2AA2 6GK5874-3AA00-2AA2	6GK5876-3AA02-2BA2 6GK5876-4AA00-2BA2
Übertragungsrate		
an der Schnittstelle 1/2	10/100 Mbit/s	
GPRS-Übertragung Up-/Downlink, max.	85,6 kbit/s	85,6 kbit/s
EDGE-Übertragung Up-/Downlink, max.	237 kbit/s	237 kbit/s
HSPA+-Übertragung Up-/Downlink, max.	5,76 Mbit/s	14,4 Mbit/s
EV-DO-Übertragung Forward Link / Reverse Link	–	3,1 Mbit/ /1,8 Mbit/s (nur M876-3)
LTE-Übertragung Up-/Downlink, max.	–	50 Mbit/s/100 Mbit/s (nur M876-4)
ADSL2+-Übertragung Up-/Downlink, max.	–	–
SHDSL-Übertragung, max.	–	–
Schnittstellen		
Anzahl der elektrischen Anschlüsse		
- für internes Netzwerk	2	4
- für externes Netzwerk	1	2
- für Spannungsversorgung	2	2
Elektrischer Anschluss		
- für inernes Netzwerk	RJ45-Port (10/100 Mbit/s, TP, Auto-Crossover)	RJ45-Port (10/100 Mbit/s, TP, Auto-Crossover)
- für externes Netzwerk	SMA-Antennenbuchsen (50 Ohm)	SMA-Antennenbuchsen (50 Ohm)
- für Spannungsversorgung	Klemmleiste	Klemmleiste
Versorgungsspannung, Stromaufnahme, Verlustleistung		
Versorgungsspannung / Bereich	10,8 V ... 28,8 V	10,8 V ... 28,8 V
Zulässige Umgebungsbedingungen		
Umgebungstemperatur während Betrieb [°C]	-20 °C ... +60 °C	-20 °C ... +60 °C
Schutzart	IP20	IP20
Bauform		
Baugruppenformat	kompakt	kompakt
Produktfunktion Security		
Ausführung Firewall	stateful inspection	stateful inspection
Bridge-Firewall	Nein	Nein
Benutzerspezifische Firewall	Ja	Ja
Passwortschutz	Ja	Ja
Packet Filter	Ja	Ja
Produktfunktion bei VPN-Verbindung	IPsec, OpenVPN (als Client)	IPsec, OpenVPN (als Client)
Anzahl der möglichen Verbindungen bei VPN-Verbindung	20	20
Schlüssellänge		
1 | 2 | 3 bei IPsec AES bei VPN	128 bit | 192 bit | 256 bit	128 bit | 192 bit | 256 bit
bei IPsec 3DES / bei Virtual Privat Network	168 bit	168 bit
VRRPv3-Kopplung	2	2
MRP-Client / HRP-Client	Nein	Nein

Industrie-Router SCALANCE M

Produkttyp-Bezeichnung	SCALANCE M drahtgebunden			
	M812-1/M816-1		M826-2	M804PB
Artikelnummer	6GK5812-1BA00-2AA2 6GK5816-1BA00-2AA2		6GK5826-2AB00-2AB2	6GK5804-0AP00-2AA2
Übertragungsrate				
an der Schnittstelle 1/2	10/100 Mbit/s		10/100 Mbit/s	10/100 Mbit/s
GPRS-Übertragung Up-/Downlink, max.	–		–	–
EDGE-Übertragung Up-/Downlink, max.	–		–	–
HSPA+-Übertragung Up-/Downlink, max.	–		–	–
EV-DO-Übertragung Forward Link / Reverse Link	–		–	–
LTE-Übertragung Up-/Downlink, max.	–		–	–
ADSL2+-Übertragung Up-/Downlink, max.	1,4 Mbit/s / 25 Mbit/s		–	–
SHDSL-Übertragung, max.	–		15,3 Mbit/s	–
Schnittstellen				
Anzahl der elektrischen Anschlüsse				
- für internes Netzwerk	1	4	4	2
- für externes Netzwerk	1	1	2	1
- für Spannungsversorgung	2	2	2	2
Elektrischer Anschluss				
- für inernes Netzwerk	RJ45-Port (10/100 Mbit/s, TP, Auto-Crossover)			RJ45-Port (10/100 Mbit/s, TP, Auto-Crossover), SUB-D
- für externes Netzwerk	RJ45-DSL-Port	–	Klemmleiste	RJ45-Port (10/100 Mbit/s, TP, Auto-Crossover)
- für Spannungsversorgung		–	–	Klemmleiste
Versorgungsspannung, Stromaufnahme, Verlustleistung				
Versorgungsspannung / Bereich	10,8 V ... 28,8 V		10,8 V ... 28,8 V	10,8 V ... 28,8 V
Zulässige Umgebungsbedingungen				
Umgebungstemperatur während Betrieb [°C]	0 °C ... +60 °C		-40 °C ... +70 °C	-20 °C ... +60 °C
Schutzart	IP20		IP20	IP20
Bauform				
Baugruppenformat	kompakt		kompakt	kompakt
Produktfunktion Security				
Ausführung Firewall	stateful inspection		stateful inspection	stateful inspection
Bridge-Firewall	Nein		Nein	Nein
Benutzerspezifische Firewall	Ja		Ja	Ja
Passwortschutz	Ja		Ja	Ja
Packet Filter	Ja		Ja	Ja
Produktfunktion bei VPN-Verbindung	IPsec, OpenVPN (als Client)		IPsec, OpenVPN (als Client)	IPsec, OpenVPN (als Client)
Anzahl der möglichen Verbindungen bei VPN-Verbindung	20		20	20
Schlüssellänge				
1 | 2 | 3 bei IPsec AES bei VPN	128 bit | 192 bit | 256 bit		128 bit | 192 bit | 256 bit	128 bit | 192 bit | 256 bit
bei IPsec 3DES / bei Virtual Privat Network	168 bit		168 bit	168 bit
VRRPv3-Kopplung	2		2	2
MRP-Client / HRP-Client	Nein		Nein	Nein

Kommunikationsprozessoren
CP 1243-1, CP 1243-7 LTE, CP1243-8 IRC, CP 1543-1, CP 1543SP-1 und CP 1545-1

Produkttyp-Bezeichnung	CP 1243-1	CP 1243-7 LTE	CP 1243-8 IRC	CP 1543-1	CP 1543SP-1	CP 1545-1
Artikelnummer	**6GK7243-1BX30-0XE0**	**6GK7243-7KX30-0XE0**	**6GK7243-8RX30-0XE0**	**6GK7543-1AX00-0XE0**	**6GK7543-6WX00-0XE0**	**6GK7545-1GX00-0XE0**
Übertragungsrate						
an der Schnittstelle 1	10/100 Mbit/s	Mobilfunk 4G/3G/2G	10/100 Mbit/s	10/100/1000 Mbit/s	10/100 Mbit/s	10/100/1000 Mbit/s
Schnittstellen						
an Schnittstelle 1 gem. IE	1x RJ45-Port	Antennenanschluss SMA-Buchse	1x RJ45-Port	1x RJ45-Port	über ET 200SP BusAdapter	1x RJ45-Port
für Spannungsversorgung	–	1	1	–	–	–
Wechselmediums C-PLUG	–	–	–	–	–	–
Versorgungsspannung						
1 aus Rückwandbus	DC 5 V	–	DC 5 V	DC 15 V	–	DC 15 V
extern	–	DC 24 V	DC 24 V	–	DC 24 V	–
Zulässige Umgebungsbedingungen während Betrieb						
- bei senkrechter Installation	-20 °C ... +60 °C	-20 °C ... +60 °C	-20 °C ... +60 °C	0 °C ... +40 °C	0 °C ... +50 °C	0 °C ... +40 °C
- bei waagerechter Installation	-20 °C ... +70 °C	-20 °C ... +70 °C	-20 °C ... +70 °C	0 °C ... +60 °C	0 °C ... +60 °C	0 °C ... +60 °C
Schutzart	IP20	IP20	IP20	IP20	IP20	IP20
Bauform						
Baugruppenformat	Kompaktbau-gruppe S7-1200 einfach breit	Kompaktbau-gruppe S7-1200 einfach breit	Kompaktbau-gruppe S7-1200 einfach breit	Kompaktbau-gruppe S7-1500 einfach breit	Kompaktbau-gruppe für ET 200SP	Kompaktbau-gruppe S7-1500 einfach breit
Produktfunktion Security						
Ausführung Firewall	stateful inspection	stateful inspection	stateful inspection	stateful inspection	stateful inspection	stateful inspection
Produktfunktion bei VPN-Verbindung	IPsec	IPSec	IPSec, SINEMA RC	IPsec	IPsec, SINEMA RC	–
Anzahl der möglichen Verbindungen bei VPN-Verbindung	8	1	8	16	4	–
Produktfunktion						
ACL – IP-based	Nein	Nein	Nein	Nein	Nein	Nein
ACL – IP-based für PLC/Routing	Nein	Nein	Nein	Nein	Nein	Nein
Sperren der Kommunikation über physikalische Ports	Nein	Nein	Nein	Nein	Ja	Nein
Logfile für unberechtigten Zugriff	Nein	Nein	Nein	Ja	Ja	Ja

Kommunikationsprozessoren
CP 343-1 Advanced, CP 443-1 Advanced und CP 1628

Produkttyp-Bezeichnung	CP 343-1 Advanced	CP 443-1 Advanced	CP 1628
Artikelnummer	**6GK7343-1GX31-0XE0**	**6GK7443-1GX30-0XE0**	**6GK1162-8AA00**
Übertragungsrate			
an der Schnittstelle 1 / 2	10/1000 Mbit/s / 10/100 Mbit/s	10/1000 Mbit/s / 10/100 Mbit/s	10/1000 Mbit/s / –
Schnittstellen			
Elektrischer Anschluss			
an Schnittstelle 1 gem. IE	1x RJ45-Port	1x RJ45-Port	2x RJ45-Port
an Schnittstelle 2 gem. IE	2x RJ45-Ports	4x RJ45-Ports	–
des Rückwandbusses	–	–	PCI Express x1
für Spannungsversorgung	2-polige steckbare Klemmleiste	–	1x 2-poliger Klemmenblock
Wechselmediums C-PLUG	ja	ja	–
Versorgungsspannung, Stromaufnahme, Verlustleistung			
Art der Spannung der Versorgungsspannung	–	–	DC
Versorgungsspannung			
1 aus Rückwandbus	DC 5 V	DC 5 V	DC 3,3 V
2 aus Rückwandbus	–	–	DC 12 V
extern	DC 24 V	–	DC 24 V
Bereich	–	–	DC 10,5 V ... 32 V
Zulässige Umgebungsbedingungen			
während Betrieb		0 °C ... +60 °C	+5 °C ... +55 °C
- bei senkrechter Installation	0 °C ... +40 °C	–	–
- bei waagerechter Installation	0 °C ... +60 °C	–	–
Schutzart	IP20	IP20	–
Bauform			
Baugruppenformat	Kompaktbaugruppe	Kompaktbaugr. S7-400 einfach breit	PCI Express x1 (halbe Länge)
Produktfunktion Security			
Ausführung Firewall	stateful inspection	stateful inspection	stateful inspection
Bridge-Firewall	Nein	Nein	Nein
Benutzerspezifische Firewall	Ja	Ja	Ja
Produktfunktion bei VPN-Verbindung	IPsec	IPsec	IPsec
Anzahl der möglichen Verbindungen bei VPN-Verbindung	32	32	64
Produktfunktion			
Passwortschutz für Web-Applikationen	Ja	Ja	Nein
ACL – IP-based	Ja	Ja	Nein
ACL – IP-based für PLC/Routing	Ja	Ja	Nein
Abschaltung nicht benötigter Dienste	Ja	Ja	Nein
Sperren der Kommunikation über physikalische Ports	Ja	Ja	Nein
Logfile für unberechtigten Zugriff	Nein	Nein	Nein
MRP-Client	Ja	Ja	Nein

SINEMA Remote Connect

Produkttyp-Bezeichnung	SINEC NMS 50, 100, 250, 500	SINEMA Remote Connect	SINEMA RC Client
Artikelnummer	**6GK8781-1BA01-0AA0, 6GK8781-1DA01-0AA0, 6GK8781-1JA01-0AA0, 6GK8781-1TA01-0AA0**	**6GK1720-1AH01-0BV0**	**6GK1721-1XG01-0AA0**
Ausführung Firewall	–	–	–
Produktfunktion bei VPN-Verbindung	–	IPsec/OpenVPN	OpenVPN
Anzahl der möglichen VPN-Verbindungen	–	unbegrenzt bzw. abhängig vom Zielsystem, Netzwerk	1:1 Beziehung zum SINEMA Remote Connect Server
Betriebssystem	Desktop: Windows 10 (64 Bit, Professional, Enterprise) ab Version 1809 Server: Windows Server 2016 (64 Bit), Windows Server 2019 (64 Bit) Virtualisierung: ESXi V6.7	SINEMA RC Virtual Appliance enthält eigenes Betriebssystem	Windows 7 Ultimate, Enterprise, Professional SP1 (32 und 64 Bit), Windows 8.1 Pro (64 Bit)
Webbrowser	Internet Explorer V11.0, Firefox V65.0 oder höher, Google Chrome V72.0 oder höher	–	–
System Integrity Check	Ja	–	–

Industrial Security

IE RJ45 Port Lock

IE RJ45 Port Lock

Physischer Netzwerkzugangsschutz durch IE RJ45 Port Lock
Zu einem ausgewogenen und ganzheitlichen Security-Konzept gehören auch physische Schutzmaßnahmen. Ein bekanntes Problem sind offene, nicht verwendete RJ45 Schnittstellen, die von Unbefugten dazu verwendet werden können, sich Zugang zum Netzwerk zu verschaffen. Um dieses Risiko zu reduzieren, wurde der IE RJ45 Port Lock entwickelt. Der RJ45 Port Lock ermöglicht ein mechanisches Abschließen von RJ45 Ports an Endgeräten beziehungsweise Netzwerkkomponenten. Durch die robuste Bauform des Port Locks in Form eines Steckers wird die RJ45 Schnittstelle komplett belegt. Somit kann das Einstecken von RJ45 Leitungen verhindert werden und ein ungewünschter Gebrauch von unbelegten RJ45 Port auch an nicht konfigurierbaren Netzwerkkomponenten vermieden werden. Durch das integrierte Schloss, das nur mit einem mechanischen Schlüssel entriegelt werden kann, wird die Rast-Nase des RJ45 Port Lock blockiert. Weitere Vorteile des Port Locks sind die robuste, industrietaugliche Aufbautechnik und die einfache Installation ohne Zusatzwerkzeug aufgrund des RJ45 kompatiblen Designs.

SIMATIC RF1000 Zugangskontroll-Reader

SIMATIC RF1000 für die Zugriffskontrolle für Maschinen und Anlagen

SIMATIC RF1000 Zugangskontroll-Reader
Der steigende Bedarf nach Sicherheit und Nachvollziehbarkeit erfordert zunehmend Lösungen, die den Zugriff auf Maschinen und Anlagen reglementieren und dokumentieren.
Mit SIMATIC RF1000 bietet Siemens eine RFID-basierte Lösung, mit welcher elektronische Zugriffsverwaltung einfach und flexibel implementiert werden kann. Als Basis für die Identifikation werden die bereits vorhandenen Mitarbeiterausweise genutzt. Das erhöht die Bedienerfreundlichkeit und reduziert Kosten. Mit den Readern der Serie SIMATIC RF1000 können fein abgestufte Zugriffskonzepte realisiert, Vorgänge dokumentiert oder benutzerspezifische Hinweise und Anweisungen hinterlegt werden – entsprechend der kundenspezifischen Anwendung. Und alles mit einer Karte. Die Zugangskontroll-Reader mit ihrer kompakten Bauform, geringen Einbautiefe und hohen Schutzart (IP65 Frontseite) sowie einem Temperaturbereich von -25 bis +55 °C ermöglichen den Einsatz direkt an Maschinen und Anlagen im rauen industriellen Umfeld.

Highlights:
- Einsatz im HF-Bereich (13,56 MHz) sowie LF-Bereich (125 kHz) (nur SIMATIC RF1040R)
- Diagnose über 3-Farben-LED Statusanzeige
- Verhinderung von Fehlbedienungen durch abgesicherten und dokumentierten Zugriff auf Maschinen
- Einfache Integration in vorhandene Hardware (HMI Geräte, IPCs und Panels)
- ATEX II Zulassung (nur für SIMATIC RF1060R und RF1070R)
- Lesen und Schreiben von Daten auf Ausweis/Karte
- Erstellung von kundenspezifischen Parametrierungen des Readers über die Config-Karte
- Handhabung und Speicherung von kundenspezifischem Schlüsselmaterial im Reader für den Datenzugriff

Security mit SCALANCE X und SCALANCE W

SCALANCE X-200 Produktlinie

SCALANCE W-Produktfamilie

SCALANCE X

Die managed Switches der SCALANCE X-Produktfamilie sind für den Aufbau von Linien-, Stern- und Ringstrukturen geeignet.

SCALANCE X-200, X-300, X-400 und X-500 können den Netzwerkzugang kontrollieren und verfügen unter anderem über die folgenden Security-Funktionen:

- Management ACL (Access Control List)
- IEEE 802.1X (RADIUS)
- 802.1Q-VLAN – ermöglicht die logische Trennung des Datenverkehrs zwischen vordefinierten Ports auf den Switches
- Broadcast/Multicast/Unicast Limiter
- Broadcast Blocking

Zudem werden folgende gesicherte Protokolle unterstützt:

- SSH
- HTTPS
- SNMP v3

SCALANCE W

Zuverlässige drahtlose Kommunikationslösung auf den unterschiedlichsten Automatisierungsebenen gemäß WLAN-Standard IEEE 802.11 – die IWLAN-Produkte SCALANCE W ermöglichen skalierbare Anwendungen.

Access Points und Client Modules SCALANCE W verfügen unter anderem über die folgenden Security-Funktionen:

- Management ACL (Access Control List)
- IEEE802.1X (RADIUS)
- Zugangsschutz nach IEEE 802.11i
- WPA2(RADIUS)/WPA2-PSK mit AES

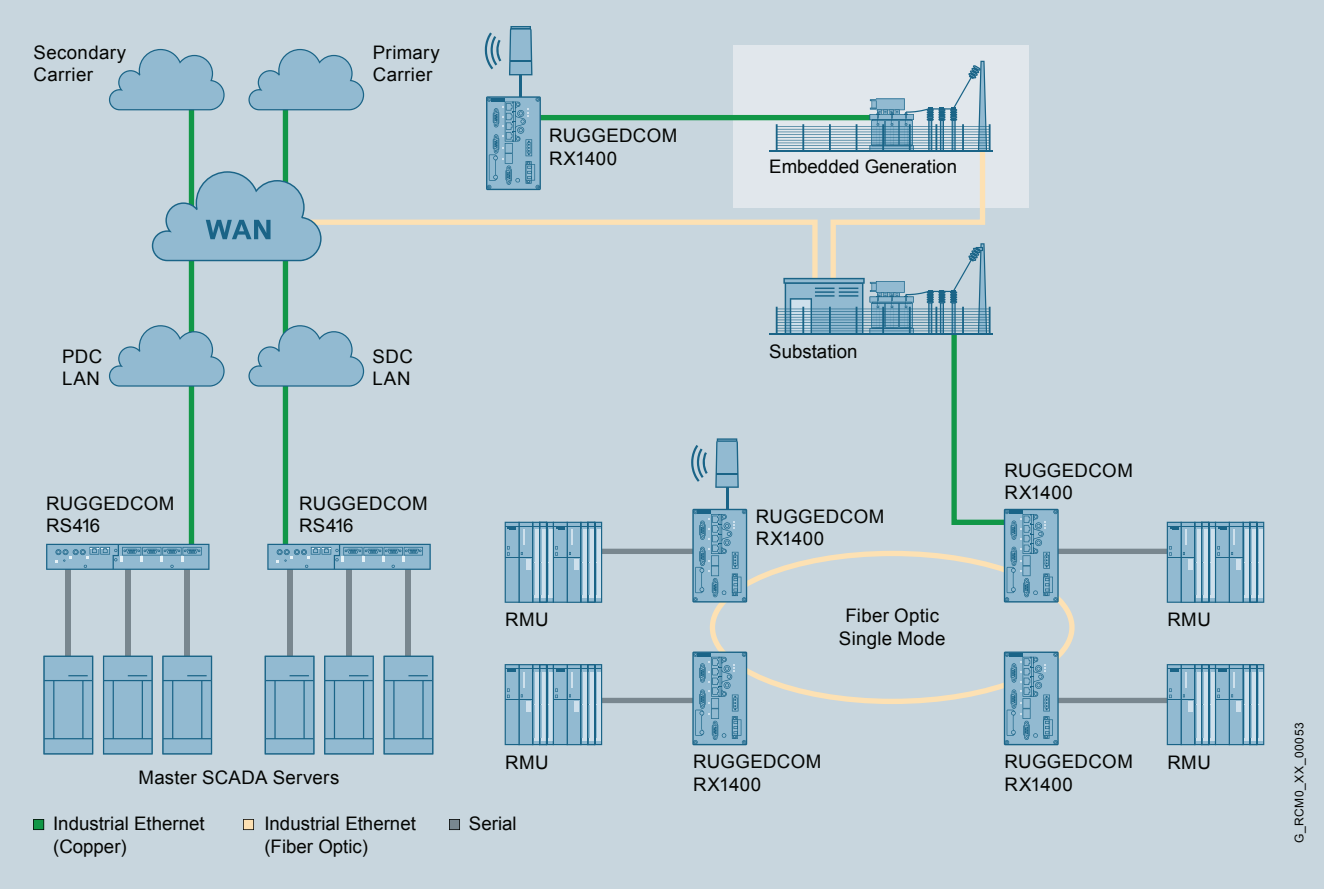
Zudem werden folgende gesicherte Protokolle unterstützt:

- SSH
- HTTPS
- SNMP v3

Inter AP-Blocking

erhöht die Sicherheit in einer Netzwerkumgebung mit mehreren Access Points SCALANCE W. WLAN Clients, die über unterschiedliche Access Points über ein Layer 2-Netz (Switches) angebunden sind, können direkt miteinander kommunizieren. Abhängig von der Applikation könnte dies ein Sicherheitsrisiko darstellen. Über „Inter AP-Blocking“ werden definierte Kommunikationspartnern oder Gateways, mit denen die WLAN Clients ausschließlich kommunizieren dürfen, vorgegeben und damit das Sicherheitsrisiko minimiert. Eine Kommunikation mit anderen sich im Netzwerk befindenden Teilnehmern wird mittels KEY-PLUG W700 Security (6GK5907-0PA00) unterbunden. Er ist mit allen Access Points SCALANCE W mit KEY-PLUG-Steckplatz verwendbar. SCALANCE W-1700-Geräte beinhalten die Funktion ohne KEY-PLUG.

Security mit RUGGEDCOM

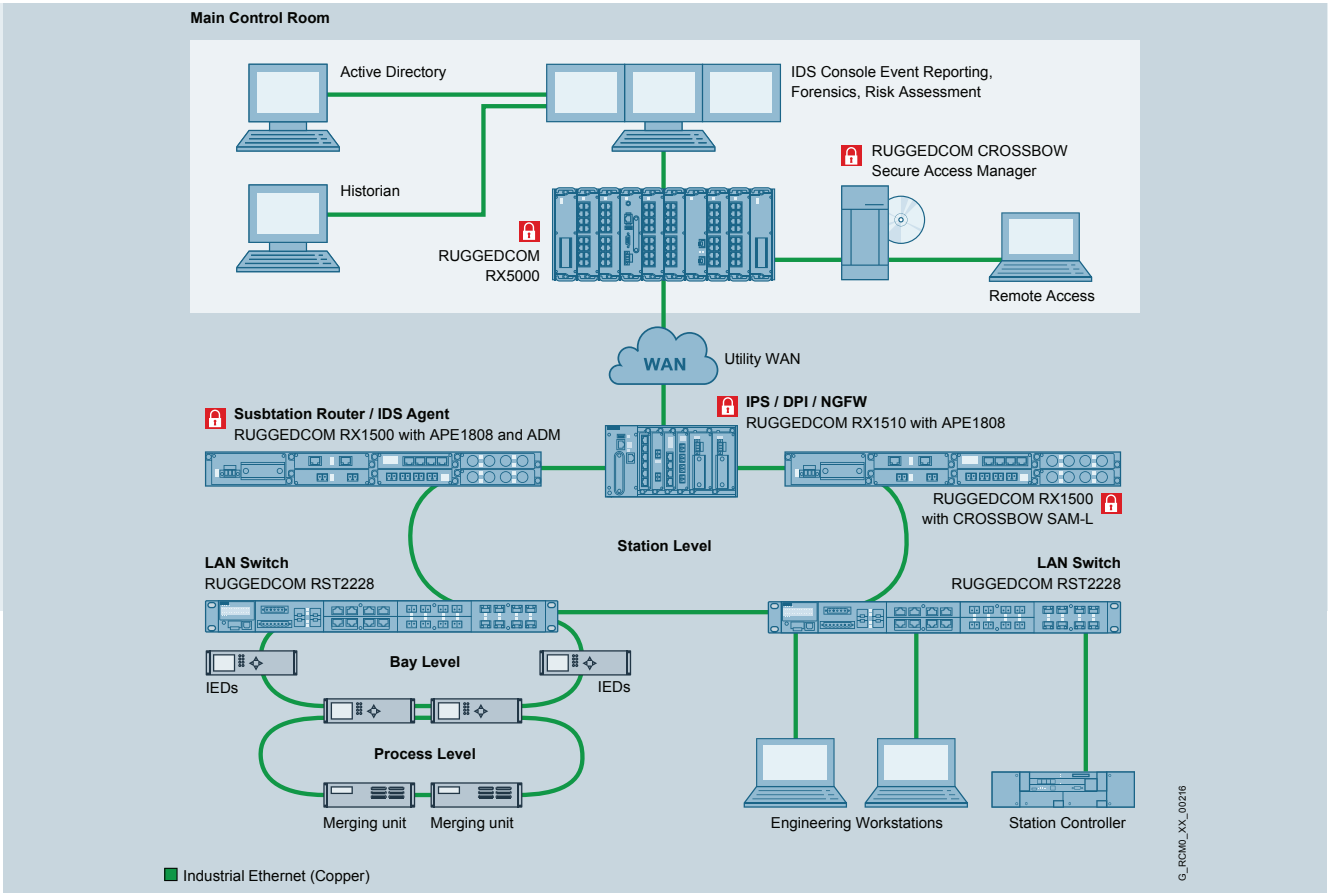


Der RUGGEDCOM RX1400 eignet sich für die zuverlässige Verbindung von Niederspannungs-Umspannwerken und verteilten Stromerzeugungsanlagen über öffentliche Mobilfunknetze.

RUGGEDCOM RX1400 und RM1224

Security ist auch ein wichtiges Thema im Energie-Umfeld. Hier spielen Automatisierungs- und Kommunikationsnetzwerke eine Schlüsselrolle für aufgabenkritische Anwendungen, und hohe Zuverlässigkeit ist von überragender Bedeutung. Mit den folgenden Merkmalen begegnet der RUGGEDCOM RX1400 und RM1224 den Sicherheitsbedrohungen auf der Netzwerkebene:

- VPN (IPsec) – Die integrierte Hardwareverschlüsselungs-Engine ermöglicht hoch leistungsfähigen IPsec-Datenverkehr ohne Verwendung des Hauptprozessors
- Passwörter – erfüllen die NERC-Richtlinien einschließlich der Möglichkeit RADIUS-basierter Authentifizierung
- SSH / SSL – erweiterter Passwortschutz mit der Möglichkeit, Passwörter und Daten bei der Übertragung innerhalb des Netzwerks zu verschlüsseln
- Freigabe/Sperrung von Ports – Möglichkeit der Sperrung von Ports, so dass unbefugte Geräte keine Verbindung zu unbelegten Ports aufbauen können
- 802.1Q-VLAN – ermöglicht die logische Trennung des Datenverkehrs zwischen vordefinierten Ports auf den Switches
- SNMPv3 – verschlüsselte Authentifizierung und Zugriffsschutz
- HTTPS – für gesicherten Zugriff auf die Webschnittstelle
- 802.1X – stellt sicher, dass nur zulässige Feldgeräte sich mit dem Gerät verbinden können
- MAC-Access List – Zugriffskontrolle für Geräte die RADIUS nicht unterstützen



RUGGEDCOM RX1500 mit CROSSBOW und APE1808 - Applikationsbeispiel

RUGGEDCOM RX1500 mit CROSSBOW und APE1808
Das Schaubild illustriert die typische Systemarchitektur eines Versorgers. Der CROSSBOW Secure Access Manager (SAM) ist der zentrale Unternehmensserver, über den alle Fernzugriffsverbindungen hergestellt werden und stellt aus der Sicht der Intelligent Electronic Devices (IED) die einzige vertrauenswürdige Datenquelle für Clients dar. Der SAM ist über ein gesichertes WAN mit Gateway-Geräten an dem Umspannwerk, wie RUGGEDCOM RX1500 oder einem anderen unterstützten Gerät, verbunden.

Mit RUGGEDCOM APE können herstellerunabhängige Software-Anwendungen in rauen und geschäftskritischen Umgebungen ausgeführt und betrieben werden. Ohne zusätzlichen Aufwand für die Installation eines externen Industrie-PCs zu verursachen, kann sie mit der entsprechenden Software für verschiedene Anwendungen genutzt werden, in denen die Daten direkt an der Quelle analysiert werden. Darunter fällt zum Beispiel die Anwendung als Firewall, Netzwerkanalysesoftware oder Intrusion Detection System. Als eigenständiges Modul kann die RUGGEDCOM APE1808 direkt in jedes Gerät der RUGGEDCOM RX1500 Multi-Service Plattform eingesteckt werden und so die eingebauten Switching- und Routingmöglichkeiten der Plattform vollständig nutzen. Dank ihrer Basis, dem Intel Quad Core sowie der x86_64 Architektur mit Support für Linux und Windows 10, bietet die RUGGEDCOM APE1808 eine normenbasierte Plattform für handelsübliche Software und ermöglicht damit Partnerschaften mit Branchenführern in Sachen Erkennung und Vermeidung von Internetbedrohungen.

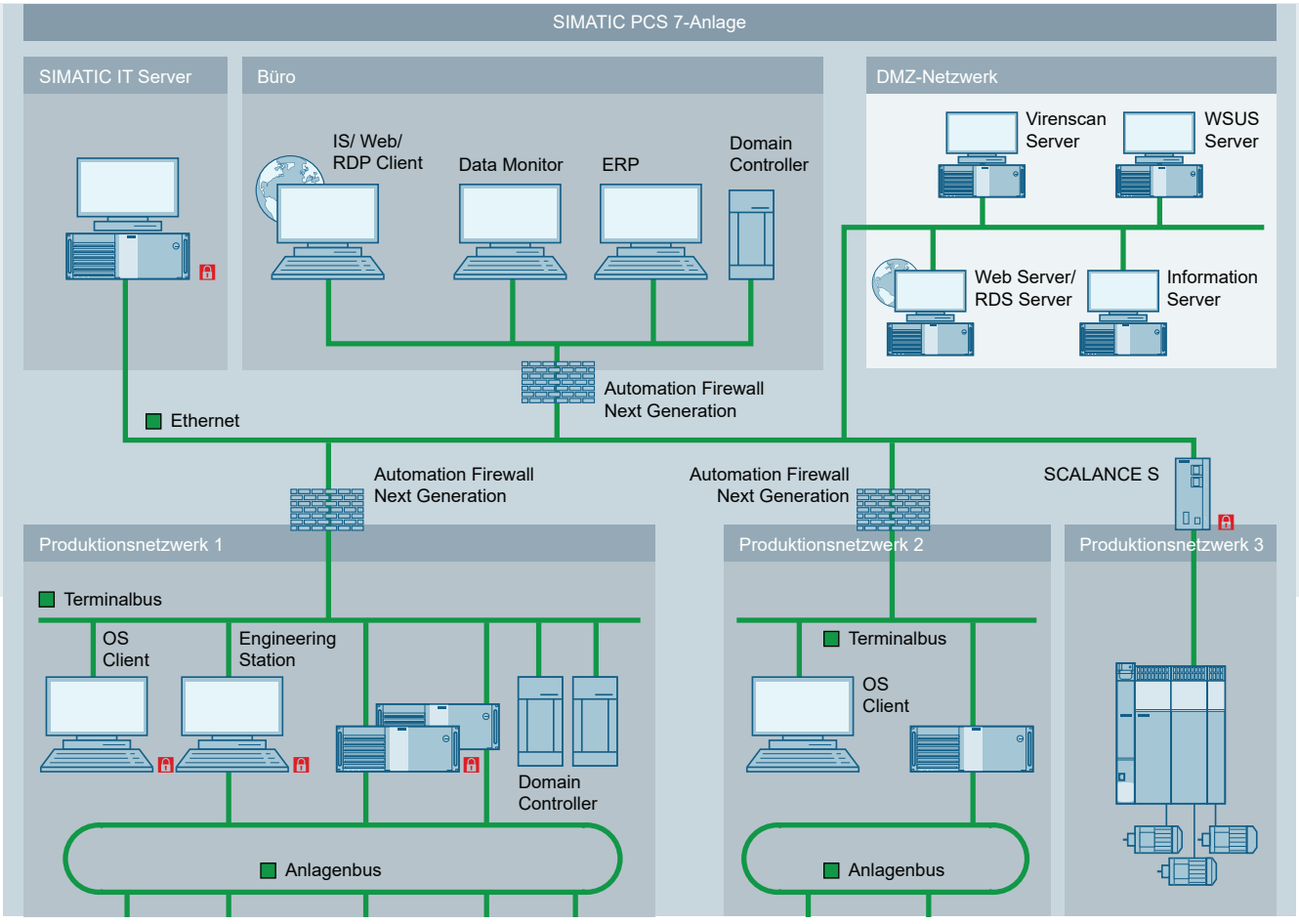
SIMATIC PCS neo Security und SIMATIC PCS 7 Security

SIMATIC PCS neo Security
Das vollständig webbasierte Prozessleitsystem SIMATIC PCS neo setzt ebenfalls auf die bewährte Defense in Depth-Strategie. Das Thema Security steht auch bei SIMATIC PCS neo an oberster Stelle. Dies zeigt sich durch die TÜV-Zertifizierung des Prozesses des Produktlebenszyklus basierend auf der IEC 62443-4-1 und der Zertifizierung gemäß IEC 62443-3-3. Die Produktentwicklung ist konform mit den aktuellen IACS Security Standards. Security ist ein „built-in"-Element von SIMATIC PCS neo. Das bedeutet, dass von Beginn an der umfassende Schutz gewährleistet wird. Nicht benötigte Funktionen können bei Bedarf abgeschaltet werden, um die Anlagen den individuellen Anforderungen entsprechend anzupassen.

Der Zugriffsschutz von SIMATIC PCS neo ist breit gefächert. Alle Funktionen und Eingriffe benötigen selbstverständlich eine entsprechende Authentifizierung und Autorisierung. Bei besonders kritischen Funktionen ist darüber hinaus eine 2-Faktor-Authentifizierung erforderlich, um höchstmögliche Sicherheit zu gewährleisten. Zusätzlich ist eine zentrale Benutzerverwaltung vom System vorgegeben.

SIMATIC PCS 7 Security
Oberste Priorität bei SIMATIC PCS 7 hat die unbedingte Aufrechterhaltung der Kontrolle über Produktion und Prozesse durch das Bedienpersonal, auch bei auftretenden Security-Bedrohungen. Die Verhinderung beziehungsweise Einschränkung der Verbreitung einer aufgetretenen Security-Bedrohung für Anlagen und Netzwerke soll unter Aufrechterhaltung der kompletten Bedien- und Beobachtbarkeit von Produktion und Prozess erfolgen. Das Sicherheitskonzept für SIMATIC PCS 7 hat die Aufgabe, sicherzustellen, dass nur authentifizierte Benutzer über die ihnen zugewiesenen Bedienmöglichkeiten an authentifizierten Geräten autorisierte Bedienungen durchführen können. Diese Bedienungen dürfen ausschließlich über eindeutige und geplante Zugriffswege erfolgen, um während eines Auftrages eine sichere Produktion oder Koordination ohne Gefahren für Mensch, Umwelt, Produkt, zu koordinierende Güter und das Geschäft des Unternehmens zu gewährleisten. Das SIMATIC PCS 7 Security-Konzept beschreibt eine Defense in Depth-Strategie, basierend auf dem internationalen Standard IEC 62443. Die Umsetzung dieser Strategie in einer Anlage wird detailliert im „PCS 7 Kompendium Teil F - Industrial Security" beschrieben. SIMATIC PCS 7 ist auf Basis dieser empfohlenen Anlagenkonfiguration gemäß IEC 62443-3-3 zertifiziert (TÜV Süd).

SIMATIC PCS 7 Security



SIMATIC PCS 7 Security – Sicherheitsarchitektur durch Defense in Depth

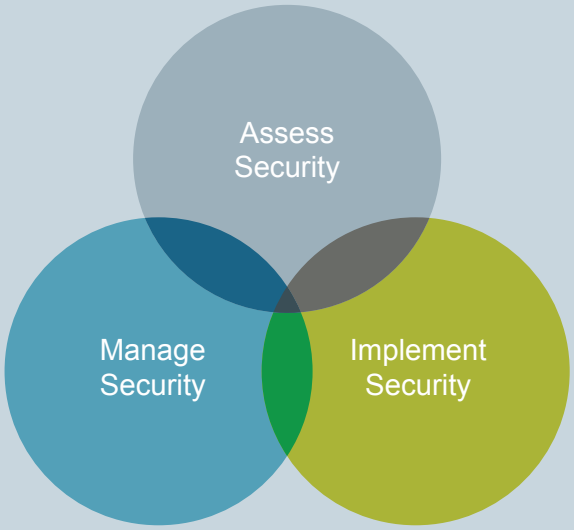
Es werden mehrere Schutzebenen geschaffen, um Risiken zu minimieren und die Sicherheit der Anlagen zu erhöhen.

Elemente des SIMATIC PCS 7 Security-Konzeptes

- Physischer Zugangsschutz
- Zellensegmentierung durch Firewalls
- Systemhärtung
- Patch Management
- Benutzerverwaltung (SIMATIC Logon)
- Malware-Erkennung und -Vermeidung
- Schulungen und Prozesse

- Zugangsschutz: Durch Werkschutz gesicherte Anlagen und Zugangskontrollen auch mittels Typo Zugangsberechtigungen
- Firewalls: Segmentierung von Netzwerken, Bildung von Perimeter-Netzwerken (DMZ), Einschränkung und Protokollierung der Netzwerk-Kommunikation
- VPN: Nutzung für verschlüsselte Kommunikation zwischen Netzwerken (z. B. Remote-Zugriff)
- Whitelisting: Festlegung, welche Programme zur Ausführung auf Ihrem System ausschließlich zugelassen sind
- Patch Management: Die Anlage wird durch eine Update-Strategie aktuell gehalten (z. B. durch Betriebssystem-, Software- und Firmware-Updates). Somit wird das Risiko eines Angriffs auf bekannte Sicherheitslücken minimiert.
- Benutzerverwaltung: Einsatz einer zentralen Benutzerverwaltung, um Zugriffsrechte, Gruppenzugehörigkeiten, Rollen und Richtlinien von Anlagenbenutzern eindeutig zu definieren. Dabei wird das Prinzip der für die jeweilige Aufgabe maximal benötigten Rechte umgesetzt.
- Virenscanner: Nutzung eines aktuellen Virenscanners, um das Risiko von Beschädigungen und negativen Beeinflussungen der Systeme und des Anlagenbetriebs zu minimieren.
- Regelmäßige Schulungen aller Personen, um so alle definierten Prozesse einzuhalten und die Sicherheit der Anlage zu gewährleisten.

Industrial Security Services



Die zunehmende Vernetzung von Produktion und Office hat viele Prozesse einfacher und schneller gemacht. Die einheitliche Verwendung der gleichen Daten und Informationen schafft Synergien. Durch diese Entwicklung steigen allerdings auch die Risiken.

Viren, internes Fehlverhalten oder Hackerangriffe bedrohen heute nicht mehr nur die Verwaltungsebene, sondern auch für Produktionsstätten besteht die Gefahr von Störungen, Beeinflussung der Integrität und Know-how-Verlust.
Viele Security-Schwachstellen sind nicht auf den ersten Blick zu erkennen. Deshalb ist es sinnvoll, eine bestehende Automatisierungsumgebung bezüglich Security zu überprüfen und zu optimieren, um die Verfügbarkeit auf einem hohen Level zu halten.

Mit dem Industrial Security Services Portfolio steht ein umfassendes Produktspektrum zur Verfügung, um eine Strategie entsprechend dem Defense in Depth-Konzeptes zu entwickeln, zu implementieren und aufrechtzuerhalten. Das skalierbare Angebot enthält umfassende Beratung (Assess Security), die technischen Implementierungen (Implement Security) und kontinuierlichen Service (Manage Security).

Assess Security für einen risikobasierten Security Fahrplan

Assess Security beinhaltet die umfassende Analyse von Bedrohungen, die Identifizierung der Risiken und die konkrete Empfehlung von Security-Maßnahmen.

- Ihr Vorteil: Ein anlagenspezifischer und risikobasierter Security-Fahrplan für ein durchgängig optimales Security Niveau.

Implement Security für Maßnahmen zur Risikominderung

Implement Security bedeutet die Umsetzung von Schutzmaßnahmen, um das Security Niveau von Anlagen und Produktionsstätten zu erhöhen.

- Ihr Vorteil: Vermeidung von Sicherheitslücken und besserer Schutz vor Cyberbedrohungen dank technischer und organisatorischer Maßnahmen.

Manage Security für einen umfassenden, kontinuierlichen Schutz

Manage Security heißt kontinuierliche Überwachung, regelmäßige Anpassung und Aktualisierung der implementierten Maßnahmen durch unsere Security Tools.

- Ihr Vorteil: Sie erhalten größtmögliche Transparenz über den Sicherheitsstatus Ihrer Anlagen und vermeiden potenzielle Bedrohungsfälle proaktiv dank unserer Security Tools, die speziell für Ihre industrielle Umgebung ausgelegt sind.

Automation Firewall Next Generation

Um Produktionsausfälle und Stillstandzeiten zu vermeiden, muss der Datenverkehr zwischen Netzwerken geprüft, analysiert und selektiv freigegeben werden, ohne die Funktion des Prozessleitsystems zu beeinträchtigen. Nur so lässt sich die Anlage ohne Nachteile für die Produktivität optimal schützen. Firewalls mit ergänzenden Services sind dafür prädestiniert. Mit der Automation Firewall Next Generation bietet Siemens eine getestete und validierte Standard-Firewall in drei Leistungsklassen (220, 820, 850) an. Sie ist auf den Einsatz mit SIMATIC PCS 7 und WinCC abgestimmt.

Die Automation Firewall Next Generation kooperiert ausgezeichnet mit den Kommunikationsprodukten von SIMATIC NET. Sie zeichnet sich durch umfassende Hardware- und Softwarefunktionen für SIMATIC PCS 7- und WinCC-Projekte aus, z. B.:

- Application Layer und Stateful Inspection Firewall
- Klassifizierung aller Anwendungen, auf allen Ports, jederzeit
- Durchsetzung von Sicherheitsrichtlinien für jeden Benutzer und jeden Standort
- Hohe Verfügbarkeit (aktiv/aktiv und aktiv/passiv)
- Redundanter Stromversorgungseingang für erhöhte Zuverlässigkeit (PA-220 und PA-850)
- Gehärtetes Betriebssystem (PanOS ist Linux-basiert)
- Möglichkeit zur Überprüfung des Layer-7-Datenverkehrs wie z. B. des S7-Protokolls (Erkennung von Start, Stopp, Lesen, Schreiben) oder von OPC
- Secure System Architecture

Vorteile auf einen Blick

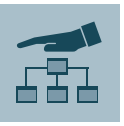
- Geprüft und freigegeben für SIMATIC PCS 7
- Schutz vor bekannten und unbekannten Bedrohungen
- Sehr gutes Preis-Leistungs-Verhältnis
- Erstklassige Firewall-Lösung für die Segmentierung von IT/OT-Netzwerken auf Basis des „Zones & Conduits"-Modells der IEC 62443
- Zeitersparnis, da viele Anwendungsprotokolle standardmäßig integriert sind

Service durch Siemens

- Überprüfung des Anlagennetzwerks
- Entwicklung eines Perimeter-Firewall-Konzeptes
- Installation und Konfiguration einer Perimeter-Firewall in Automatisierungssystemen
- Dokumentierung der Firewall-Konfiguration

Support durch Palo Alto Networks (3 oder 5 Jahre)

- Premium-Support rund um die Uhr verfügbar (24/7)
- Ersatzteilversand und Hardware-Austausch am folgenden Werktag
- Feature-Releases und Software-Updates, Updates für Subscriptions
- Dokumentation und FAQs, Online-Portal für Kundensupport



Begriffe, Definitionen

Cybersecurity
Cybersecurity, auch bekannt als Computer Security oder IT Security, bezeichnet den Schutz der Hardware, Software, Information und angebotener Services von computerbasierten Systemen vor Diebstahl, Sabotage und Missbrauch.

Demilitarisierte Zone (DMZ)
DMZ, auch ent- oder demilitarisierte Zone, bezeichnet ein Computernetzwerk mit sicherheitstechnisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netzwerke (z. B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste (z. B. E-Mail) gestattet und gleichzeitig das interne Netzwerk (LAN) vor unberechtigten Zugriffen geschützt werden. Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnerverbundes sowohl dem WAN (Internet) als auch dem LAN (Intranet) zur Verfügung zu stellen. Ihre Schutzwirkung entfaltet eine DMZ durch die Isolation eines Systems gegenüber zwei oder mehreren Netzwerken.

Firewall
Security-Komponenten, die den Datenaustausch zwischen miteinander verbundenen Netzwerken entsprechend gegebener Sicherheitsbeschränkungen ermöglichen oder ausschließen. Hierzu werden Firewall-Regeln projektiert. Somit kann fest-gelegt werden, dass z. B. nur ein bestimmter PC auf eine bestimmte Steuerung zugreifen darf.

Industrial Security
Industrial Security umfasst den Schutz von Informationen, Daten und geistigem Eigentum („Intellectual Property") während der Verarbeitung, Übertragung und Speicherung im industriellen Umfeld. Verfügbarkeit, Integrität und Vertraulichkeit sollen gesichert werden. Das dient zur Abwehr von möglichen Angriffen, Bedrohungen, Gefahren, wirtschaftlichen Schäden und zur Risikominimierung. Orientierung bieten diverse nationale bzw. international gültige Normen, z. B. IEC62443, ISO/IEC_27000, ISO/IEC_15408 sowie die jeweils gültigen Landesgesetze, z. B. in Deutschland das BDGs (Bundesdatenschutz-Gesetz).

Port Security
Mithilfe der Access Control-Funktion lassen sich einzelne Ports für unbekannte Teilnehmer sperren. Ist die Funktion Access Control auf einem Port aktiviert, werden Pakete, die von unbekannten MAC-Adressen kommen, sofort verworfen. Lediglich Pakete von bekannten Teilnehmern werden angenommen.

RADIUS (IEEE 802.1X):
Authentifizierung über einen externen Server
Das Konzept von RADIUS basiert auf einem zentralen Authentifizierungs-Server. Für ein Endgerät ist der Zugang zum Netzwerk oder auf eine Netzwerk-Ressource erst möglich, nachdem die Anmeldedaten des Geräts beim Authentifizierungs-Server verifiziert wurden. Sowohl das Endgerät als auch der Authentifizierungs-Server müssen das EAP-Protokoll (Extensive Authentication Protocol) unterstützen.

Systemhärtung
Bei der Systemhärtung deaktiviert man nicht benötigte Schnittstellen und Ports und reduziert so die Anfälligkeit des Netzwerks gegenüber Angriffen von außen und von innen. Dabei werden alle Ebenen eines Automatisierungssystems betrachtet: Leitsystem, Netzwerkkomponenten, PC-basierte Systeme und speicherprogrammierbare Steuerungen.

Virtual Private Network (VPN)
Ein sogenannter VPN-Tunnel verbindet zwei oder mehrere Netzwerkteilnehmer (z. B. Security-Komponenten) und die dahinter liegenden Netzwerksegmente. Durch die Verschlüsselung der Daten innerhalb dieses Tunnels wird sichergestellt, dass die Daten bei der Übertragung über ein an sich unsicheres Netzwerk (z. B. Internet) durch Dritte nicht abgehört und verfälscht werden können.

Virtual LAN (VLAN)
VLANs (IEEE 802.1Q) ermöglichen die logische Trennung des Datenverkehrs zwischen vordefinierten Ports auf den Switches. Auf dem physikalisch nur einmal vorhandenen Netzwerk entstehen damit mehrere „virtuelle" Netzwerke. Datenaustausch findet nur innerhalb eines VLAN statt.

Whitelisting
Ob Personen, Unternehmen oder Programme: Eine Whitelist – 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.

Erfahren Sie alles über Industrial Security:

- Unsere Security-Produkte und Leistungen im Überblick
- Aktuelle Neuigkeiten aus dem Umfeld von Industrial Security
  www.siemens.de/industrial-security
- **www.siemens.de/netzwerksicherheit**
- **www.siemens.de/scalance-s**

Folgen Sie uns auf:

twitter.com/siemensindustry

youtube.com/siemens

Weitere Informationen

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Deutschland

Artikel-Nr. 6ZB5530-1AP01-0BA9
Dispo 26000
BR 1119 1. WÜ 36 De
Printed in Germany

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können.
Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Erzeugnisbezeichnungen können Marken oder Erzeugnisnamen der Siemens AG oder anderer Unternehmen sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyberbedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z. B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter **https://www.siemens.com/industrialsecurity.**

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyberbedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter **https://www.siemens.com/industrialsecurity.**

siemens.de/netzwerksicherheit