Secure remote Connectivity
Presenter Profile

Christoffer Karlsson

Organisation
Siemens Australia

Job Function
Product manager – Industrial Communication
Introducing Siemens Industrial Communications Team....

Support capabilities:

- Network & Security Audits
- Trainings
- Design and Commisioning services
- Tender support
- Technical clarifications
- Pre- sales support
- Proof of concepts
- Seminars
- Workshops
Driving the digital transformation of discrete and process industries with Siemens Digital Industries

Digitalization
Automation
Electrification

Digital Enterprise

Process industries
- Design
- Planning
- Engineering
- Production
- Automation and industrial software for the process industries
- Industrial communication
- Industrial security
- Industrial services

Discrete industries
- Design
- Planning
- Engineering
- Production
- Services
- Automation and industrial software for the discrete industries

Digital twin of the real world across the entire value chain
Digitalization changes everything

And the right communication networks enable you to be ready for it!
Digitalization will change the way you work…

**Yesterday**
Non-digital industry

- Manual processes
- Intransparent processes
- Separated islands of automation
- Legacy systems
- No central alarms

**Tomorrow**
Digitalized manufacturing

- Secured remote access
- Industrial security
- Full automation
- Mobile applications
- Full process transparency
- Interoperability of processes
- Vertical integration
- Central alarm reporting
Digitalization results in enterprise and production layer to get closer connected.

Yesterday: Limited interoperability

Limited communication between enterprise and production layer

Today: Arising challenges through increasing interoperability

Challenge to handle complexity of increasing communication

Future: Defined interface to handle complexity

Two dedicated networks with defined managed interface
Our product range for remote access solutions covers all areas of application

Remote Networks
Remote communication via private and public heterogeneous networks

Industrial Remote Communication

**Permanent connectivity**
- Permanent point-to-point connection
- Low bandwidth requirement

**Spontaneous connectivity**
- Establish connection on demand
- Medium bandwidth requirement

**Other applications (Smart grid applications, video monitoring, …)**
- Permanent/on demand connection
- High bandwidth requirement

Integration into the industrial security concept
Solutions for remote access

Simple operation
- Control systems for process control
- Remote programming and diagnostics

Security and availability
- Redundancy
- Security integrated: firewall & VPN

Integrated RTU concept
- SIMATIC based modular RTUs and compact battery operated RTU's
- Various protocols
- Convenient engineering

Cost reduction
- SCADA solutions, teleservice systems and network components from a single source

Fast integration
- Network management
- Standard interfaces
- Software tools
- Integration in TIA Portal V16

Investment protection
- Compatibility with previous and future system solutions
- Migration concepts

Secure remote access
Management platform
SINEMA RC

Simple operation
Cost reduction
Fast integration
Investment protection
Integrated RTU concept
Security and availability

+ + + +
Industrial Remote Communication portfolio: Use in a wide variety of industrial environments

Complete SCADA solutions for water and energy
- Wide-ranging RTU portfolio based on SIMATIC S7
- Simple and redundant communications via heterogeneous networks
- Intelligent control systems based on PCS 7, WinCC and WinCC OA

Remote access to machinery and plants
- Secured teleservice access using VPN and firewall
- Simple access to serial machines via the SINEMA Remote Connect management platform

The right transmission for any communication
- A complete range of products for wireless connections and landlines
- High security standards
- Flexible modular system for networks
Industrial Security concept Siemens
Defense in depth according to IEC 62443

Defense in depth

**Plant security**
- Physical access protection
- Processes and guidelines
- Comprehensive security monitoring

**Network security**
- Cell protection and perimeter network
- Firewalls and VPN

**System integrity**
- System hardening
- Authentication and user management
- Patch management
- Detection of attacks

Further information: [www.siemens.com/industrialsecurity](http://www.siemens.com/industrialsecurity)
SCALANCE – Industrial Communication portfolio

SCALANCE: Industrial Communication proved to enable communication in production

- **High availability**
  based on industrial features and industrial design

- **Fast & easy integration**
  for new and existing networks based on TIA design

- **Easy to use**
  with configuration via Web Based Management or TIA Portal

- **Easy device replacement**
  with C-PLUG, also by untrained staff

- **For all Ethernet networks**
  local, wireless and remote

---

**Our Portfolio**

<table>
<thead>
<tr>
<th>Wired</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Industrial features</td>
</tr>
<tr>
<td>• Industrial design</td>
</tr>
<tr>
<td>• Fast &amp; easy integration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote / SCALANCE M</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Different medias (DSL, UMTS, LTE)</td>
</tr>
<tr>
<td>• Transparent connectivity</td>
</tr>
<tr>
<td>• Easy enrollment with SINEMA RC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Indoor and outdoor applications</td>
</tr>
<tr>
<td>• Several country approvals</td>
</tr>
<tr>
<td>• Real-time capability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security / SCALANCE S</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Firewall &amp; VPN</td>
</tr>
<tr>
<td>• Remote access</td>
</tr>
<tr>
<td>• Fits to industrial security concepts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Transparency for the industrial network</td>
</tr>
<tr>
<td>• Integration into HMI / SCADA systems</td>
</tr>
</tbody>
</table>
SINEMA Remote Connect
Remote maintenance and remote control with ease....

SINEMA Remote Connect Client

VPN Connection

SINEMA Remote Connect Server

WAN

Company network

Mobile network

LAN router

SCPADA

A

B

SCALANCE S615
e.g. CP1243-1

A

A

A

Remote pumping station

SCALANCE M804PB

A

B

A

B

A

B

B

B

Non-Conformance

Unrestricted © Siemens 2019
Page 13
SINEMA Remote Connect
Step-by-step implementation

1. Select hardware for remote location
   - Modems, SIMATIC S7 systems or firewalls

2. Accessories
   - Server and client software

3. Software
   - Server and client software

4. Software location
   - Virtualization or Cloud

Remote access from TIA portal with SINEMA RC/ works as independent software side by side
SINEMA Remote Connect Server Functions

Management of devices and users:
• User management with the configuration of rights
• Device and user management with group management

Connection management:
• Establishment of encrypted connections with OpenVPN and IPsec
• Establishment of permanent or event-based connections (establishment by wake-up SMS or digital input (DI))
Establishment of a remote connection:

- Direct connection to SINEMA RC server and the remote location
- By issuing a wake-up SMS (in connection with mobile routers SCALANCE M874/876)

Security mechanisms

- Tunnel encryption with OpenVPN

PKI smart card login (optional):

- With two-factor authentication by smart card and key

Usability:

- Flexible display of information and saving of user-specific view. IP addresses that cannot be reached are grayed out.
**Task**
- Remote maintenance of machines and larger plants
- Accesses to the machines/plants/system are protected by security mechanisms (OpenVPN, IPsec)

**Solution**
- Easy creation of devices with routing/ NAT information in SINEMA Remote Connect
- Simple selection of a device from the list of devices in SINEMA RC Client by mouse click
- Industry routers and service technicians can separately set up a secured connection to the SINEMA Remote Connect server
- SCALANCE M and S devices support firewall and VPN

**Benefits**
- Time and money saved
- Can be used without specialized IT knowledge
- Flexibility through easy expandability
- Transparent IP communication
- Prevention of manipulation and unauthorized access by means of secured data transmission and authentication
SINEMA Remote Connect use case
Secured access to Siemens RTU’s with DNP3

Task

- Telecontrol plant with encrypted connections to the remote terminal units

Solution

- Telecontrol server and SINEMA Remote Connect server are available in the telecontrol center
- All secured VPN connections managed by means of SINEMA Remote Connect
- Local connection of the telecontrol center to SINEMA RC
- Telecontrol accesses to remote terminal units via SINEMA RC

Benefits

- Use of standardized encryption protocols
- Direct connection of the control center to SINEMA Remote Connect without additional security components (in the control center)
- Simpler administration because SINEMA Remote Connect server and telecontrol server are at a single location

Configuration example SINEMA Remote Connect: Secured access from telecontrol center to remote terminal units
SINEMA Remote Connect use case
Remote service with SCALANCE M804PB and Step 7

Task

• Remote service with remote access for PROFIBUS via MPI: A service technician is to access a PROFIBUS plant from outside the company network

Solution

• Connection of PROFIBUS/MPI plants over SCALANCE M804PB that is connected to the production cell over MPI
• Easy configuration and management of the VPN tunnels with the SINEMA Remote Connect management platform enables secure remote access to the plant

Benefits

• Remote Acess on machines and plants with PROFIBUS/MPI reduces time and costs for on-site operation
• Easy connection of consiting plants
• Prevention of manipulation and unauthorized access thanks to secure data transmission and authentication
SINEMA Remote Connect
Getting started....

Promotional package

Application example

With SINEMA Remote Connect, machines from serial production can easily be connected via remote access – even if they have identical IP addresses. SINEMA Remote Connect offers NAT functionality for this purpose. Users can conveniently connect any machine via an address book function. Dedicated Device Access allows only authorized users to access selected machines.

SINEMA Remote Connect

Summary of advantages

• High security with maximum flexibility
  • Full end-to-end encryption
  • Unlimited number of connections/devices, infinitely scalable
  • Controlled enabling/locking of the maintenance object

• Advanced security functionality and process maturity
  • Connection to central user management
    (UMC server, optionally supplied by MS Active Directory)
  • Two-factor authentication through PKI smart card and key
  • Secure development process to IEC 62443-4-1)

• Direct support and very high functionality
  • Consultation and support during system setup
  • Support of common/established VPN standards

• Integrated Siemens network
  • Reliable and rugged hardware
  • Complete solution from one source for guaranteed compatibility
Secure Remote Connectivity with SCALANCE M

<table>
<thead>
<tr>
<th>Features / Functions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>High data rate (100 Mbps download, 50 Mbps upload) and antenna diversity</td>
<td>Transmission of high data rates over robust wireless connection</td>
</tr>
<tr>
<td>Extended temperature range (-20°C to +60°C)</td>
<td>Use in environments with increased climatic fluctuations</td>
</tr>
<tr>
<td>Supported security mechanisms: IPsec, OpenVPN, firewall</td>
<td>Increased network security through the use of common standards</td>
</tr>
<tr>
<td>Integrated managed 4-port switch</td>
<td>Up to 4 IP addresses for various subnets can be configured</td>
</tr>
<tr>
<td>Redundant power supply</td>
<td>Reliable operation, even if one power supply should fail</td>
</tr>
<tr>
<td>Support of country-specific standards UMTS / LTE (incl. US)</td>
<td>Widespread global use</td>
</tr>
<tr>
<td>Supported in SINEMA Remote Connect</td>
<td>Convenient and secured maintenance of widely distributed machines and installations via remote access</td>
</tr>
</tbody>
</table>
Secure Remote Connectivity with SCALANCE S

Industrial security appliance SCALANCE S

## Task

The security components employed in the network are to be configurable via standard engineering methods as well as from a central location.

## Solution

The industrial security appliance SCALANCE S supports common standard methods such as WBM and SNMP, and can also be centrally engineered via the TIA Portal\(^1\).

## Benefit

- Standard methods such as WBM, SNMP, MIB are supported
- End-to-end engineering with the TIA Portal\(^1\)
- Integration into network management systems such as SINEMA Server and SINEC NMS\(^2\)

---

1) TIA Portal V15 or higher
2) Planned start of delivery in 9/2018

---

**Network view**

1. Setting of firewall rules
2. Creation of VPN connections

---
Secure Remote Connectivity – RTU’s based on SIMATIC S7 with DNP3

Performance of modular RTUs

- **Modular RTU based on SIMATIC S7-400**
  - For large applications with high demands on the performance.

- **Modular RTU based on SIMATIC S7-300 / S7-1500**
  - For medium-sized applications with flexible configuration.

- **Modular RTU based on Distributed Controller SIMATIC ET 200SP**
  - For small and medium-sized applications with flexible configuration.

- **Modular RTU based on SIMATIC S7-1200**
  - For small applications with autonomous power supply.
## Secure Remote Connectivity - Battery powered compact RTU (RTU3000C)

### Security mechanisms
- OpenVPN tunnel
- Encrypted e-mail connection

### Web Server for configuration and diagnostics

### Remote reading and setting of I/Os

### Data logging on memory card

### Wake-up through SMS or phone call

### High degree of protection with IP68 external enclosure

### Localization und time synchronization via GPS (only with RTU3031C)

### Remote communication
- via cellular radio 2G/3G
- Through external routers (only RTU3010C)

### Communication
- SMS or e-mail
- Event- or time-controlled
- Telecontrol protocols: TeleControl Basic, DNP3, IEC 60870-5-104, SINAUT ST7
- FTP-Client
- MODBUS RTU/TCP
- HART

### Time Synchronization via
- NTP
- Telecontrol protocol
- Cellular network

### Expanded temperature range
- -40 to +70 °C (conformal coating)
Secure Remote Monitoring / Control via DNP3
Easy VPN Configuration via SINEMA Remote Connect

Task
All remote stations of a telecontrol system are to be connected to the control center via public networks using encrypted connections. All VPN connections should be configured from a central location.

Solution
The SINEMA Remote Connect Server is installed on a PC at the control center. This is where the devices and users, as well as the encrypted tunnel connections (VPN) are managed.

Benefit
SINEMA Remote Connect makes secure connections to remote stations (RTUs) particularly easy. The CP 1542SP-1 IRC supports SINEMA Remote Connect with autoconfiguration, enabling encrypted connections to be established directly to the RTU.
Thank you for your attention!

Christoffer Karlsson
Product manager
Industrial Communication

885 Mountain Highway
3153, VIC Bayswater
Australia
Christoffer.karlsson@siemens.com
+61437584211

The information provided in this brochure 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.

siemens.com/scalance