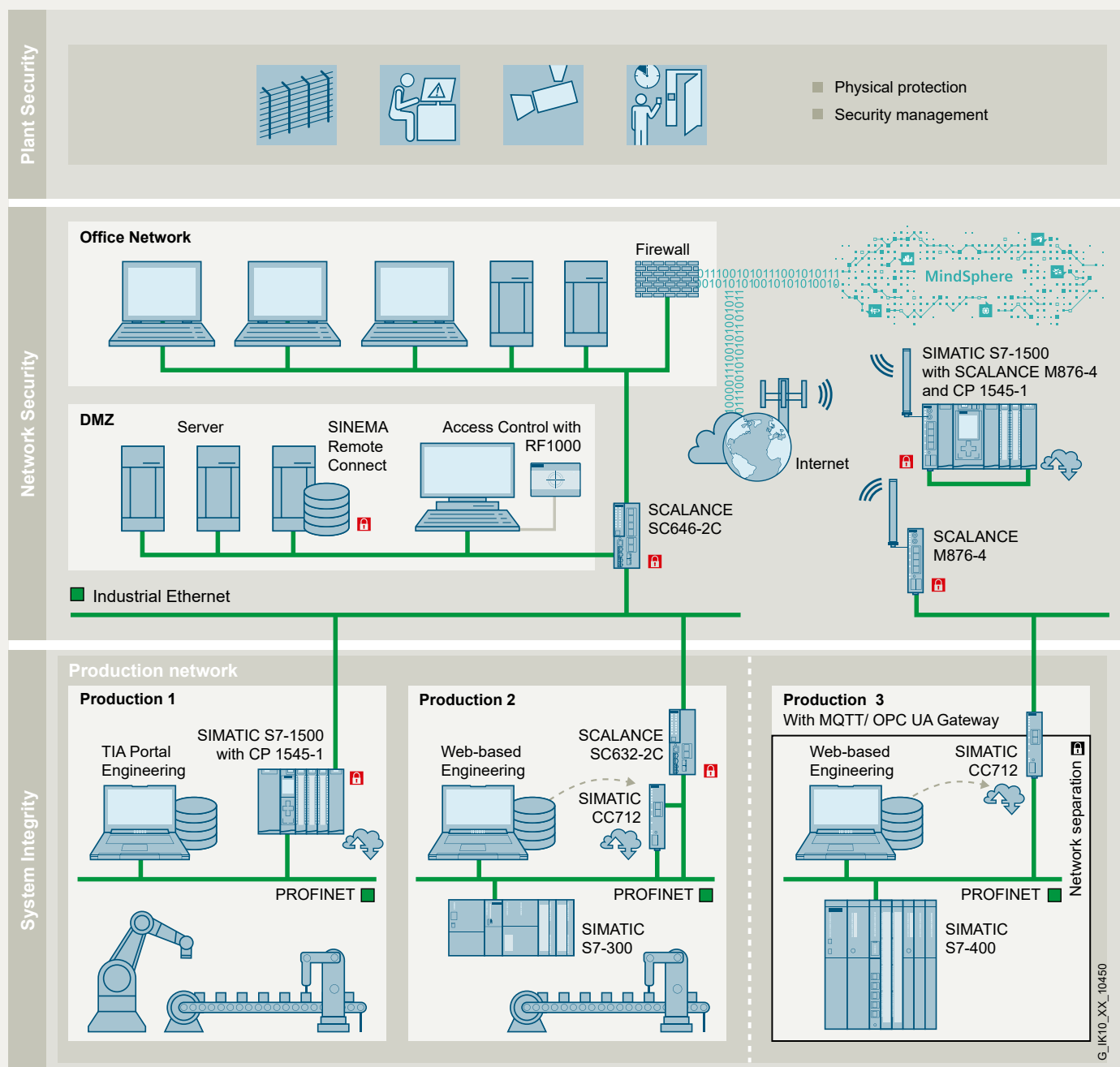




## Components for network security and access control

Cybersecurity for Industry  
Ordering overview – Edition 07/2022  
[siemens.com/network-security](https://www.siemens.com/network-security)



Network security with cell protection, secure remote access and secure cloud connectivity.

### Security threats demand action



#### Plant security

- Physical access protection
- Processes and guidelines
- Holistic security monitoring

#### Network security

- Cell protection, perimeter network and trusted zones
- Firewalls and VPN

#### System integrity

- System hardening
- Patch management
- Detection of attacks
- Authentication and access protection

### Defense in depth

To provide industrial plants with comprehensive protection from internal and external cyber attacks, all levels must be addressed simultaneously: from operations to field level, from access control to copy protection. With this in mind we have implemented a multi-faceted "defense in depth" protection concept based on IEC 62443 recommendations, the leading international standard for security in industrial automation. An essential component of this concept, which has already proved its worth in IEC 62443-based and certified product development, is network security.

- This includes safeguarding automation networks against unauthorized accesses through network access protection, network segmentation and encrypted communication. SCALANCE S industrial security appliances, SCALANCE M industrial routers for wired and wireless networks (4G/5G), or the security communications processors for SIMATIC S7 provide reliable cell protection.
- Through the combination of the cell protection concept with zero trust principals from the IT, application-specific remote access is possible for a consistent OT/IT security concept: [www.siemens.com/zero-trust](https://www.siemens.com/zero-trust)
- The reliability of network security components plays a major role in automation and communication networks in the energy sector and other industries where harsh ambient conditions prevail. The robust RUGGEDCOM security devices enable network security to be achieved in these environments as well.
- As a complement to integrated solutions for the management and administration of secured remote accesses, other passive components are available for physical network protection, such as the IE RJ45 Port Lock. The SCALANCE TAP104 supports the export of data traffic for advanced network analyses.



TIA Selection Tool  
[www.siemens.com/tst](https://www.siemens.com/tst)

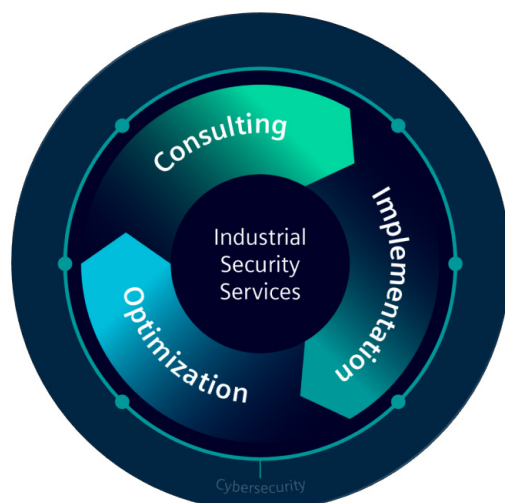
RUGGEDCOM Selector  
[www.siemens.com/ruggedcom-selector](https://www.siemens.com/ruggedcom-selector)

### Specific concepts for reliable protection

Want to find out how secure your industrial plant is, or what further security measures are available for your systems?

With Siemens Industrial Security Services you benefit from the comprehensive know-how and technical expertise of a global network of automation and cybersecurity specialists. The holistic approach of the industry-specific concept is based on the latest technologies and applicable norms and security standards. Threats and malware are recognized at an early stage, vulnerabilities are analyzed in detail and appropriate comprehensive security measures are implemented. Continuous monitoring gives plant owners maximum transparency regarding the security of their industrial facility, thus providing optimal investment protection at all times.

Find out more at:  
[www.siemens.com/iss](https://www.siemens.com/iss)



### "Charter of Trust" for a more secure digital world

"We can't expect people to support the digital transformation if the security of their data and networked systems is not guaranteed."

That is why Siemens will be working partners from industry, government and society to sign the "Charter of Trust" – a charter aimed at three important objectives:

- Protecting the data of individuals and companies
- Preventing damage to people, companies and infrastructures
- Establishing a reliable foundation on which confidence in a networked, digital world can take root and grow.

Find out more about the key principles and our partners:

[www.charter-of-trust.com](https://www.charter-of-trust.com)

### Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.


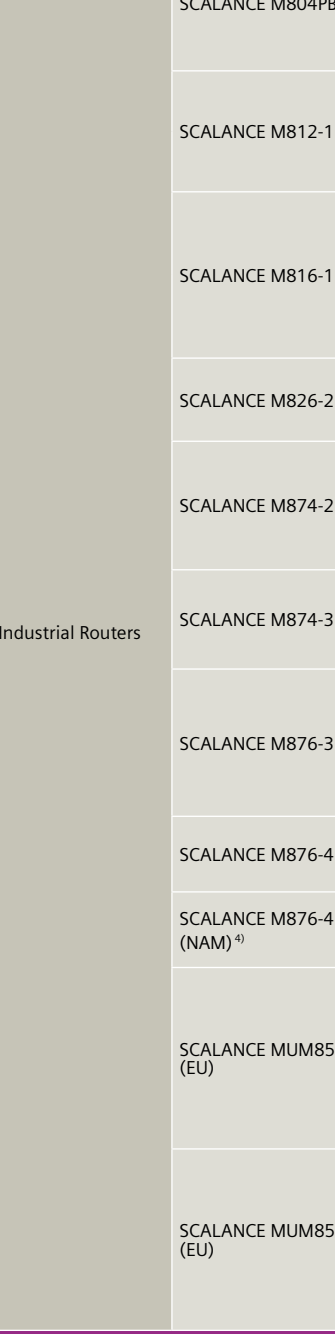



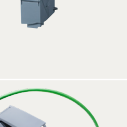


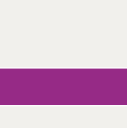





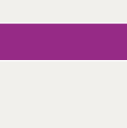
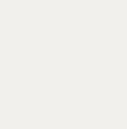
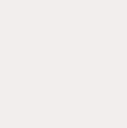

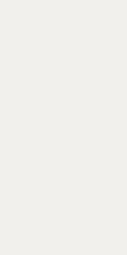


In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/cert>.

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

## Ordering overview – Components for network security and access control

	Application	Product	Network type 1	Network type 2	Interfaces	Comments	Article no. <sup>1)</sup>		
<b>SCALANCE S Industrial Security Appliances for flexible network segmentation</b>									
	Industrial Security Appliances	SCALANCE SC622-2C	Industrial Ethernet		2 × combo port with RJ45 or SFPs	Protection of devices and networks with firewall (750 Mbps data throughput); address translation with NAT/NAPT; connection to SINEMA Remote Connect	6GK5622-2GS00-2AC2		
		SCALANCE SC632-2C			4 × RJ45		6GK5632-2GS00-2AC2		
		SCALANCE SC636-2C			2 × combo port with RJ45 or SFPs		6GK5636-2GS00-2AC2		
		SCALANCE S615			5 × RJ45	Protection of devices and networks with firewall (100 Mbps data throughput) and VPN (IPsec/OpenVPN); address translation with NAT/NAPT; connection to SINEMA Remote Connect	6GK5615-0AA00-2AA2		
		SCALANCE SC642-2C			2 × combo port with RJ45 or SFPs	Protection of devices and networks with firewall (750 Mbps data throughput) and VPN (IPsec/OpenVPN); address translation with NAT/NAPT; connection to SINEMA Remote Connect	6GK5642-2GS00-2AC2		
		SCALANCE SC646-2C			4 × RJ45 2 × combo port with RJ45 or SFPs		6GK5646-2GS00-2AC2		
<b>SCALANCE M Industrial Routers for secured remote access via public and private networks<sup>2)</sup></b>									
	Industrial Routers	SCALANCE M804PB	Industrial Ethernet	PROFIBUS/MPI	2 × RJ45 1 × RS-485	Router for connecting PROFIBUS/MPI automation devices to Ethernet networks; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5804-0AP00-2AA2		
		SCALANCE M812-1			1 × RJ45 1 × RJ12	ADSL2+, Annex A; firewall and VPN (IPsec/OpenVPN)	6GK5812-1AA00-2AA2		
		SCALANCE M816-1				ADSL2+, Annex B, J; firewall and VPN (IPsec/OpenVPN)	6GK5812-1BA00-2AA2		
		SCALANCE M816-1		4 × RJ45 1 × RJ12	ADSL2+, Annex A; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5816-1AA00-2AA2			
		SCALANCE M816-1			ADSL2+, Annex B, J; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5816-1BA00-2AA2			
		SCALANCE M826-2		2-wire (SHDSL)	4 × RJ45 2 × terminal block (2-pin)	SHDSL; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5826-2AB00-2AB2		
		SCALANCE M874-2		Mobile wireless GSM (2G)	2 × RJ45 1 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and 2G mobile wireless network; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5874-2AA00-2AA2		
		SCALANCE M874-3		Mobile wireless GSM (2G), UMTS (3G)		IP router for transparent data transmission between Industrial Ethernet and 3G mobile wireless network; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5874-3AA00-2AA2		
		SCALANCE M876-3		Mobile wireless GSM (2G), UMTS (3G)/DMA2000 (EV-DO)	4 × RJ45 2 × SMA antenna connection		6GK5876-3AA00-2BA2		
		SCALANCE M876-4 (EU)		Mobile wireless GSM (2G), UMTS (3G), LTE (4G)	4 × RJ45 2 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and 4G mobile wireless network; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5876-4AA00-2BA2		
		SCALANCE M876-4 (NAM) <sup>4)</sup>					6GK5876-4AA00-2DA2		
		SCALANCE MUM853-1 (EU)			4 × RJ45 4 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and 5G public mobile network; firewall and VPN (IPsec/OpenVPN) or the connection to private 5G networks; SINEMA Remote Connect	6GK5853-2EA00-2DA1		
SCALANCE MUM856-1 (EU)		1 × M12 X-coded with PoE 4 × N-Connect antenna connection (mobile wireless, private 5G)	IP router for transparent data transmission between Industrial Ethernet and 5G public mobile network; firewall and VPN (IPsec/OpenVPN) or the connection to private 5G networks; SINEMA Remote Connect	6GK5856-2EA00-3DA1					
<b>Zero Trust for secure demand-based access to OT applications</b>									
	Local Processing Engine	SCALANCE LPE9403	Industrial Ethernet		3 × 10/100/1000 Mbps RJ45; 1 × 100/1000 Mbps SFP; 1 × combo port; 1 × USB3.0	Local Processing Engine with performant CPU; 64Bit ARMv8 (4core); 4 GB RAM; Debian Linux, Zero Trust Gateway by means of installation of additional software	6GK5998-3GS00-2AC2		
<b>Industrial Security Communications Processors (CPs) for remote SIMATIC controls</b>									
		CP 1243-7 LTE EU	Mobile wireless GSM (2G), UMTS (3G), LTE (4G)		1 × SMA antenna connection for LTE	For connecting SIMATIC S7-1200 to the 4G mobile wireless network (LTE); for connection to control rooms via TeleControl Basic remote control protocol; consider country approvals; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7243-7KX30-0XE0		
		CP 1243-7 LTE US					6GK7243-7SX30-0XE0		
		CP 1243-1			1 × RJ45	For connecting SIMATIC S7-1200; for connection to control rooms via remote control protocols (DNP3, IEC 60870, TeleControl Basic); firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7243-1BX30-0XE0		
		CP 1243-8 IRC			1 × RJ45 1 × 18-pin socket left for connecting TS modules	For connecting SIMATIC S7-1200; for connection to control rooms via remote control protocols (SINAUT ST7, DNP3, IEC 60870-5-104); can be expanded with TS module; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7243-8RX30-0XE0		
	Security Communications Processors	CP 1543-1	Industrial Ethernet		1 × RJ45	For connecting SIMATIC S7-1500; firewall and VPN (IPsec); and support of FTSP and SNMPv3 protocols for data encryption	6GK7543-1AX00-0XE0		
		CP 1545-1			1 × RJ45	For connecting SIMATIC S7-1500; firewall; and support of FTSP and SNMPv3 protocols for data encryption; with CloudConnect functionality	6GK7545-1GX00-0XE0		
		CP 1543SP-1			BusAdapter (BA), 2 ports (RJ45 or FO) depending on BA type	For connecting SIMATIC ET 200SP Distributed Controller; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7543-6WX00-0XE0		
		CP 1542SP-1 IRC			BusAdapter (BA), 2 ports (RJ45 or FO) depending on the BA type	For connecting SIMATIC ET 200SP Distributed Controller; for connection to control rooms via telecontrol protocols (SINAUT ST7, DNP3, IEC 60870-5-104, TeleControl Basic); VPN (OpenVPN); connection to SINEMA Remote Connect	6GK7542-6VX00-0XE0		
<b>RUGGEDCOM – rugged security components for harsh environmental conditions</b>									
	Mobile Wireless Routers	RUGGEDCOM RX1400	Industrial Ethernet		Mobile wireless GSM (2G), UMTS (3G), LTE (4G)	Industrial hardened compact edge router, integrated Ethernet switch with Cellular, GPS, Wireless LAN, Serial Device Server interfaces and Virtual Processing Engine for third party applications <sup>3)</sup>	6GK6014-0AM2-.....		
		RUGGEDCOM RM1224 (EU)			4 × RJ45 2 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and 4G mobile wireless network; VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK6108-4AM00-2BA2		
		RUGGEDCOM RM1224 (NAM) <sup>4)</sup>			4 × RJ45 2 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and 4G mobile wireless network; VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK6108-4AM00-2DA2		
		RUGGEDCOM RX1500	Industrial Ethernet		Mobile wireless GSM (2G), EVDO (3G), LTE (4G)	12/24/36 ports RJ45, up to 6 line modules, up to 4 or 8 Gigabit Ethernet ports, antenna connection	Industrial hardened Layer 2 and Layer 3 switch/router; firewall and VPN (IPsec); APE module for 3rd party applications <sup>3)</sup> (except in RUGGEDCOM RX1512)	6GK6015-0AM2-..... 6GK6015-0BM2-..... 6GK6015-1AM2-..... 6GK6015-1BM2-..... 6GK6015-1CM2-..... 6GK6015-0CM2-..... 6GK6015-0DM2-.....	
		RUGGEDCOM RX1501							
		RUGGEDCOM RX1510							
		RUGGEDCOM RX1511							
		RUGGEDCOM RX1512							
		RUGGEDCOM RX1524							
		RUGGEDCOM RX1536							
		RUGGEDCOM APE1808			2 × USB 3.0 ports, 2 × Gigabit Ethernet ports, 1 × display port, 1 × micro SD card slot	Utility grade application processing engine that can run commercially available third-party software, including cybersecurity and Edge Computing applications	6GK6015-0AL2-.....		
		RUGGEDCOM RX5000	Industrial Ethernet		Up to six line modules for up to 98 ports	Routing and switching platform with high port density; firewall and VPN (IPsec)	6GK6050-0AM2-.....		
<b>SCALANCE TAP104 for exporting entire data traffic for detection of anomalies</b>									
	Test Access Port	SCALANCE TAP104	Industrial Ethernet		2 × RJ45 network ports 2 × RJ45 diagnostic ports	For frame export in 10/100 Mbps Industrial Ethernet networks for data analysis	6GK5104-0BA00-1SA2		
<b>Access control</b>									
	Physical Network Access Protection	IE RJ45 Port Lock				Port lock with key for mechanical locking of RJ45 ports	6GK1901-1BB50-0AA0		
			SIMATIC RF1040R				With USB connection (1.8 m connection cable) and RS232 interface for the LF and HF range	6GT2831-6CA50	
SIMATIC RF1060R					With USB connection (1.8 m connection cable) for the HF range	6GT2831-6AA50			
SIMATIC RF1070R					With USB connection (1.8 m connection cable) and RS232 interface for the HF range (incl. Legic)	6GT2831-6BA50			
					OEM version; with neutral front film for customer-specific design; with USB connection (1.8 m connection cable) and RS232 interface for the HF range (incl. Legic)	6GT2831-6BA50-0AX0			
<b>Software for control and transparent management of network access and accessories</b>									
	Management Platform for Secured Connections and Simple Remote Access	SINEMA Remote Connect Virtual Appliance				Basic software package for 4 VPN connections; SINEMA Remote Connect Client, license key	6GK1720-1AH01-0BV0		
		SINEMA Remote Connect Upgrade 64				64 VPN connections upgrade	6GK1722-1JH01-0BV0		
		SINEMA Remote Connect Upgrade 256				256 VPN connections upgrade	6GK1722-1MH01-0BV0		
		SINEMA Remote Connect Upgrade 1024				1024 VPN connections upgrade	6GK1722-1QH01-0BV0		
		SINEMA Remote Connect Client V3				OpenVPN client for connecting to SINEMA Remote Connect, license key	6GK1721-1XG03-0AA0		
		SINEMA Remote Connect Client V3 (OSD)				OpenVPN client for connecting to SINEMA Remote Connect, license key, OSD (Online Software Delivery)/Software download	6GK1721-1XG03-0AK0		
		SINEMA Remote Connect UMC License				License to enable the connection of the UMC server for central user management	6GK1724-2VH03-0BV0		
		SINEMA Remote Connect API License				License to enable the API interface	6GK1724-3VH03-0BV0		
		KEY-PLUG SINEMA RC				Removable data storage medium for activating the SCALANCE M-800/S615 connection to SINEMA Remote Connect	6GK5908-0PB00		
		SCALANCE CLP SINEMA RC				Removable data storage for activating the SCALANCE MUM85X to SINEMA Remote Connect with auto configuration	6GK5908-0UA00-0AA0		
		<b>SINEMA Remote Connect with autoconfiguration</b>							
		SCALANCE M Industrial Routers				SCALANCE M-800 (except SCALANCE M812-1)		Yes, with KEY-PLUG SINEMA RC	–
SCALANCE S Industrial Security Appliances				SCALANCE S615		Yes, with KEY-PLUG SINEMA RC	–		
				SCALANCE SC-600		Yes	–		
Security Communications Processors (CPs)				CP 1243-1/CP 1243-7 LTE		Yes, firmware V3.1 or higher	–		
				CP 1243-8 IRC					
				CP 1543SP-1/CP 1542SP-1 IRC		Yes, firmware V2.0 or higher	–		
				CP 1543-1		Yes, firmware V3.0 or higher	–		
	Software for Network Management	SINEC NMS				Scalable Network Management System for policy-based configurations and transparent monitoring of industrial networks	6GK8781-1.....		
		SINEC INS				Network infrastructure tool for central management of network services (e.g., DHCP, Syslog, NTP, RADIUS, TFTP Server)	6GK8751-1.....		
	Secure Access Management Solution	RUGGEDCOM CROSSBOW				Software for managing and securing remote maintenance access for field devices according to NERC CIP standards	6GK6000-1BC43-0AA0		

<sup>1)</sup> Current ordering data can be found on the Internet at: [www.siemens.com/industry/mall](http://www.siemens.com/industry/mall)<sup>2)</sup> Conditions of sales and delivery can be found at: [https://mall.industry.siemens.com/legal/vw/en/terms\\_of\\_trade\\_en.pdf](https://mall.industry.siemens.com/legal/vw/en/terms_of_trade_en.pdf)<sup>3)</sup> Suitable accessories and details can be found on the Internet at: [www.siemens.com/mall-remote-networks-accessories](http://www.siemens.com/mall-remote-networks-accessories)<sup>4)</sup> For further information on tested software applications, please contact your local Siemens partner<sup>5)</sup> For use in North America