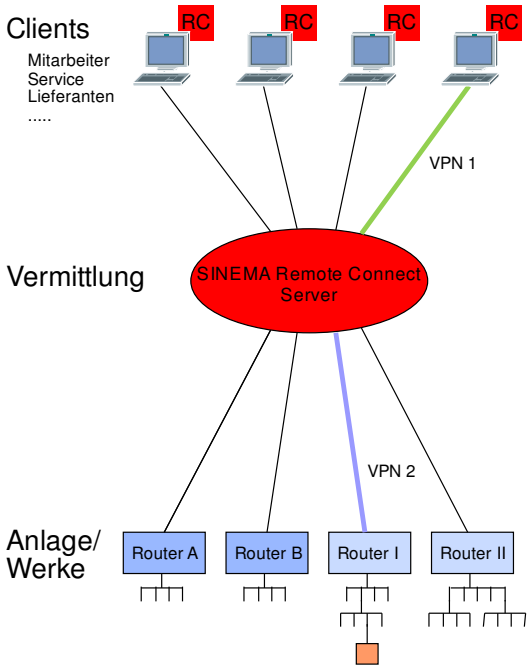
Fernwartung über SINEMA Remote Connect

Produktinformation

Version 1.1 / 15.04.2016



Herstelleradresse: Bolder automation GmbH
In den Klostergärten 9
D- 65549 Limburg

Telefon: +49-(0)6431-9848-0
Fax: +49-(0)6431-984828
email: info@bolder.eu

Versionsverwaltung: PI-Sinema_de_v1.1.docx

Doku Version	Sprache	Ausgabe Datum	Geräte Version	Ref.	Bemerkung
1.1	DE	15.4.2016	1.0	--	

1 Einleitung

Bolder automation nutzt das Produkt SINEMA Remote Connect der Firma Siemens, um eine sichere Internet-Kommunikation von autorisierten Nutzern zu Maschinen und Anlagen aufzubauen. Diese Verbindung kann den folgenden Aufgaben dienen.

- Überwachung der laufenden Produktion
- Diagnose von Betriebszuständen
- Fernwartung

SINEMA Remote Connect ist einsetzbar zwischen jeder Art von Nutzern (Clients) und Maschinen, Steuerungen oder Geräten, die über eine Ethernet-Schnittstelle verfügen und über einen Router angesprochen werden können.

2 Grundlegendes zu SINEMA Remote Connect

Ziel der Kommunikationsverbindung ist der Zugriff von einem beliebigen Ort der Welt auf ein Gerät an entfernter Stelle über das Internet. Der Schutz der Anlage und der Verbindung hat oberste Priorität.

Das Herzstück der Anwendung ist der **SINEMA Remote Connect Server**. Dieser stellt als Vermittler die Verbindung her zwischen den einzelnen maschinennahen Routern und entsprechenden autorisierten Nutzern. Die Verbindung zum Vermittlungsrechner wird von beiden Seiten über getrennte sichere VPN-Tunnel abgewickelt. Der Nutzer greift auf das Gerät zu, als würde er davor stehen. Ein Zugang zum Firmen-LAN ist durch den Tunnel nicht möglich.

Kommunikation	VPN-Tunnel 1	VPN-Tunnel 2	Beispiel 1 Webserver	Beispiel 2 Programmierung	Beispiel 3 Diagnose
Nutzer (Client)			PC mit Browser	PC mit Anwendung (TIA)	Smartphone mit App
Netzwerk			WLan	Ethernet Kabel	--
Gateway			DSL-Router (Fritzbox)	Mobilfunk	Mobilfunk
Internet			Internet	Internet	Internet
Vermittlung			**SINEMA Connect Server**	**SINEMA Connect Server**	**SINEMA Connect Server**
Internet			Internet	Internet	Internet
Firmengateway			DSL-Router	DSL Router	DSL Router
Netzwerk			Firmen-LAN	Firmen-LAN	Firmen-LAN
Router			Scalance S615	Scalance S615	Scalance S615
Netzwerk			LAN	LAN	WLAN
Gerät			S7-1200 Webserver	S7-1500	Smart home Überwachung

Die Sicherheit ist über die folgenden Mechanismen gewährleistet:

Clientsoftware: Über den VPN Client wird eine sichere Verbindung zum Vermittlungsrechner aufgebaut.

Vermittlungsrechner: Der Vermittlungsrechner ist das Herzstück der Kommunikation. Er verbindet nur bekannte Router mit angemeldeten Clients. Die beiden Verbindungen werden über zwei unterschiedliche VPN- Tunnel aufgebaut, die bei Anfrage miteinander gekoppelt werden.

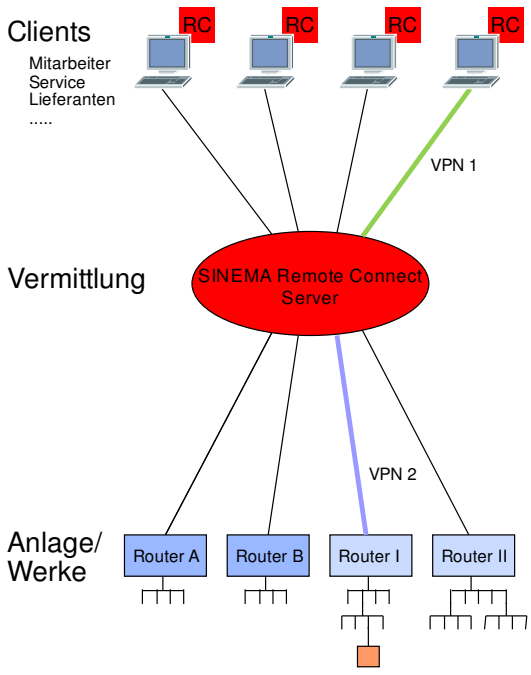
Scalance-Router: Der Router ist das definierte Ende der sicheren Verbindung. Der Router kann bei Bedarf abgeschaltet werden, um jede Kommunikation zu unterbinden. Der Router meldet sich selbstständig beim Vermittlungsrechner an, damit der Client die Verbindung auswählen kann.

Der Router verfügt über max. 5 Ethernet Ports, die konfiguriert werden können.

Da dieser Router auch Bestandteil eines Firmennetzes ist, lassen sich Regeln vereinbaren, die den allgemeinen Zugriff von innen nach außen und umgekehrt definieren.

Geräte Die einzelnen Geräte im abgesicherten Anlagennetz verfügen in der Regel über eigene Zugangsberechtigungen (Log-In), die nur den entsprechenden Teilnehmern bekannt sind.

Zusammenfassung Mit Hilfe von SINEMA Remote Connect kann über zwei VPN-Tunnel zwischen Client und Gerät eine sichere Verbindung aufgebaut werden. Der Client spricht nach dem Start der VPN-Verbindung das gewünschte Gerät an, als wäre er mit dem eigenen Netzwerk verbunden. Andererseits lässt der VPN-Tunnel keinen Zugang zu anderen Zielen der durchquerten Netze zu. Damit ist die Sicherheit des Firmennetzes gewährleistet.



3 Dienstleistungen von Bolder automation

3.1 Planung eines Remote Connect Konzepts

Die Sicherheit eines Netzwerkes, das über die Bürovernetzung hinaus bis an die Maschinen in der Produktion reicht, ist sorgfältig zu planen. An dieser Planung beteiligt sich die IT des Kunden, um den Zugang zum Internet oder die Einbindung von MES/ERP festzulegen.

Die Aufgaben sind:

- Festlegung der Netzwerk- Topologie
- Abgrenzung der Sicherheitszonen
- Definition der Zugangsregelung aus bzw. in die Produktionszelle
- Abklärung des Zugangs zu Geräten in der Produktionszelle
- Festlegung administrativer Regeln

3.2 Installation und Inbetriebnahme

Die Scalance Router werden auf der einen Seite in ein bestehendes Netz (Firmen LAN) integriert und auf der anderen Seite mit allen vorgesehenen Feldgeräten verbunden. Zu installieren sind:

- Verlegung des Netzwerks und Einbau von notwendigen Netzwerkgeräten.
- Anschluss und Einrichten aller Teilnehmer
- Einrichten des Scalance Routers inklusive der Tests

3.3 Betrieb des SINEMA Remote Connect Servers

Bolder automation betreibt den oben genannten Vermittlungsrechner und pflegt alle Benutzer. Dieser Rechner ist rund um die Uhr erreichbar. Zu den administrativen Aufgaben gehören:

- An- und Abmeldung von Zugangsberechtigungen aller Teilnehmern
- Dokumentation der Zugangsberechtigung und der angeschlossenen Geräte
- Pflege von Updates die von Siemens vorgegeben werden.

3.4 Pflege und Wartung

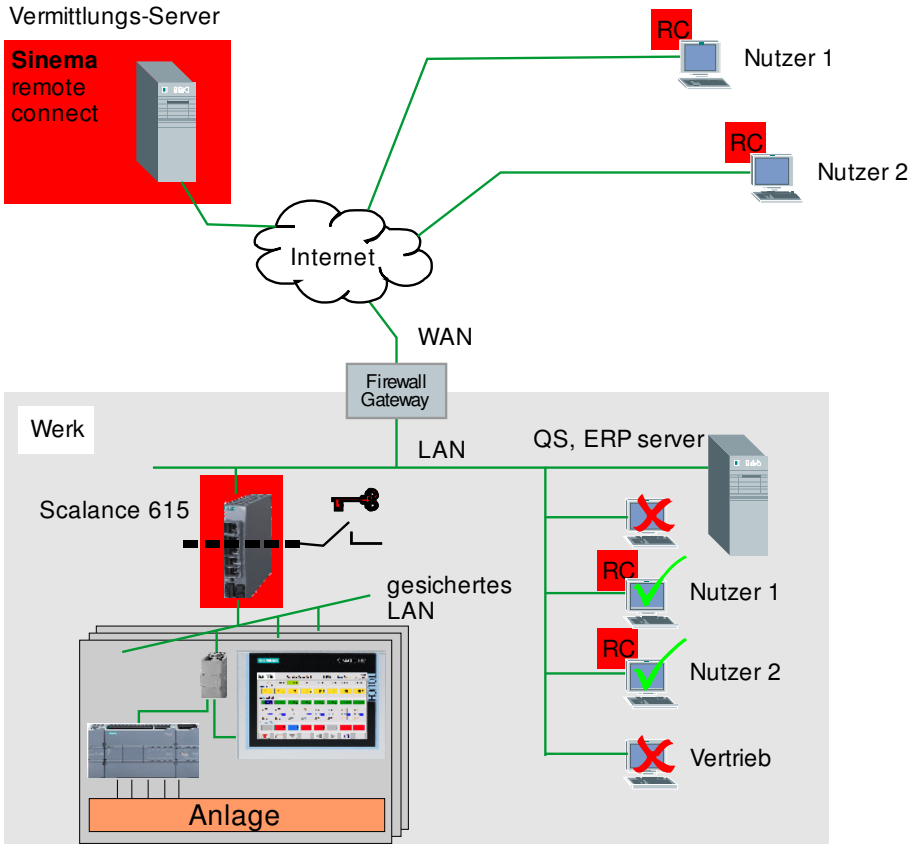
Die beim Kunden installierte Scalance Router müssen ebenfalls gepflegt werden. Hierzu gehören:

- Änderung von Regeln auf Anforderung
- Einspielen von vorgegebenen Updates
- Analyse von Störungen

Dies Arbeiten können in der Regel per Fernwartung ausgeführt werden.

4 Starter Paket

Mit dem Starter Paket lässt sich die für den betrieblichen Alltag notwendige Funktionalität für eine wirkungsvolle und sichere Fernwartung aufbauen. Weitere Anlagen und Nutzer können später ergänzt werden.



Der Lieferumfang schließt folgendes ein:

Aus dem Hause Siemens:

- 1x Scalance S615 LAN-Router mit einem Key-Plug SINEMA RC
- 2x SINEMA Remote Connect Client Lizenz

Aus dem Hause Bolder automation wird bereitgestellt:

- SINEMA Remote Connect Vermittlungs-Server für 365 Tage/24h
- Einrichten der Zugangsrechte der Nutzer 1 & 2 auf dem Vermittlungs-Server

Die Ersteinrichtung umfasst die folgenden weiteren Leistungen:

- Installation der Remote Connect Clients auf zwei PCs und Notebooks per Fernwartung
- Absprache mit der Firmen IT bezüglich der Portfreigabe auf dem Gateway/Firewall zum Internet.
- Einrichten des Scalance S615 LAN-Routers bezüglich abgesprochener Zugangsregeln
- Test der LAN und WAN-Verbindung

Der Einbau des Scalance S615 und die Vernetzung werden kundenseitig realisiert.

Bolder automation legt zur Abklärung und Projektierung die folgenden Unterlagen vor:

- Vorgaben zum ergänzenden Einrichten des Gateways und der Firewall (Zugang zum Internet)
- Formular für die Festlegung der Zugangsregeln zwischen LAN und Anlage
- Formular für die Festlegung der Zugangsregeln zwischen WAN und Anlage
- Formular zur Dokumentation angeschlossener Geräte im Anlagenbereich
- Schaltschema zur Installation des Scalance S615

Den Abschluss der Installation des Starter-Pakets dokumentiert ein Abnahmeprotokoll.

Für einen Zeitraum von 3 Monaten ab Abnahme ist der Betrieb des Vermittlungsrechner (SINEMA Remote Connect Servers) als Service im Starterpaket enthalten.

Nachfolgend bieten wir Ihnen gerne die sichere Einbindung weiterer Anlageteile oder den Zugriff durch weitere Nutzer an.

5 Allgemeines Leistungspaket

5.1 Konzeptphase

Die Erstellung eines Kommunikationskonzepts in schriftlicher Form regelt die Ausgestaltung der Lösung zwischen allen Beteiligten unter den Vorgaben der Geschäftsleitung des Kunden. Die Dokumentation dient weiterhin der Pflege der Installation.

5.1.1 Definition eines Subnetzes

Das Subnetz fasst alle Teilnehmer einer Produktionszelle zusammen, die in einem geschützten Bereich liegen. Eine Unterteilung der Produktion in Bereiche schützt soweit sinnvoll vor unberechtigten Zugriffen aus dem Intra- und Internet. Die Zuordnung von festen IP-Adressen schützt vor Konflikten zwischen den Bereichen.

					Zugang			
			Name	**IP-Adr.**	Abteilungsleiter	Instandh.	Maschinenherst.	Lieferant
Bereich			**Rohrproduktion**	192.168.10.x				
	Router		Scalance 615	192.168.10.1				
	Produktionseinheit A		Linie 11					
		Geräte 1	SPS	192.168.10.11			A	
		Geräte 2	Monitor	192.168.10.12				
		Geräte 3	Antrieb	192.168.10.13				
		Geräte 4	Temperierung	192.168.10.14				
		Geräte 5	Abzug	192.168.10.15				
		Geräte 6	Messtechnik	192.168.10.16				D
		Geräte 7	…					
	Produktionseinheit B		Linie 12					
		Geräte 1	SPS	192.168.10.21			B	
		Geräte 2	Monitor	192.168.10.22	Schmitz	Huber		
		Geräte 3	Antrieb	192.168.10.23				
		Geräte 4	Temperierung	192.168.10.24				
		Geräte 5	Abzug	192.168.10.25				
		Geräte 6	Messtechnik	192.168.10.26				D
		Geräte 7	…					
	Produktionseinheit C		Linie 13					
		Geräte 1	SPS	192.168.10.31				
		Geräte 2	Monitor	192.168.10.32				
		Geräte 3	Antrieb	192.168.10.33				
		Geräte 4	Temperierung	192.168.10.34				
		Geräte 5	Abzug	192.168.10.35				
		Geräte 6	Messtechnik	192.168.10.36				D
		Geräte 7	…					
Bereich			**Profilextrusion**	192.168.20.x				
	Router		Scalance 615	192.168.20.1				
	Produktionseinheit A		Linie 11					
		Geräte 1	SPS	192.168.20.11			C	
		Geräte 2	Monitor	192.168.20.12				
		Geräte 3	Antrieb	192.168.20.13				
		Geräte 4	…	192.168.20.14				
	Produktionseinheit B		Linie 12		Meyer	Huber		
		Geräte 1	SPS	192.168.20.21			C	
		Geräte 2	Monitor	192.168.20.22				
		Geräte 3	Antrieb	192.168.20.23				
		Geräte 4	…	192.168.20.24				
	Produktionseinheit C		Linie 13					
		Geräte 1	SPS	192.168.20.31			C	
		Geräte 2	Monitor	192.168.20.32				
		Geräte 3	…	192.168.20.33				

5.1.2 Konfiguration des Gateways zum Internet

5.1.2.1 Anbindung über das Firmennetzwerk

Typischerweise wird der Router in das Firmen-LAN integriert. Damit ist der Router einerseits über das Gateway mit der Firewall zum Internet verbunden und andererseits von den internen Client-PCs aus erreichbar. Das Gateway verwaltet den Verkehr in oder aus dem Internet. Hierfür sind Freigaben für die Dienste zu erteilen, die vom Router benötigt werden.

5.1.2.2 Direkte Anbindung an Internet

Für die direkte Anbindung an das Internet bieten sich Geräte aus der Scalance- Serien an.

G3- Router M874-3 über das Mobilfunkband G3 / GSM

G4- Router M876-5 über das Mobilfunkband G4 / LTE

DSL- Router Scalance S615 … über DSL

Eine Abstimmung mit der Firmen-IT betrifft nur die Bereitstellung eines DSL-Kanals.

Wenn eine Anbindung über Funk geplant wird, hat der Kunde den Mobilfunk-Provider zu beauftragen und eine SIM-Karte bereitzustellen.

5.1.3 Zugang aus dem Firmen-LAN auf den Router

Der Zugang aus dem Firmen-LAN auf den Router ist über das Gateway zu organisieren. Der Weg über den Remote Connect Server wird hierbei nicht beschritten.

5.2 Installation

Für die Installation des Routers wird ein Schaltschema bereitgestellt, das vom Betriebselektriker umgesetzt werden kann.

Die Installation umfasst:

- Stromversorgung 24V, 170mA (max. 2A) aus bestehender 24V-Versorgung oder mit zusätzlichem Netzteil
- Anschaltung an das Firmennetz
- Anschaltung an das Anlagennetz
- Schlüsselschalter bei Bedarf

5.3 Inbetriebnahme

5.3.1.1 Router

Auf Basis des Konzepts können der Router und das Gateway so konfiguriert werden, dass eine Verbindung zum Remote Connect Server nach dem Einschalten automatisch erfolgt. Damit ist sichergestellt, dass ein VPN-Tunnel bis zum Subnetz aufgebaut werden kann.

Wenn die Host-IPs auf den Geräten richtig eingerichtet sind, kann eine Verbindung aufgenommen werden. Alle anderen Änderungen können per Fernwartung ausgeführt werden.

5.3.1.2 Clients

Auf allen PCs und Laptops, die auf das Subnetz zugreifen sollen, müssen die Client-Software und der Lizenzschlüssel installiert werden. Die Siemens-Dokumentation beschreibt die notwendigen Schritte.

Auf Wunsch kann die Installation auch über einen Fernzugang per Teamviewer unterstützt werden.

5.3.1.3 Remote Connect Server

Auf Basis des Konzepts wird die Zugangsberechtigung individuell auf dem Remote Connect Server eingetragen damit Mitarbeiter auch von außen Zugriff erhalten und externer Service sich auf die Anlage schalten kann.

5.4 Schulung

Eine spezielle Schulung für die Nutzung des VPN-Tunnel ist nicht notwendig. Bevor eine Anwendung aus der Ferne gestartet wird hat lediglich der Aufruf der VPN Verbindung vom Client aus zu erfolgen. Bei Bedarf kann man diesen Vorgang per Teamviewer unterstützen.

5.5 Pflege

Die Pflege der Installation garantiert die Sicherheit und Funktionsfähigkeit. In diese Aufgabe sind Kunden und Bolder automation gleichermaßen verantwortlich eingebunden. Sinnvoll wäre die folgende Absprache:

Die Kunden-IT ist verantwortlich für:

- Pflege der IP-Adressen der Subnetze
- Pflege der Gateway Konfiguration

Die Geschäftsleitung des Kunden gibt bekannt:

- Wer erhält Zugang zu welchem Subnetz: (Mitarbeiter/ Externer)
- Wem wird der Zugang gesperrt (Mitarbeiter/ Externer) und ab wann.

Bolder automation ist verantwortlich für:

- Betrieb und Pflege des Remote Connect Servers
- Vermittlung notwendiger Updates und Abstimmung der Umsetzung
- Jährlicher Bericht über die Zugangsberechtigungen

6 Weitere Leistungen

6.1 Service zum Vermittlungsrechner

Der Vermittlungsrechner (SINEMA Remote Connect Server) ist das Rückgrat der sicheren Kommunikation und der Drehpunkt für die Systempflege. Für die Bereitstellung dieser Einheit ist für jeden Scalance-Router ein Servicevertrag für ein Kalenderjahr abzuschließen.

6.2 Pflege der Konfiguration

Bestehende Anlagen-Konfigurationen können geändert oder erweitert werden bei:

- Ausbau der Anlagentechnik
- Integration von weiteren Geräten an der Kommunikation
- Erweiterung des Nutzerkreises, interner oder externer Teilnehmer

Alle diese Wünsche können im Rahmen unserer Technik umgesetzt werden. Hierzu wird jeweils ein Angebot erstellt und der Aufwand nach Zeit berechnet. In der Regel lassen sich alle Änderungen per Fernwartung administrieren.

6.3 Dokumentation

Bei Auslieferung, später nach Änderungen oder jederzeit auf Wunsch werden alle Verbindungen und Teilnehmer dokumentiert.

Ein Verbindungsnachweis wird nicht angeboten.

6.4 Abstimmung zum Nutzerkreis

Bei der Pflege des Vermittlungsrechners ist es für Bolder automation wichtig zu erfahren, wer als Nutzer gelöscht werden soll. Dies kann ausscheidende Mitarbeiter genauso betreffen wie Lieferanten, denen der Zugang zur Fernwartung gesperrt wird.