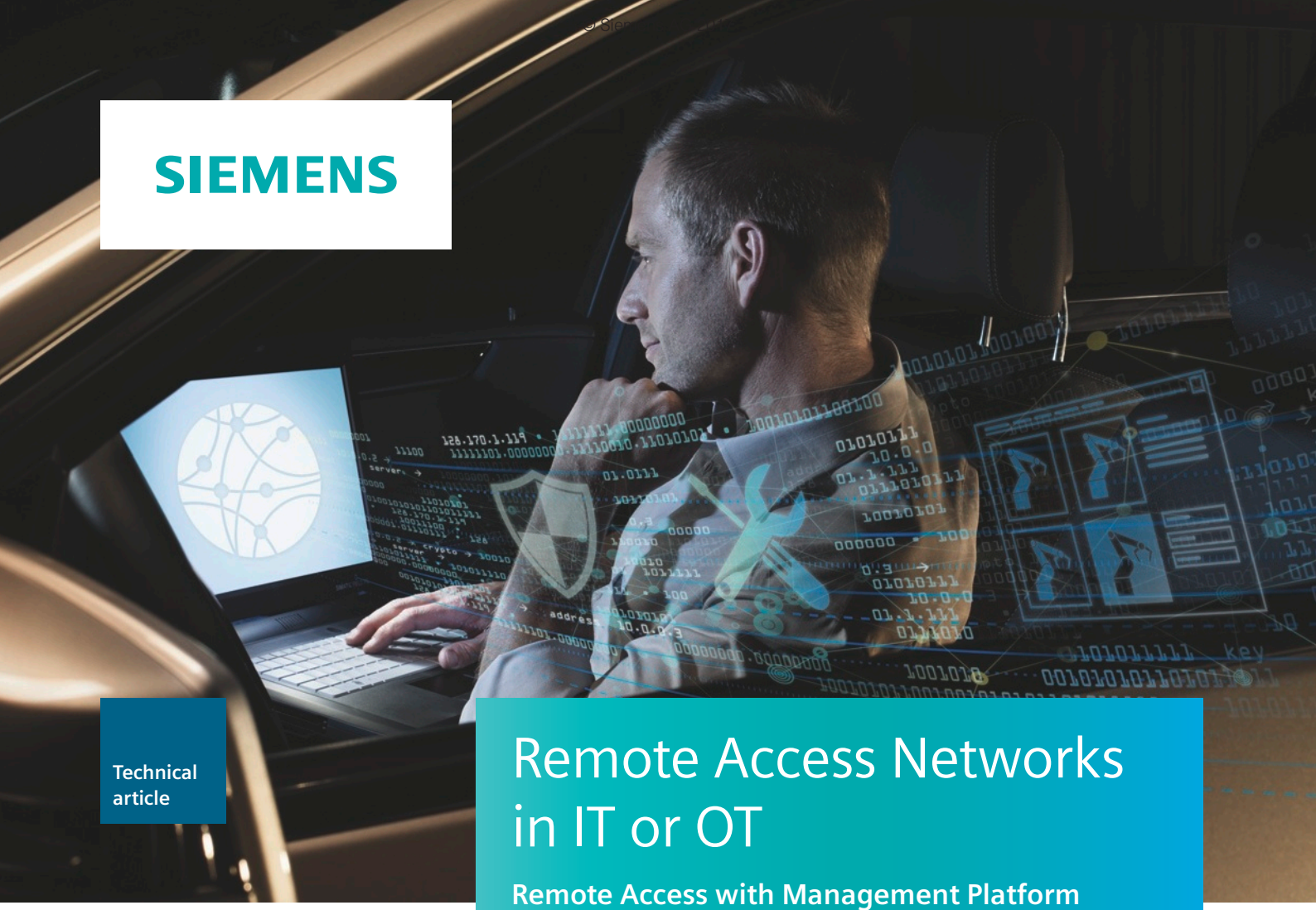
SIEMENS



Technical article

# Remote Access Networks in IT or OT

## Remote Access with Management Platform or Remote Networks via Jump Server and Private Cloud

**The requirements concerning industrial security and the protection of confidential company data are growing continuously.**

**In companies, IT departments and IT service providers are also increasingly assuming tasks to secure the remote access to plants and machines for the performance of remote maintenance services by third parties.**

**In doing so, there are specific requirements regarding the location and the responsibilities for the server – from hosting in the enterprise IT to private cloud solutions as managed service.**

The requirements for simple and secure remote maintenance concepts continue to grow with the increasing demand for remote access solutions for the performance of remote services in an industrial environment.

IT infrastructures at companies are increasingly converging and boundaries between IT and OT are shifting in both directions depending on the situation.

Different solutions and offerings arise on the market to meet the various requirements.

The focus is always on maintaining the productivity of the plant. This requires maintenance from time to time, which in this case is to take place remotely. The productivity of the plant, however, must not suffer from the sporadic remote access. Consequently, the remote access must be planned and reliably executed.

For this, a concept is suitable in which the automation cell is put in a remote maintenance mode when necessary and available. If the plant is not in this operating mode, a remote access is not permitted. It is recommended to equip the cell in such a way that it initiates the connection when in maintenance mode – ideally to a trustworthy and available partner.

If this is to be done for a large number of cells in the network, a central concept suggests itself, which can be utilized by all cells in the same way.

On the central side, this provides the opportunity to centrally manage the connections received.

A service technician wanting to reach a cell for maintenance should be able to reach various cells successively within a short time or simultaneously. It is crucial for this to be possible without much effort and IT expertise. The service technician therefore needs a simple tool, with which he can reach the remote maintenance end points (automation cell in the network). As the cells centrally report to a platform (see above), it is evident that the service technician also must be able to reach this central location if required.

For the execution of this concept, which is also referred to as a "rendezvous server", the central management platform must be implemented according to the security guidelines of the companies. This often excludes cloud-hosted solutions on external servers.

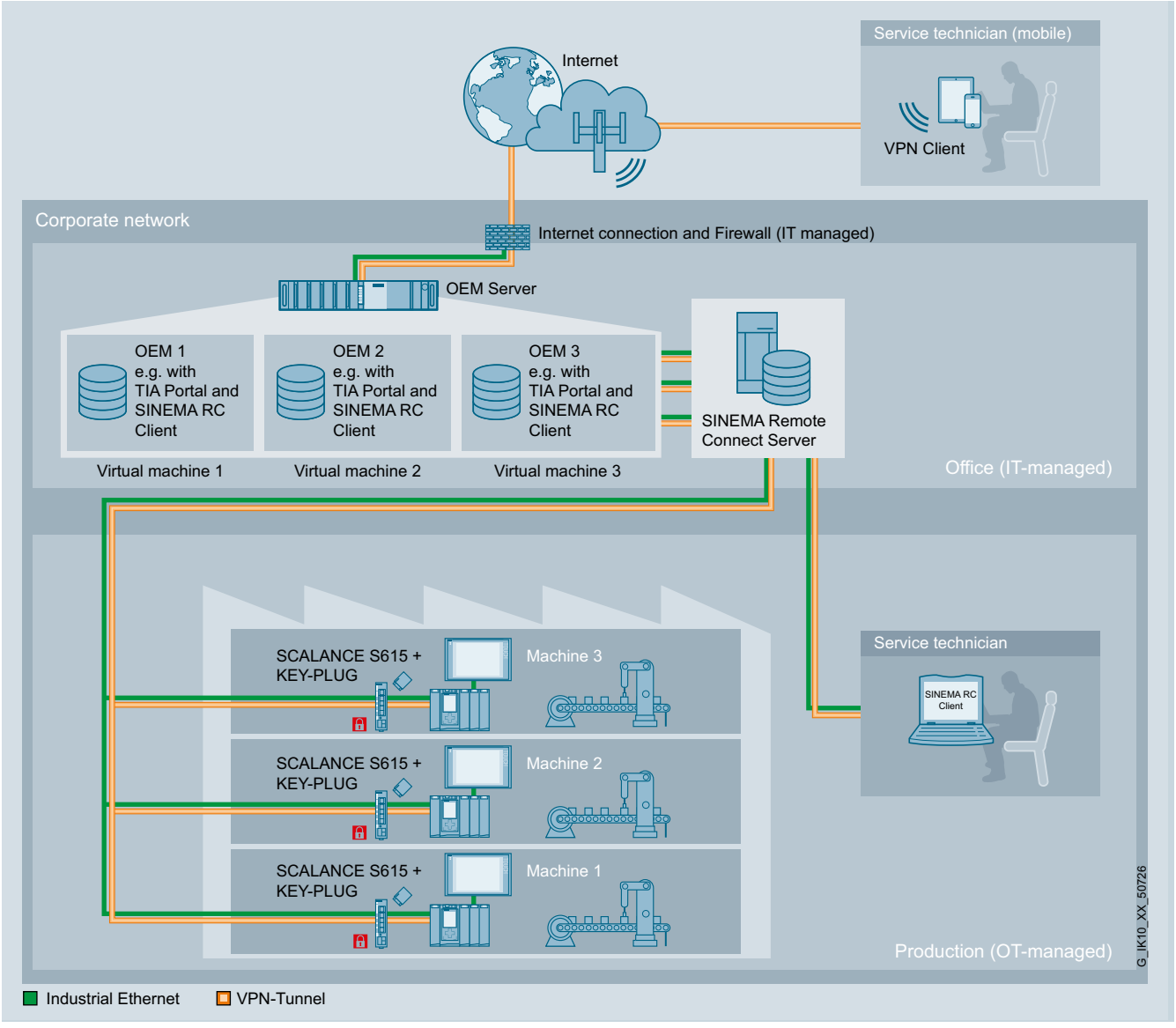
**Remote Access – but please securely and through my IT!**

As a leading supplier of automation and network components for the industry, Siemens always has an entire view of the needs of the users.

In addition to devices, Siemens also offers consulting services and services related to the customer network and IT security – all over the world.

State-of-the-art remote access solutions are systems based on central servers, which receive tunnel connections from machines and service personnel and interconnect them depending on the authorization. This allows one of BSI's (German Federal Office for Information Security) core requirements for industrial remote access networks to be met: Connections originating from the plants to locally enable full control over connections to the outside.

The following examples illustrate how such a server-based system – the management platform for remote networks (SINEMA Remote Connect) – can be used in scenarios where hosting beyond the end customer's sphere of influence (company network) is not permitted.




Remote access – the central server is the responsibility of the enterprise IT

In the first case, the IT of the operator gives the service technician access via remote desktop to a computer, which is the responsibility of the operator's IT. On this jump host, the operator provides the service technician with all the tools required for performing the maintenance (e.g., TIA Portal and TIA projects).

The IT thus prevents the use of possibly unsafe service laptops, which could introduce infected data into the company network.

### Service case example

The access takes place via an upstream computer on the company intranet, which is logged into by the OEMs / service technicians via tools provided by their office (remote desktop application).

From then on, they are in the secure area of their company network and can access the SINEMA Remote Connect server (likewise hosted on the operator's IT network) via the intranet – instead of the Internet – using the client application (SINEMA Remote Connect client) on the upstream computer.

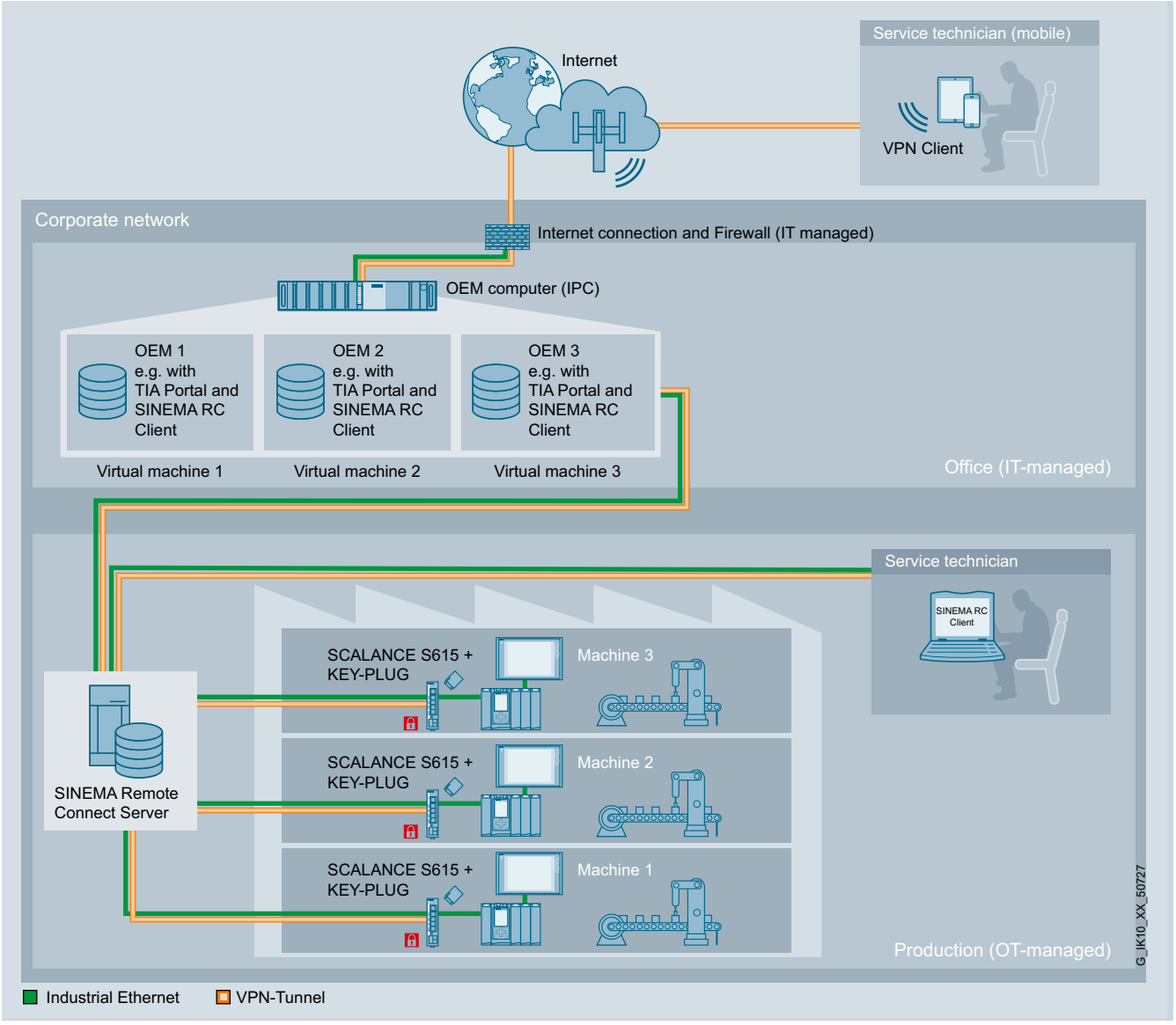
Another scenario is that the responsibility of the central remote maintenance server (SINEMA Remote Connect) lies not with the IT, but with the customer's factory network.

This, for example, is demanded by customers that want to manage the server by themselves – to be independent of IT processes – because of the need for quick response times to changes (users, authorizations, plants, ...).

The basic concept is the same as in the previous example with the jump host, only now SINEMA Remote Connect is operated on the factory network.

The management of the remote desktop connections from the outside, as well as the associated, upstream computer, remains with the IT of the operator.

Internal service technicians who have access to SINEMA Remote Connect via the factory intranet are therefore independent of the IT.




Remote access – the central server is the responsibility of the production IT (OT)

### Managed Services

With "Managed Services", Siemens offers a complete system based on server hardware, which is practically employed as a "private cloud" on-site at the customer.

Included are the hardware, virtualization environment, pre-installed virtual machines for SINEMA Remote Connect and a Windows operating system on which, for example, a TIA Portal can be installed next to the SINEMA Remote Connect client.

A complete system is thus available – freely configurable according to the needs of the customer – through which the service can be conducted. It only requires the SCALANCE routers already shown in the field as well as the possibility for service technicians to remotely access the virtual machine with the SINEMA Remote Connect client, e.g., via an in-house IT solution (VNC, remote desktop, ...).

In this scenario, Siemens takes care of the operation of the "private cloud" – Siemens service engineers have a separate remote access to the hardware and virtual environment of the "private cloud" to service it while in operation, and to provide support during optimization, expansion and trouble-shooting. Always separate from the customer's data, and without possible access to the customer's equipment.

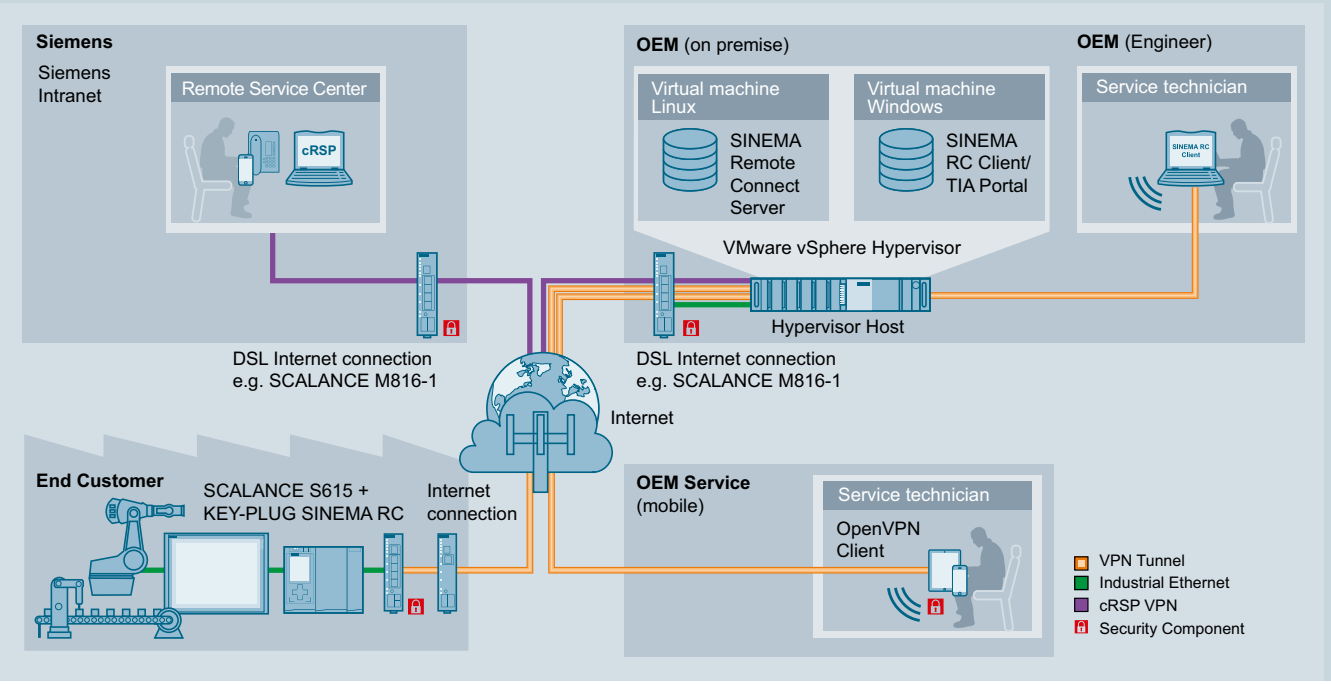
An all-round secure solution that enables customers to control their data at all times (and as required within their own company!) – without having to worry about the upkeep and operation of the various drivers, operating systems and software.

### Easy, transparent, secure

The decentralization of production plants and the fast as well as secure access to them remain important steps for companies to protect and gain market shares in light of the global competition. As a result, the demand for remote access scenarios with ever-increasing performance will only continue to grow.

The industrial routers SCALANCE M-800 and SCALANCE S615 form a rugged foundation for the remote access network. Modern security mechanisms such as firewalls, IPsec and OpenVPN as well as the latest mobile communications standards up to 4G (LTE) are part of today's solutions from Siemens.

Rounding out the remote access solution is SINEMA Remote Connect, the management platform for remote networks. IP-based, transparent remote access – easy and secure – from virtually anywhere and at any time with SINEMA Remote Connect and SCALANCE industrial routers.




Remote access – the central server as managed appliance (private cloud)

**SCALANCE M –**
**Secure. Flexible. Unlimited.**

The devices in the current industrial design of the controller SIMATIC S7-1500 are equipped with corresponding adapters for the rails of the 300-/1500-series and 35 mm DIN rail.

Furthermore, the temperature range and the requirements regarding the power supply and the digital inputs/outputs are matched to the SIMATIC automation world – thus meeting one of the highest industrial standards in the international marketplace.

Thanks to a wide range of accessories including antennas and cables as well as corresponding control cabinet feed-throughs and lightning protection elements, it is easy to mount the mobile communications devices in the control cabinet, and to install the antennas (some of which are IP65 splash-/dust-proof) at the best location for reliable reception.

In remote areas, too, a mobile communications router from the product line SCALANCE M-800 can be employed to actively initiate the connection establishment. By means of the integrated SMS function, it is possible to initiate the sending of a wake-up SMS to the mobile communications device using SINEMA Remote Connect.

## Benefits at a Glance

**SINEMA Remote Connect, Managed Appliance and SCALANCE M**

- **Increased Plant Flexibility and Cost Savings**
  - Remote access shortens response times and reduces the costs for maintenance and service.
- **Investment Protection for existing Plants**
  - Connection of existing plants, connection of new plants – future-proof solutions from a single source.
- **Investment Protection for future Plants**
  - Future-proof technologies and continuous expansion of available products with end-to-end compatibility.
  - Innovative technologies specifically for tasks in industrial environments.
- **Optimum Machine and Plant Availability**
  - Maximum reliability of the products during operation.
  - Plus service and support around the clock (24/7), worldwide.
- **Planning Security and Know-how Protection**
  - Long product life and availability safeguard long-term plant concepts and the utilization of employee know-how.
- **Compatibility**
  - Integrated products and accessories for the entire industrial infrastructure – from Key Plug to router to management platform.
- **Worldwide Application**
  - Mobile communications routers with radio licenses for more than 50 countries.
  - Our development processes take into consideration future applications and solutions (starting with the planning stage). As a result, our products are always easy to integrate and tailored to the needs of the users and end customers.
- **Product Quality “Made in Germany”**
  - Development and production at German locations (Karlsruhe/Nuremberg). That is why we give a 5-year warranty on the devices.

### Security information

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 only form one element of such a concept. For more information about industrial security, please visit **http://www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany


PDF
Technical article
FAV-21-2017-PD-PA
BR 0617 / 5 En
Produced in Germany



**siemens.com/remote-networks**