INDUSTRIAL REMOTE COMMUNICATION

Remote Networks

Easy remote access to machines and plants

Brochure

Edition
09/2022

SIEMENS

Many ways of connecting to remote networks

Increasing bandwidths, higher speeds and performance levels, as well as falling communication costs are all opening up new possibilities in both public and industrial environments.

It's now easier than ever to connect your widely distributed plants, remote machines, or mobile applications via remote networks. Siemens offers a wide range of modems and routers for establishing the ideal connection to remote networks over dedicated lines, public switched or cellular telephone networks, or Internet – regardless of whether wired or wireless, IP-based, or analog.

The IP-based network components of SCALANCE M and SCALANCE S can be used widely in the fields of telecontrol, teleservice, and any other application for industrial remote communication. These devices protect remote networks and the communication between them against unauthorized access and data espionage by means of integrated security functions, like firewall and VPN encryption.

In addition, SINEMA Remote Connect, a management platform, facilitates secure and straightforward administration of communication connections.

The remote networks portfolio for IP-based networks is suitable for use in many different industries, such as:

- Power distribution
- Transportation systems
- Plant and machine building
- Water/wastewater treatment plants
- Oil and gas supply
- District heating networks
- Pumping stations

In the field of wind energy and photovoltaic plants, this portfolio also enables a global network to be set up for condition monitoring.

For more information, visit:
siemens.com/remote-networks

Your benefits with the Siemens remote networks portfolio:

- Low investment and operating costs for operator control and monitoring of remotely connected substations
- Reduction in travel and personnel costs thanks to remote programming and diagnostics
- IP-based and analog routers for any application
- Higher standard of data communication security thanks to integrated encryption and access protection mechanisms
- Commissioning and diagnostics via user-friendly web interface
- Easy and secure administration of virtual private network (VPN) connections
- Greater clarity in the control cabinet thanks to space-saving SIMATIC module design
- Integrated into TIA (Totally Integrated Automation)
- 5 years warranty for all SCALANCE products

SCALANCE M

The SCALANCE M portfolio consists of industrial routers for wireless or wired access. The products facilitate the efficient connection of stationary and mobile stations to a control center. Extensive security functions, such as firewalls and VPN encryption, offer protection during transmission of data.

Wireless routers

The wireless SCALANCE M routers use the globally available, public cellular telephone networks (3G, 4G, and 5G) for data transmission. This makes them a cost-effective alternative to the set-up of corporate wireless networks.

Your benefits:

- High data rates allow the transmission of mass data or images in real time
- Provider-independent
- Connection of extremely remote substations is possible

	SCALANCE MUM856-1	SCALANCE MUM853-1	SCALANCE M876-4 (LTE)
Standard	5G, 4G, 3G	5G, 4G, 3G	4G
Frequency bands	Public, private (private 5G networks)	Public, private (private 5G networks)	Public (public mobile networks)
Bandwidth	Downlink: up to 1000 Mbps Uplink: up to 500 Mbps	Downlink: up to 1000 Mbps Uplink: up to 500 Mbps	Downlink: up to 100 Mbps Uplink: up to 50 Mbps
DI/DO	1/1	1/1	1/1
Antenna connectors	4 x n-connect	4 x SMA	2 x SMA
LAN interfaces	1 x M12 (1000 Mbit)	4 x RJ45 (1000 Mbit)	4 x RJ45 (100 Mbit)
Temperature range	–30 °C ... +60 °C	–30 °C ... +60 °C	–20 °C ... +70 °C
Safety class	IP65	IP30	IP20
Security	VPN (IPsec/OpenVPN*)/Firewall	VPN (IPsec/OpenVPN*)/Firewall	VPN (IPsec/OpenVPN*)/Firewall
Special characteristics	Certified for rail applications; Sleep-Mode (hardware-based); VXLAN	Managed 4-port switch; Sleep-Mode (hardware-based); VXLAN	Managed 4-port switch; certified for rail applications
	Redundant power supply; network management via SNMP; text message alerts; NAT; connection to SINEMA Remote Connect		
Advantages	High security standards by means of a firewall (stateful packet inspection) and VPN connections (IPsec) as an integral component of the Industrial Security concept		

* For connection to SINEMA Remote Connect as a client

Wired routers

Wired SCALANCE M routers enable the connection of Ethernet-based subnets and automation devices via existing cable infrastructures. The connection of devices in PROFIBUS networks is also possible. This portfolio includes devices for connection to two-wire cables or wired telephone and DSL networks.

Your benefits:

- Simple connection of local networks using IP communication via WAN
- High process availability due to redundant transmission paths

	SCALANCE M804PB	SCALANCE M826-2
Standard	PROFIBUS/MPI	SHDSL
Frequency bands	Private (existing infrastructure)	Private (existing infrastructure)
Bandwidth	Up to 12 Mbps (at the PROFIBUS/MPI interface)	Up to 15.3 Mbps
DI/DO	1/1	1/1
DSL connection system	–	2 x SHDSL (terminal strip)
LAN interfaces	2 x RJ45	4 x RJ45
Temperature range	–20 °C ... +60 °C	–40 °C ... +70 °C
Safety class	IP20	IP20
Security	VPN (IPsec/OpenVPN*)/Firewall	VPN (IPsec/OpenVPN*)/Firewall
Special characteristics	PROFIBUS/MPI interface	Certified for rail applications
	Redundant power supply; network management via SNMP; NAT; connection to SINEMA Remote Connect with autoconfiguration	
Advantages	• Convenient and cost-efficient connection of existing systems with PROFIBUS/MPI to SINEMA Remote Connect for secured remote access • Standardized remote maintenance concept for new and existing plants	• Connection to existing two-wire infrastructure thanks to SHDSL support • Wide range of possible network topologies – e.g., point-to-point, line, link aggregation (4-wire) • Low investment and operating costs for operator control and monitoring of remotely connected substations

* For connection to SINEMA Remote Connect as a client

SCALANCE S

SCALANCE S Industrial Security Appliances ensure secured access to globally distributed plants, machines, and applications. They protect automation cells and all devices without their own protection functions from unauthorized access, such as espionage and manipulation.

SCALANCE S components secure communication with stateful inspection firewall and virtual private networks (VPN). All variants enable configuration via Web-based Management (WBM), Command Line Interface (CLI), Simple Network Management Protocol (SNMP), Network Management SINEC NMS, and TIA Portal. A digital input enables the controlled establishment of a VPN connection, e.g., for remote maintenance.

Your benefits:

- High firewall and encryption performance
- Management of up to 200 VPN connections
- Network Address Translation (NAT/NAPT) for communication with serial machines with identical IP addresses





	SCALANCE SC632-2C	SCALANCE SC636-2C	SCALANCE S615	SCALANCE SC642-2C	SCALANCE SC646-2C
Firewall data throughput	750 Mbps	750 Mbps	100 Mbps	750 Mbps	750 Mbps
DI/DO	1/1	1/1	1/1	1/1	1/1
Electrical connection	2 x RJ45 ports	6 x RJ45 ports	5 x RJ45 ports	2 x RJ45 ports	6 x RJ45 ports
Optical connection	2 x combo ports with SFP	2 x combo ports with SFP	–	2 x combo ports with SFP	2 x combo ports with SFP
Temperature range	–40 °C ... +70 °C	–40 °C ... +70 °C	–40 °C ... +70 °C	–40 °C ... +70 °C	–40 °C ... +70 °C
Protection class	IP20	IP20	IP20	IP20	IP20
Bridge firewall	Yes	Yes	No	Yes	Yes
Dynamic firewall	Yes	Yes	Yes	Yes	Yes
User-specific firewall	Yes	Yes	Yes	Yes	Yes
Product function with VPN connection	OpenVPN*	OpenVPN*	IPsec, OpenVPN*	IPsec, OpenVPN*	IPsec, OpenVPN*
Number of VPN tunnels	–	–	20	200	200
Number of firewall rules	1000	1000	128	1000	1000
MRP-Client/ HRP-Client	No	Yes	No	No	Yes
Special characteristics	Configurable security zones, VRRPv3 coupling, connection to SINEMA Remote Connect				

* For connection to SINEMA Remote Connect as a client

THE MANAGEMENT PLATFORM FOR REMOTE NETWORKS

SINEMA Remote Connect

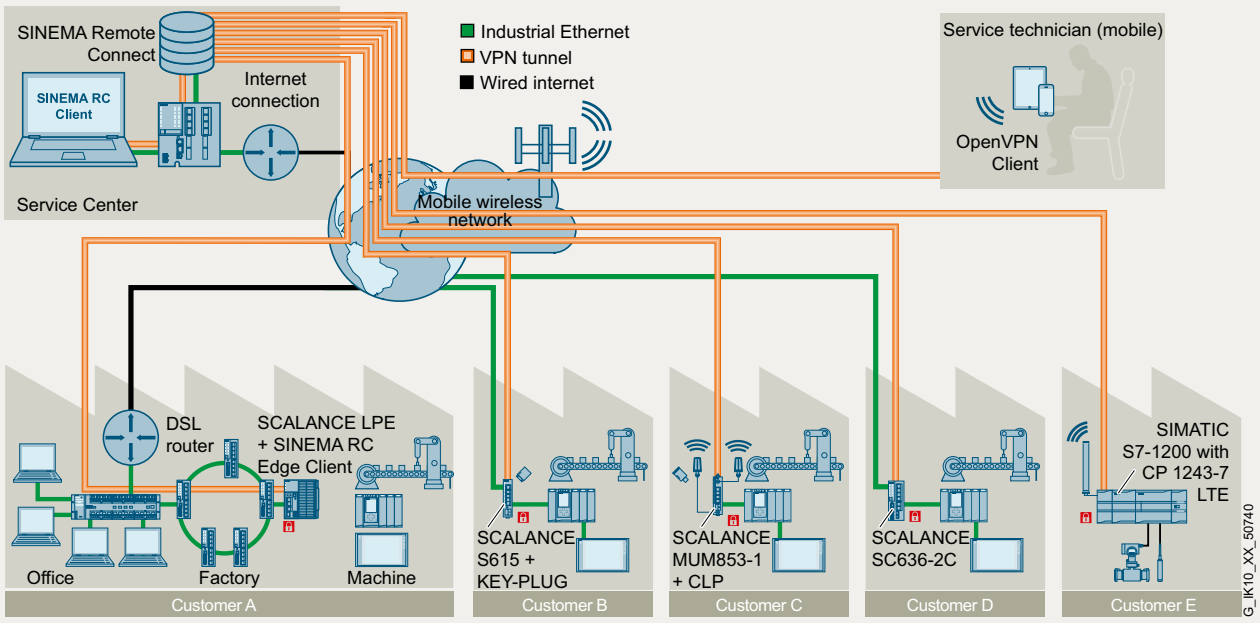
The management platform for remote networks – SINEMA Remote Connect – is a server application. It allows users to easily maintain widely distributed plants or machines by secured remote access.

SINEMA Remote Connect ensures the secured administration of VPN connections between the control centers, the service engineers, and the installed plants. Direct access to the corporate network, in which the plant or machine is integrated, is avoided. The service engineer and the machine to be maintained each establish an independent connection to a SINEMA Remote Connect server. The identity of the partners is verified by an exchange of certificates, before any access to the machine is granted. The connection to SINEMA Remote Connect can be set up over diverse media, such as cellular phone networks, DSL, or existing private network infrastructures.

For more information, visit:
siemens.com/sinema-remote-connect

Your benefits:

- Central administration of all VPN connections
- Simple management of different users, including user-specific access rights – even to unique IP addresses in the subnet (Dedicated Device Access)
- Address book function for fast connection
- Protocol-independent, IP-based communication
- Easy integration of Siemens routers, Industrial Security Appliances, compact RTUs, and communications processors by auto-configuration
- Special IT knowledge regarding remote access is not necessary
- Easy selection and connection to identical serial machines for original equipment manufacturers (OEM)
- Operation also in virtualized environment (on-premise or Cloud)
- Multi-factor authentication



Secured remote service of serial machines and remote stations by means of SINEMA Remote Connect

For more information, please visit:
siemens.de/remote-networks

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

Article No. 6ZB5530-0CB02-0BA5
Dispo 26000
BR 0922 0 PoD 8 En
Produced in Germany

Security information

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
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
siemens.com/cert.