

# Industrial Security

Schutz einer Automatisierungszelle durch Firewall.



# simatic net

# CONFIGURATION 5

**SIEMENS**

# Industrial Security

## Schutz einer Automatisierungszelle durch Firewall

Moderne Automatisierungstechnik baut auf Kommunikation und zunehmende Vernetzung einzelner Fertigungsinseln. Dabei wird die Integration aller Fertigungskomponenten mit durchgängiger Vernetzung zum Office-Netzwerk bzw. dem Firmen-Intranet immer wichtiger. Die industrielle Kommunikation arbeitet zunehmend mit der IT-Welt zusammen und ist den gleichen Gefährdungen ausgesetzt, die aus dem Office- und IT-Umfeld bekannt sind.

Die Configuration 5 ist für folgende Aufgabenstellung geeignet:

Eine Automatisierungszelle soll mit dem Firmennetz so verbunden werden, dass über eine "Zutrittskontrolle" nur be-

stimmte Partner/ Netzknoten bzw. Kommunikationsdienste Zugriff auf die internen Teilnehmer dieser Zelle haben. Dabei sollen folgende Anwenderszenarien nur für einen Partner freigeschaltet werden.

- Projektieren/ Diagnostizieren mit STEP 7
- Visualisieren mit WinCC flexible
- Zugriff auf zelleninterne Web- und FTP-Server

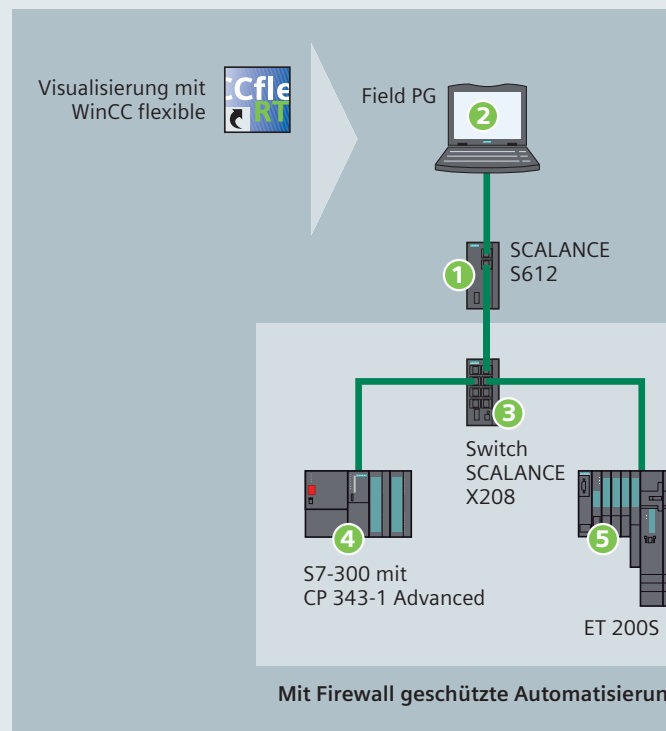
Die Zugriffssteuerung soll einfach und kostengünstig erfolgen und auch vom Automatisierungspersonal erstellt und gepflegt werden können.

## Schnell startklar. SIMATIC NET Configurations

SIMATIC NET bietet alle Komponenten für den Aufbau durchgängiger Netzwerklösungen auf Basis offener, internationaler Standards. Für anspruchsvolle industrielle Anwendung macht SIMATIC NET die Vorteile von Ethernet nutzbar und sorgt für einfache Integration der Feldbussysteme.

SIMATIC NET Configurations repräsentieren Komponenten, die sich systemgetestet für typische Aufgabenstellungen der industriellen Kommunikation empfehlen. Für umfassendere Lösungen können jederzeit weitere Komponenten aus dem breiten und vielfältigen SIMATIC NET-Programm hinzugefügt werden.

*In dieser Configuration wird gezeigt, wie das SCALANCE Security Module als Firewall konfiguriert und so zum Schutz von Automatisierungszellen/ -komponenten eingesetzt werden können. Auf einfache Weise kann so erreicht werden, dass auf die Einzelgeräte innerhalb der Automatisierungszelle nur von bestimmten PGs/ PCs aus zugegriffen werden kann. Zusätzlich ist ein Zugriff nur für explizit erlaubte Kommunikationsdienste mit bestimmten Port-Nummern erlaubt.*



### Hinweis:

Die Stromversorgung (DC 24 V) der SIMATIC-Station wird im Testaufbau auch zur Versorgung des Switches, des Security Modules und der ET 200S PNIO verwendet.

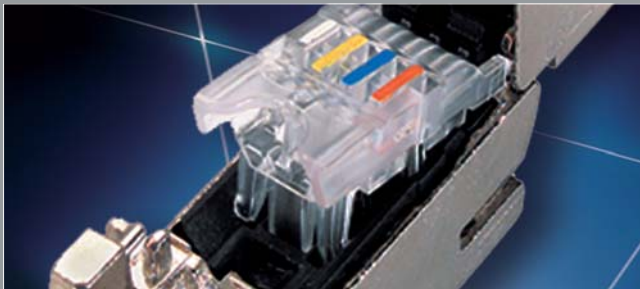
# Designed for Industry



SECURITY kann so aufregend sein.  
Wenn Sie sie nicht haben.  
SCALANCE S.



Einfach projektieren.  
SOFTNET Security Client für IP-basierten Zugriff .



Schnell und sicher mit System.  
FastConnect.



Diagnose vor Ort.  
SCALANCE X.

STEP 7- Projektierung,  
Diagnose



WBM/IT-CP



Datentransfer  
CP 343-1 Advanced

File  
Transfer  
Protokoll

- 1 Security Module SCALANCE S612 zum Schutz der Automatisierungszelle
- 2 SIMATIC Field PG mit SOFTNET Security Client
- 3 Switch SCALANCE X208
- 4 SIMATIC S7-300 mit CP 343-1 Advanced
- 5 Dezentrales Peripheriegerät ET 200S PNIO

Die SCALANCE Security Modules sind speziell für den Einsatz in produktionstechnischen Anlagen konzipiert. Sie können hier zum Schutz von Einzelgeräten oder auch ganzer Netzsegmente (z.B. von Automatisierungszellen) eingesetzt werden. Die geschützte Automatisierungszelle enthält eine SIMATIC S7-300 mit dem CP343-1 Advanced und einer E/A-Simulationsbaugruppe. Über einen Industrial Ethernet Switch SCALANCE X208 ist der CP 343-1 Advanced mit der ET 200S PN IO verbunden. Ebenfalls am Switch hängt das Security Modul SCALANCE S612 mit seinem internen Port. An den externen Port des Security Modules ist das Field-PG angeschlossen, auf dem die Applikationen laufen, die auf die geschützte Zelle zugreifen dürfen.

# Technische Daten

## 1 SCALANCE S612

<b>Schnittstellen</b>	
Anschluss von Endgeräten oder Netzkomponenten über Twisted Pair	2 x RJ45 Buchse, 10/100 Mbit/s
■ roter Port	External Network
■ grüner Port	Internal Network
Anschluss für Spannungsversorgung	1x4-poliger steckbarer Klemmenblock
Anschluss für Meldekontakt	1x2-poliger steckbarer Klemmenblock
<b>Diagnose-LEDs</b>	Power, Linkstatus, Datenverkehr
<b>Versorgungsspannung</b>	DC 24 V, redundant einspeisbar
<b>Stromaufnahme</b>	130 mA
<b>Verlustleistung</b>	ca. 4 W
<b>Schutzart</b>	IP30
<b>Anzahl gleichzeitig betreibbarer VPN- Verbindungen</b>	max. 64
<b>Anzahl interner Knoten</b>	max. 32

## 3 SCALANCE X208

<b>Schnittstellen</b>	
Anschluss von Endgeräten oder Netzkomponenten über Twisted Pair	8xRJ45-Buchsen, 10/100 Mbit/s (Halb-/Voll duplex)
Anschluss für Spannungsversorgung	1x4-poliger steckbarer Klemmenblock
Anschluss für Meldekontakt	1x2-poliger steckbarer Klemmenblock
<b>Diagnose-LEDs</b>	Power, Linkstatus, Datenverkehr
<b>Versorgungsspannung</b>	2 x DC24 V
<b>Stromaufnahme</b>	185 mA
<b>Verlustleistung</b>	ca. 4 W
<b>Schutzart</b>	IP30

## 4 CP 343-1 Advanced

<b>Versorgungsspannung</b>	DC +24 V
<b>Stromaufnahme, typ.</b>	160 mA aus DC 24 V extern
<b>Industrial Ethernet-Schnittstelle</b>	RJ45
<b>Übertragungsrate</b>	10/100 Mbit/s Autosensing
<b>S7-Kommunikation</b>	max. 16 Verbindungen
<b>S5-kompatible Kommunikation (SEND/RECEIVE)</b>	max. 16 Verbindungen
<b>PG/OP-Kommunikation</b>	max. 16 Verbindungen
<b>Multiprotokollbetrieb</b>	ISO, TCP/IP, UDP, RFC 1006
Summe aller gleichzeitig betreibbaren Verbindungen	max. 48
<b>PROFINET IO-Controller</b>	
Anzahl betreibbarer PN IO-Devices	125



PNIO

ngszelle

# Bestelldaten

Security- und Netzkomponenten	Bestellnummer
<b>Industrial Security Module</b>	
■ SCALANCE S612	<b>6GK5 612-0BA00-2AA3</b>
<b>VPN-Client</b>	
■ SOFTNET Security Client	<b>6GK1704-1VW01-0AA0</b>
<b>Industrial Ethernet Switch</b>	
■ SCALANCE X208 8 RJ45-Ports managed	<b>6GK5 208-0BA00-2AA3</b>
<b>IE Fast Connect Anschlussstechnik</b>	
■ IE FC Busleitungen	<b>siehe Katalog IK PI</b>
■ IE FC RJ45 Plug 180 RJ45-Steckverbinder mit integrierten Schneid-/ Klemm-Kontakten, 180° Kabelabgang	
1 Packung = 1 Stück	<b>6GK1 901-1BB10-2AA0</b>
1 Packung = 10 Stück	<b>6GK1 901-1BB10-2AB0</b>
1 Packung = 50 Stück	<b>6GK1 901-1BB10-2AE0</b>
SIMATIC Hard- und Software	Bestellnummer
<b>Field PG</b>	<b>6ES7712- ...</b>
<b>STEP 7 Version 5.3</b>	<b>6ES7 810-4CC07-0YA5</b>
<b>HMI-Software</b>	
■ WinCC flexible 2005 Runtime	<b>6AV6 613-1BA01-1CA0</b>
■ WinCC flexible Advanced Engineering-SW	<b>6AV6 613-0AA01-1CA5</b>
<b>Kommunikationsprozessor</b>	
■ CP 343-1 Advanced	<b>6GK7 343-1GX21-0XE0</b>
<b>ET 200S PN IO</b>	
■ Interfacemodul IM 151-3 PN	<b>6ES7 151-3AA10-0AB0</b>
■ Powermodul PM-E DC 24V	<b>6ES7 138-4CA01-0AA0</b>
■ Digitales Ausgabemodul 6 DO DC 24V	<b>6ES7 132-4BD00-0AB0</b>
■ Terminalmodul TM-P	<b>6ES7 193-4CC20-0AA0</b>
■ Terminalmodul TM-E	<b>6ES7 193-4CB20-0AA0</b>



# Immer aktuell informiert!

Informationen zur Inbetriebnahme von  
SIMATIC NET Configuration 4  
[www.siemens.com/simatic-net/configurations](http://www.siemens.com/simatic-net/configurations)

Informationen über die Netzwerkkomponenten SCALANCE  
[www.siemens.com/scalance](http://www.siemens.com/scalance)

Unseren Online-Support erreichen Sie unter  
[www.siemens.com/automation/service&support](http://www.siemens.com/automation/service&support)

Ansprechpartner in Ihrer Nähe finden Sie unter  
[www.siemens.com/automation/partner](http://www.siemens.com/automation/partner)

*Configurations sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten. Sie stellen keine kundenspezifische Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen. Sie sind für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Diese Configurations entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung. Durch Nutzung dieser Configuration erkennen Sie an, dass Siemens über die oben beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden kann. Wir behalten uns das Recht vor, Änderungen jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in dieser Configuration und anderen Siemens-Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.*

## Vorteile auf einen Blick:

- Robustes, industrietaugliches Design
- Rückwirkungsfreie Integration in bestehende Netztopologien möglich
- Sehr einfache und benutzfreundliche Konfiguration und Administration ohne IT-Spezialwissen
- Schutz vor gegenseitiger Beeinflussung
- Schutz vor versehentlicher Fehladressierung
- Verhinderung von Kommunikationsüberlast im Produktionsbereich
- Schutz vor Datenmanipulation und -ausspähung
- Alternativer oder ergänzender Schutz durch VPN möglich
- Skalierbare Schutzfunktionen

# [www.siemens.com/simatic-net](http://www.siemens.com/simatic-net)

## Siemens AG

Automation and Drives  
Postfach 48 48  
90327 NÜRNBERG  
DEUTSCHLAND

[www.siemens.com/automation](http://www.siemens.com/automation)

*SIMATIC® und SIMATIC NET® sind Marken von Siemens. Die übrigen Bezeichnungen in dieser Druckschrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann. Die Informationen in dieser Broschüre 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.*