SIEMENS

Technical article

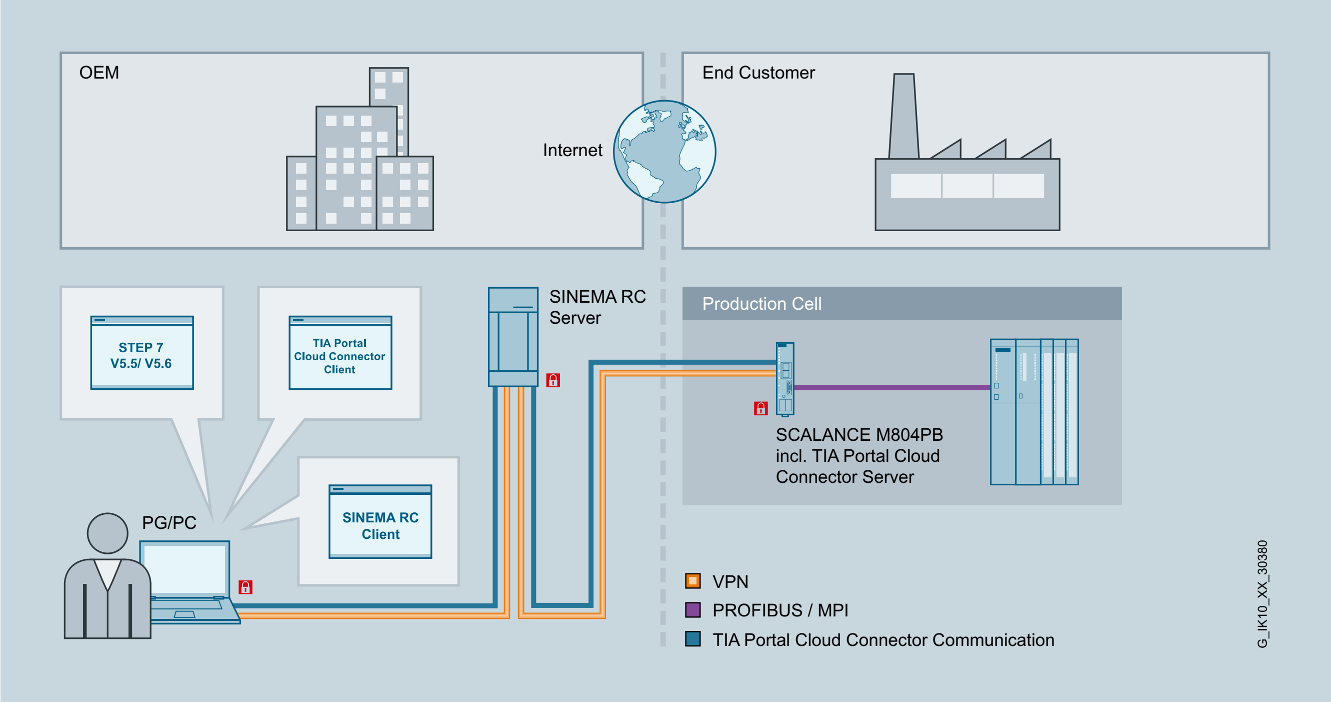
Secured remote access for PROFIBUS/MPI systems in the brownfield

With the increasing digitalization of existing installations, the demands on industrial security and the protection of company-confidential data in regards to remote services are growing. Especially in the brownfield, i.e., the modernization of existing plants, there are particular challenges when it comes to the connection (remote access/configuration) of PROFIBUS systems to modern IP networks.

Remote access has become an indispensable part of today's industrial production. Driven by the demands of the growing digitalization, manufacturers are increasingly networking even older machinery and equipment, some of which are still configured via MPI (e.g., SIMATIC S7-300/SIMATIC S7-400).

If secured remote access is now to take place directly on a PROFIBUS-/MPI-capable controller in the network (configuration of the participants behind it), a central concept lends itself, which can be used by all cells in the same manner, though it also requires a corresponding MPI interface. In doing so, the remote access always occurs under the stipulation that the systems locally initiate the connection if needed and the connection is established "from the inside to the outside".

With that, the basic requirements for the remote maintenance and configuration of PROFIBUS cells in an existing plant can be derived (in addition to Ethernet, now also by means of PROFIBUS/MPI). In the case of a pure connection via MPI, but also in mixed plant concepts (expansion/modernization, e.g., with SIMATIC S7-1500), IP routers with firewall and VPN technology are to be used throughout. A higher-level management system for remote networks can thus be set up, which centrally manages both the MPI and the Ethernet participants in one instance. The service technician – wanting to reach a cell for maintenance – can, within a short period of time, successively reach various cells or, in the case of Ethernet participants, also reach cells simultaneously. It is crucial for that to be possible without much effort and IT knowledge.



Secured remote access with SCALANCE M804PB

In contrast, it does not matter whether they are MPI or Ethernet participants, as both can be reliably and securely reached via the central management platform. The service technician therefore needs a simple tool with which the remote maintenance endpoints (automation cell in the network) can be reached. Since the cells centrally report to a platform, it suggests itself that the service technician also should be able to access this central location when necessary.

When choosing the encryption technology for the connection establishment, it should be kept in mind that it must be correspondingly simple and flexible to adapt to the different needs of industrial networks, but nevertheless be secure. For example, certificate-based mechanisms based on OpenVPN or IPsec lend themselves. The topics of access control, authentication and authorization have to be looked at more critically for existing plants as well as new plant sections than when it comes to daily office life. It thus makes sense to exactly analyze who may be connected when to which participant and with what permissions. From that, the planning, e.g., of firewall rules and user/ device groups as well their communication relationships to one another, can be derived. With SINEMA Remote Connect from Siemens, users can conveniently and securely maintain widely distributed plants or machines via remote access

Access to MPI systems in the field

As mentioned in the introduction, one of the challenges for machine builders is to also remotely access machinery and equipment still employing MPI. The management of the access points to the plants for the remote access takes place centrally in the SINEMA Remote Connect server. Via the SINEMA Remote Connect client, these MPI systems can be directly selected and connected to.

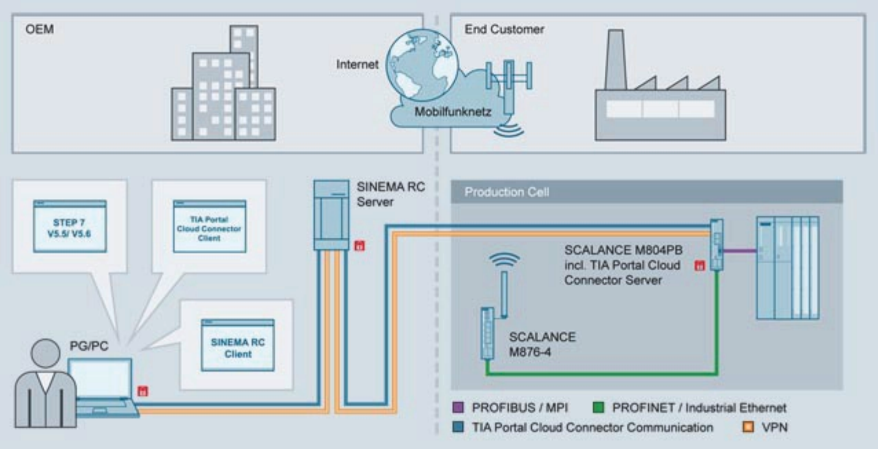
As soon as the tunnels from the plant side to the server and from the client PC to the server have been established, the PROFIBUS/MPI participants located behind the router can be accessed via the TIA Portal. From a user perspective, this technology makes the access just like as if the technician were locally (on-site at the plant) connected to the MPI network.

Decentralized project management

In the remote access case, the required engineering tool, the TIA Portal, can either be locally executed on the client computer of the service technician, or be retrieved from a central service center via the network or the Internet using the “TIA Portal Cloud Connector” functionality integrated into the router. Through the use of SINEMA Remote Connect, both the access of the service technician to the TIA Portal and the connection establishment of the router from the plant are secured end-to-end by an encrypted VPN tunnel.

Always keeping track and staying in control

The central user and device management of the central management platform provides transparency and clarity of devices and users. If required, the control over the actual connection establishment to the plant can be fully handed over to become the responsibility of the on-site plant operator. Here, the operator can use the router functionality that only allows the establishment of the VPN tunnel following a request by a local key switch (digital input). As a result, the initiator is always on the side of the plant.

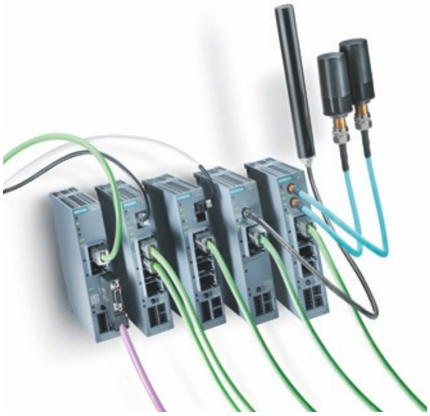

OEM
Internet
Mobilfunknetz
End Customer
STEP 7 V5.5/ V5.6
TIA Portal Cloud Connector Client
SINEMA RC Server
SINEMA RC Client
PG/PC
Production Cell
SCALANCE M804PB incl. TIA Portal Cloud Connector Server
SCALANCE M876-4
PROFIBUS / MPI
PROFINET / Industrial Ethernet
TIA Portal Cloud Connector Communication
VPN

Secured remote access with SCALANCE M804PB, STEP 7 and TIA Portal Cloud Connector

Simple, transparent, secure

The SCALANCE M804PB industrial router forms a robust foundation for the remote access network in conjunction with PROFIBUS/MPI systems. Modern security mechanisms such as firewall, OpenVPN and IPsec are part of the established solutions from Siemens.

The remote access solution is complemented by SINEMA Remote Connect, the management platform for remote networks: IP-based, transparent remote access – simple, secure, at any time and from almost anywhere – with SINEMA Remote Connect and SCALANCE industrial routers.



Secured remote access solution from a single source

The basis for functional and secured remote access is a professional industrial communication network. The assembly and maintenance of such communication networks require experience and extensive application know-how.

As part of the automation, industrial networks are always designed based on the application. Hence, when it comes to industrial networks, it is recommended to rely on partners who can develop and implement network and remote concepts that are precisely tailored to the respective requirements. As a partner to the industry, Siemens offers a future-oriented, comprehensive portfolio of network components. Furthermore, customers benefit from Siemens'

Professional Services for Industrial Networks, which build on many years of experience in designing, planning and implementing industrial networks, and also train and certify employees responsible in the operation of the networks.

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

Subject to change without prior notice
PDF
Technical article
FAV-79-2018-PD-PA
BR 0618 / 3 En
Produced in Germany

The information provided in this catalog contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

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.

www.siemens.com/remote-networks