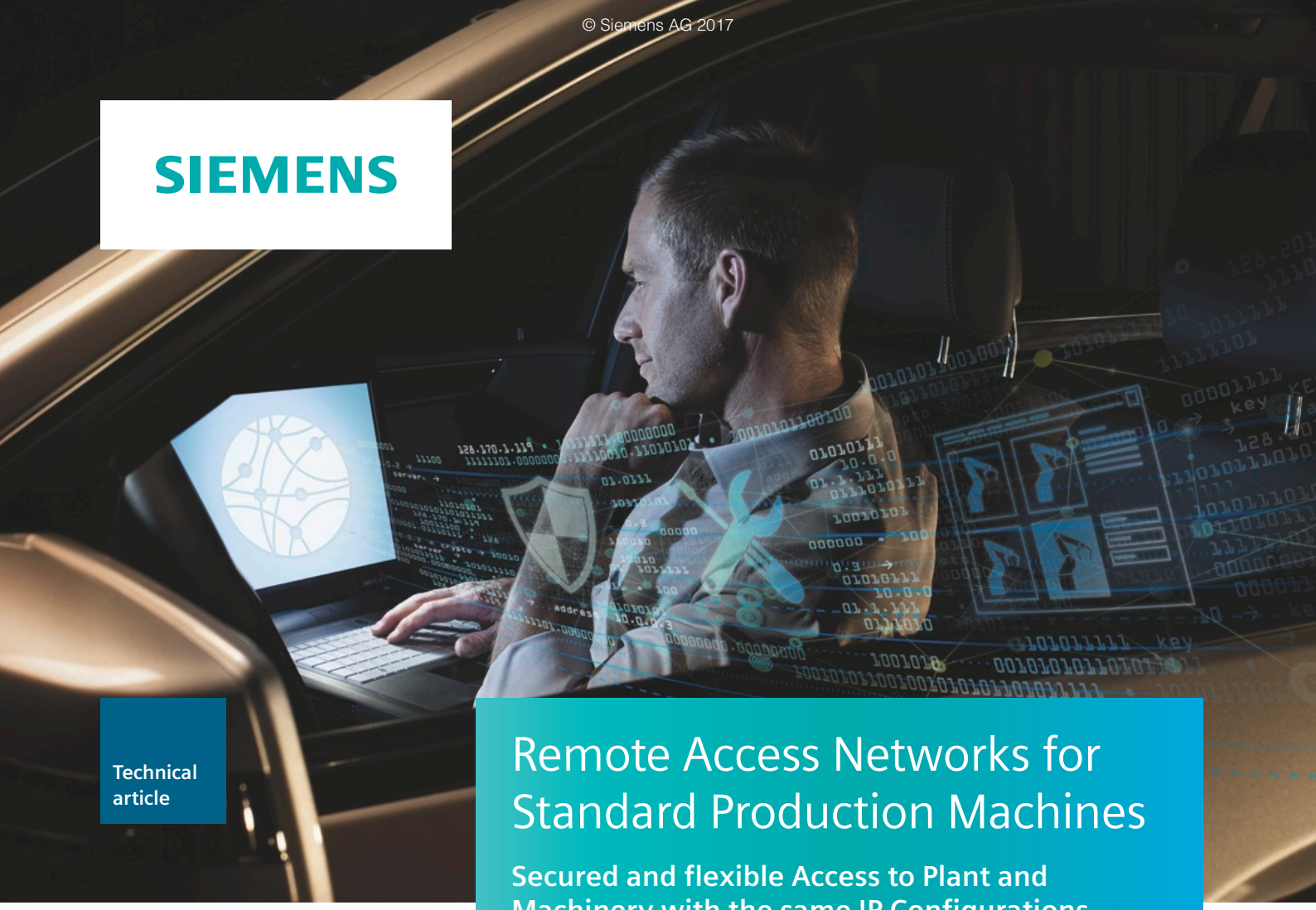
SIEMENS



Technical article

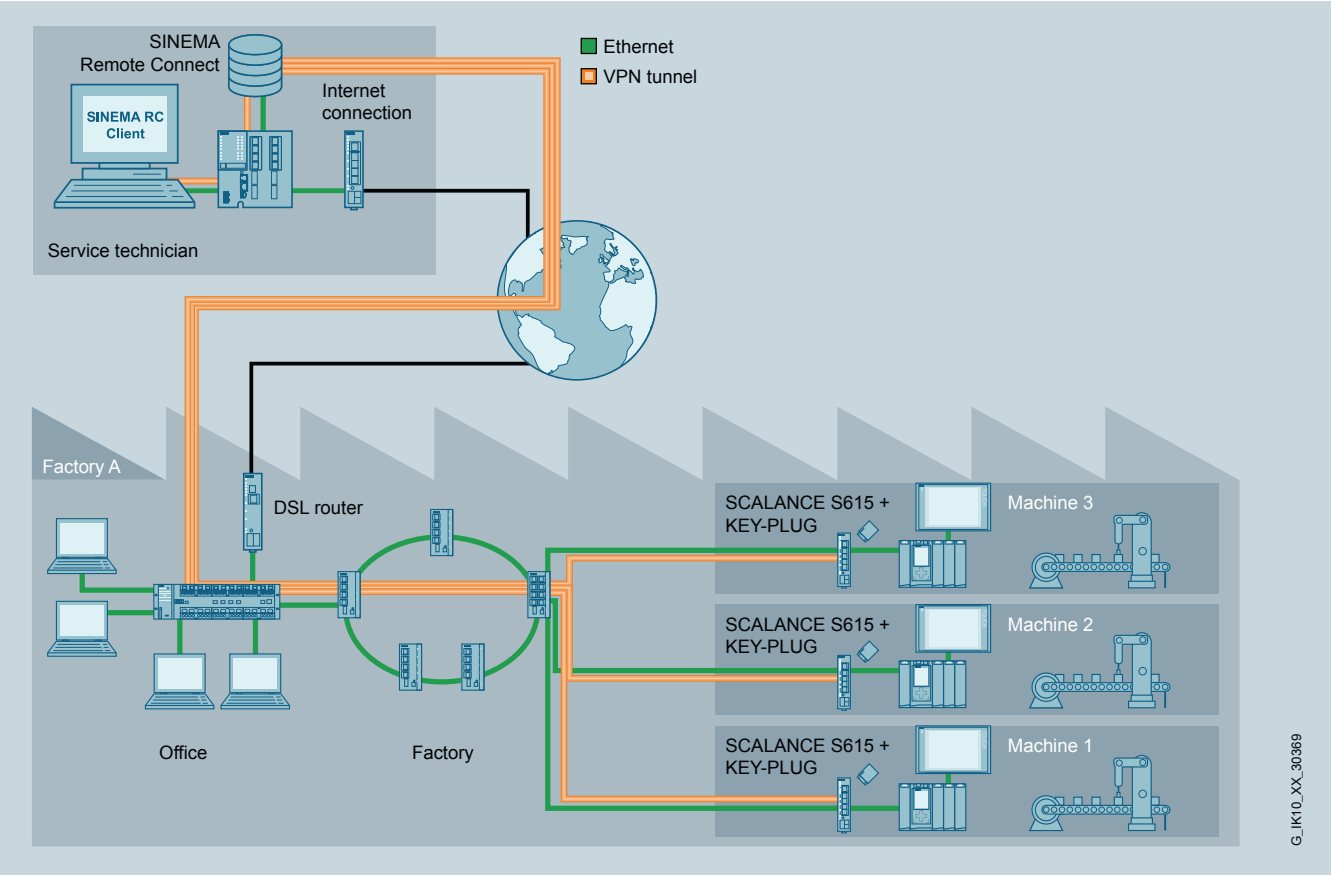
# Remote Access Networks for Standard Production Machines

## Secured and flexible Access to Plant and Machinery with the same IP Configurations

**The requirements concerning industrial security and the protection of confidential company data – while at the same time satisfying the growing demand for secured remote access to plant and machinery – often lead to complex, less flexible solutions. Especially in the area of standard production machines, there is great potential for savings through remote maintenance.**

Remote access has become indispensable in today's industrial production. Driven by the requirements of the growing digitalization, manufacturers are increasingly also networking smaller plants and standard production machines. If secured remote access is now to take place for a multitude of cells in the network, a central concept suggests itself, which can be used by all cells in the same manner. Always with the stipulation that the machinery initiates the connection establishment locally when necessary – establishing the connection "from the inside to the outside".

On the other, the central side, this makes possible the central management of the receiving connections and the clear depiction of identical machinery. This allows the basic requirements for the networking of automation cells in a network to be derived. In the case of standard production machines / multiple identical cells, this includes, e.g., the central management, which enables the easy administration of a large number of identical, local IP subnets. From the management of these cells, the possibilities of the remote stations for the remote access in the network are derived accordingly.




Easy, secured remote access to standard production machines.

The service technician, who wants to reach the cell for maintenance purposes, can reach various cells successively or simultaneously within a short time. It is crucial that this is possible effortlessly and without IT expertise.

The service technician therefore needs a simple tool, via which he can reach the remote maintenance end points (automation cell in the network). As the cells centrally report to a platform, it is obvious that the service technician must also be able to reach this central location if required.

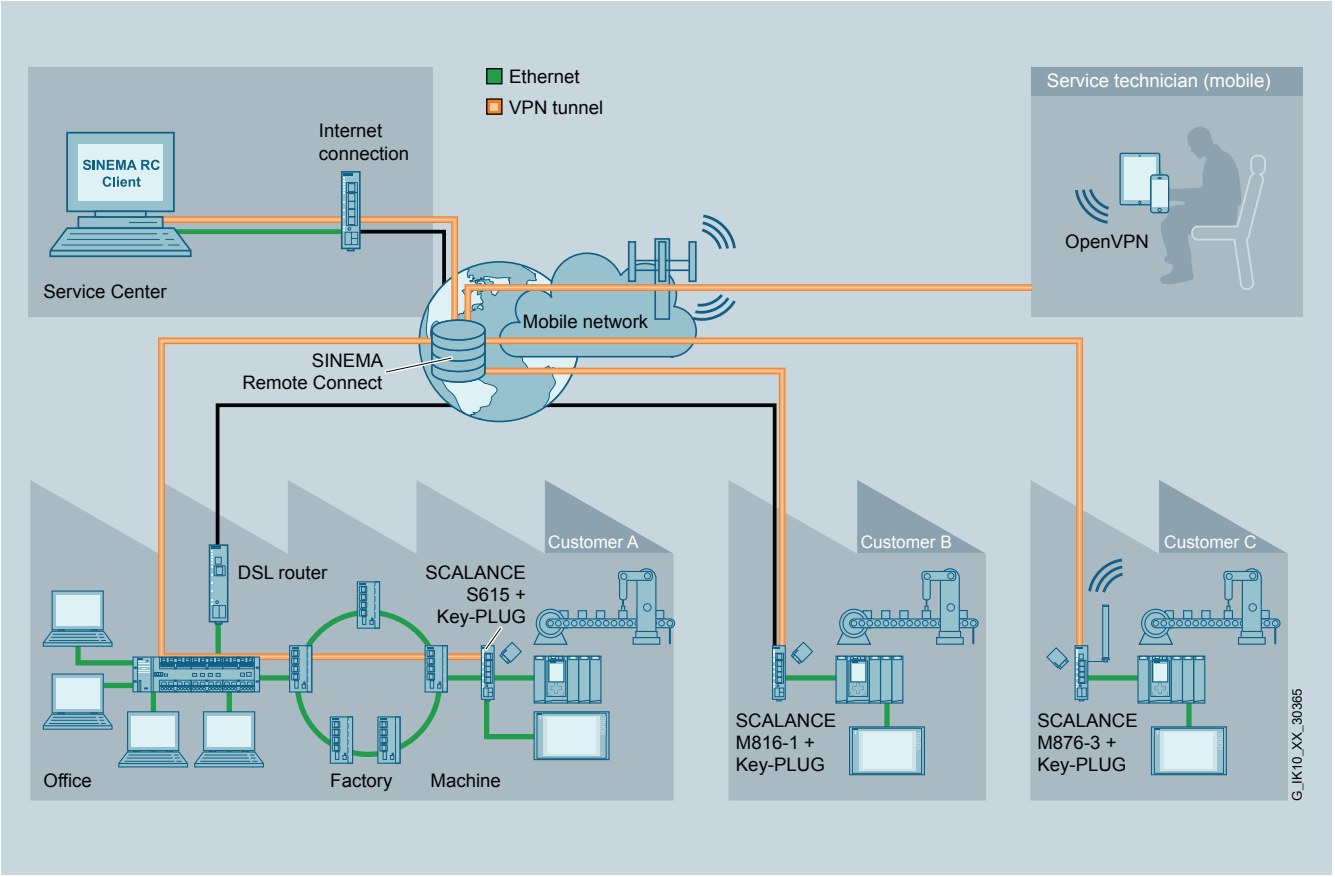
When selecting the encryption technology for the connection establishment, it should be ensured that it is easily and flexibly adaptable to the different needs of the industrial networks, but nevertheless be secure. For example, certificate-based mechanisms based on OpenVPN or IPsec suggest themselves.

The topics of access control, authentication and authorization also need to be viewed more critically than in everyday office life. Thus it should be precisely analyzed who is allowed to be connected to which participant at what time, and what authorizations he has there. This allows, e.g., firewall rules, user and device groups as well as their communication relationships with each other to be derived.

SINEMA Remote Connect is a server application. With SINEMA Remote Connect from Siemens, users can conveniently and securely maintain widely distributed plants or machines via remote access. This is true even if the machines are integrated into foreign networks, are standard production machines or mobile plants. Using the examples “standard production machine” and “mobile installation”, a more detailed description of the possibilities follows.

### The Standard Production Machine – Access to identical Systems in the Field

As mentioned at the beginning, one of the challenges for standard production machine builders is to reach identical machines and plants – which also have the same network configuration (e.g., identical IP addresses since the same TIA project is always loaded) – via remote access. Interconnected to a virtual network, the same addresses would lead to conflicts – with the result that the systems would not be accessible. Here, the solution lies in “1:1 NAT” – this type of address translation allows different virtual addresses to be assigned to machines having the same local IP addresses. The administration of the addresses (local and virtual) takes place centrally in SINEMA Remote Connect. Via the SINEMA Remote Connect client, which supports this 1:1 NAT scenario, these identical systems can be directly selected and connected using their associated virtual addresses. The convenient telephone book function in the SINEMA Remote Connect client provides a clear presentation of the machines – so that the right machine can be selected and connected via a VPN with a click of the mouse.




Mobile participants (customer C) can also be easily and securely reached.

**No Internet Connection available – Connection of mobile and remote Installations**

As long as the remote access to plant and machinery takes place within a factory, an Internet connection is usually available via the company network. Here, the security module SCALANCE S615 from Siemens is employed.

If such a connection is not possible, a dedicated DSL line can usually be used. For this purpose, the DSL router SCALANCE M816 can be utilized. However, if the plant sections are located in remote areas (e.g., as with water and wastewater plants) or are even mobile (e.g., waste containers or compactors), the use of mobile communications devices is necessary.

With the SCALANCE M876-4, Siemens offers a modern LTE device for broadband connectivity, e.g., needed by surveillance cameras. For worldwide use, 2G and 3G as well as a device for the US market (EV-DO) are available. All mobile routers can be connected to the management platform SINEMA Remote Connect. Depending on the version, the mobile routers feature 2 or 4 local LAN ports, via which corresponding devices (automation devices, cameras, ...) can be connected.

The connection establishment from the device to the server can be carried out via digital inputs as with wired devices, but also by sending an SMS to the device. In this case, too, the central administration of all devices and users helps with the connection of identical systems via different media.

Using the telephone book function in the SINEMA Remote Connect client, the participants to be reached can be unambiguously selected (1:1 NAT). Furthermore, the devices are visible in the client – so that, e.g., a node behind a mobile communications device can be reached on demand via an SMS wake-up call to the device. Simply by mouse click in the SINEMA Remote Connect client.

**Easy, transparent, secured**

The decentralization of production plants and the fast as well as secured 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 – that at the same time are easy to operate – will only continue to grow.

The industrial routers SCALANCE M-800 and security modules 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.

## SINEMA Remote Connect and Scalance M – Benefits at a Glance:

- **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 (even during 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 manufacture at German locations (Karlsruhe/Nuremberg). Our devices come with a 5-year warranty.

### SCALANCE M – Secured. Flexible. Boundless.

The devices in the present 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 feedthroughs 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-/dustproof) at the best location for reliable reception.

In remote, isolated areas, 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.

### 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-13-2017-PD-PA
BR 0317 / 4 En
Produced in Germany



**siemens.com/remote-networks**