SIEMENS

Fachartikel

Gesicherter Fernzugriff für PROFIBUS-/MPI-Anlagen im Brownfield

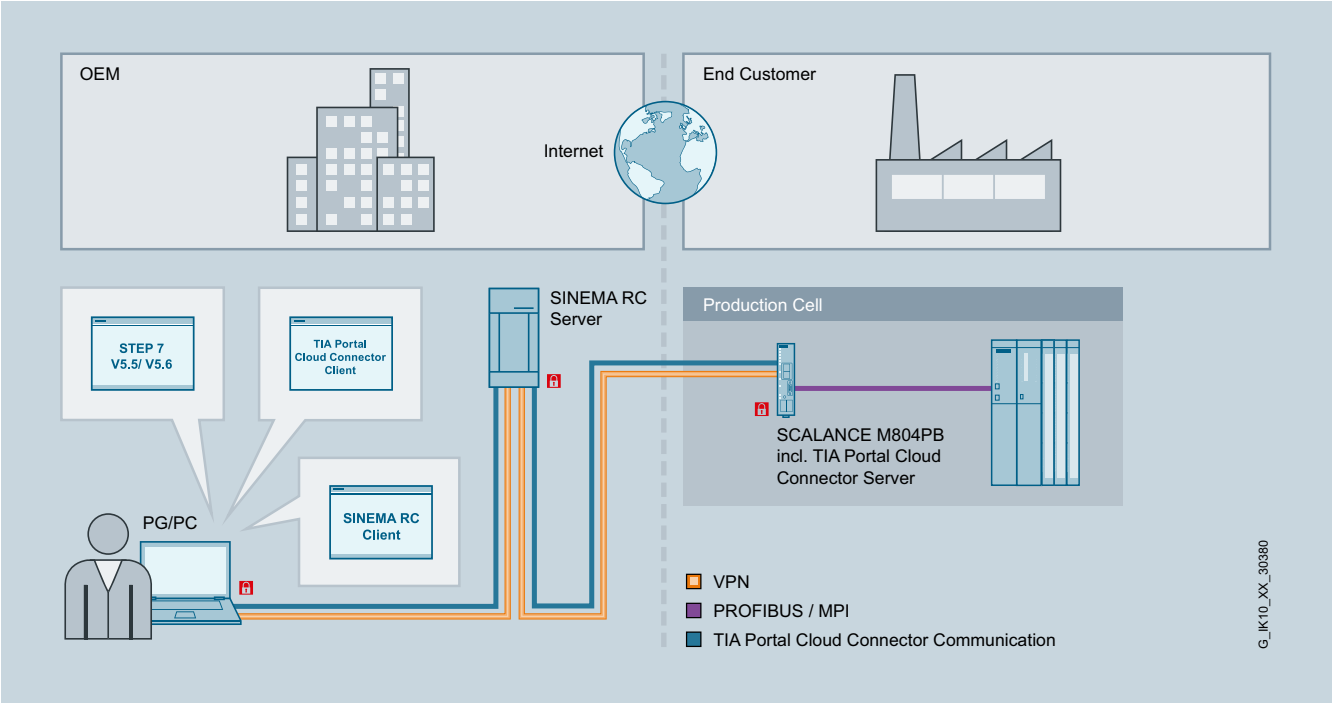
Mit zunehmender Digitalisierung bereits bestehender Anlagen wachsen die Anforderungen an industrielle Sicherheit und den Schutz firmenvertraulicher Daten im Rahmen von Remote Services. Vor allem im Brownfield – also bei der Modernisierung von Bestandsanlagen – gibt es besondere Herausforderungen bei der Anbindung (Fernzugriff/Konfiguration) von PROFIBUS-Anlagen an moderne IP-Netzwerke.

Soll gesicherter Fernzugriff nun direkt auf eine PROFIBUS-/MPI-fähige Steuerung (Konfiguration der dahinter liegenden Teilnehmer) im Netzwerk erfolgen, bietet sich zum einen ein zentrales Konzept an, das von allen Zellen auf die gleiche Art und Weise genutzt werden kann, andererseits benötigt man aber auch ein entsprechendes MPI-Interface. Der Fernzugriff erfolgt dabei stets unter der Vorgabe, dass die Anlagen den Verbindungsaufbau bei Bedarf lokal initiieren und die Verbindung „von innen nach außen“ aufgebaut wird. Damit können grundlegende Anforderungen an die Fernwartung und Konfiguration von PROFIBUS-Zellen in einer Bestandsanlage abgeleitet werden (jetzt neben Ethernet auch mittels PROFIBUS/MPI).

Im Fall einer reinen Anbindung mittels MPI, aber auch bei gemischten Anlagenkonzepten (Erweiterung/Modernisierung mit zum Beispiel SIMATIC S7-1500) sollen durchgängig IP-Router mit Firewall und VPN-Technologie eingesetzt werden. Dadurch kann man ein übergeordnetes Managementsystem für Remote Networks aufsetzen, das sowohl die MPI-Teilnehmer, als auch die Ethernet-Teilnehmer zentral in einer Instanz verwaltet. Der Servicetechniker, der die Zelle zur Wartung erreichen möchte, kann innerhalb kurzer Zeit verschiedene Zellen nacheinander oder – im Fall von Ethernet-Teilnehmern – auch gleichzeitig erreichen. Dabei ist es entscheidend, dass dies ohne großen Aufwand und IT-Fachkenntnisse möglich ist.

Keine Rolle spielt hingegen, ob es sich um MPI- oder Ethernet-Teilnehmer handelt, da beide über die zentrale Managementplattform zuverlässig und gesichert erreicht werden können.

www.siemens.de/remote-networks



Gesicherter Fernzugriff mit SCALANCE M804PB

Der Servicetechniker benötigt also ein einfaches Werkzeug, mithilfe dessen er die Fernwartungs-Endpunkte (Automatisierungszelle im Netzwerk) erreichen kann. Da sich die Zellen zentral an einer Plattform melden, ist es also naheliegend, dass der Servicetechniker diese zentrale Stelle ebenfalls bei Bedarf erreichen kann.
Bei der Wahl der Verschlüsselungstechnologie für den Verbindungsaufbau ist zu beachten, dass sie entsprechend einfach und flexibel an die unterschiedlichen Bedürfnisse der industriellen Netzwerke anpassbar, aber dennoch sicher sein muss. Es bieten sich zum Beispiel Zertifikat-basierte Mechanismen auf der Basis von OpenVPN oder auch IPsec an.

Die Themen Zugriffskontrolle, Authentisierung und Autorisierung sind sowohl bei Bestandsanlagen, aber auch bei den neuen Anlagenteilen kritischer zu betrachten als im täglichen Büroalltag. So bietet es sich an, genau zu analysieren, wer zu welchem Zeitpunkt mit welchem Teilnehmer verbunden sein darf und welche Berechtigungen er dort besitzt. Daraus lässt sich die Planung von beispielsweise Firewall-Regeln, Benutzer- und Gerätegruppen sowie deren Kommunikationsbeziehungen zueinander ableiten.

Mit SINEMA Remote Connect von Siemens können Anwender weit verteilte Anlagen oder Maschinen über Fernzugriff komfortabel und gesichert warten.

Zugriff auf MPI-Anlagen im Feld

Wie einleitend erwähnt, ist eine der Herausforderungen für Maschinenbauer, auch ältere Maschinen und Anlagen, die noch mit MPI aufgebaut sind, über Fernzugriff zu erreichen. Die Verwaltung der Zugangspunkte zu den Anlagen für den Fernzugriff erfolgt zentral im SINEMA Remote Connect Server.

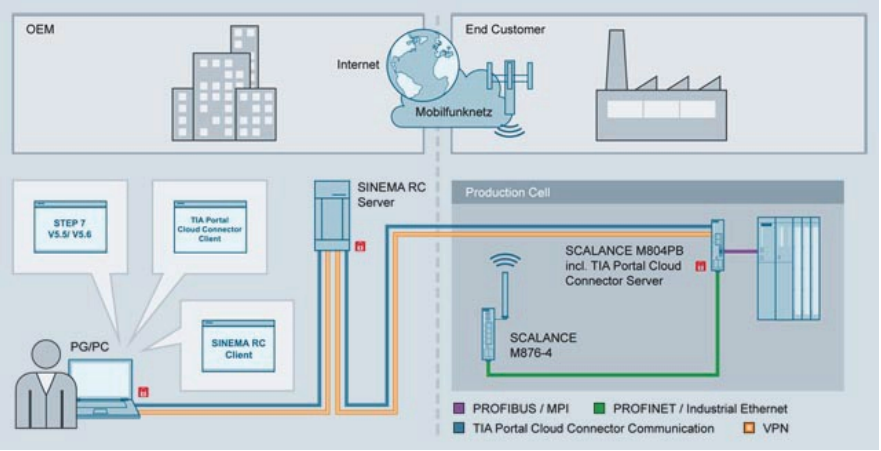
Über den SINEMA Remote Connect Client können diese MPI-Anlagen direkt ausgewählt und verbunden werden. Sobald die Tunnel von der Anlagenseite zum Server und vom Client-PC zum Server aufgebaut sind, kann über das TIA-Portal auf die hinter dem Router gelegenen PROFIBUS-/MPI-Teilnehmer zugegriffen werden. Über diese Technologie erfolgt der Zugriff aus Anwendersicht genau so, als wäre der Techniker lokal vor Ort auf der Anlage mit dem MPI-Netzwerk verbunden.

Dezentrale Projektverwaltung

Im Fernzugriffsfall kann das benötigte Engineering-Tool TIA Portal entweder lokal auf dem Client-Rechner des Servicetechnikers ausgeführt werden, oder über die in den Router integrierte Funktionalität des TIA Portal Cloud Connectors von einem zentralen Service Center über das Netzwerk oder das Internet abgerufen werden. Durch die Verwendung von SINEMA Remote Connect ist sowohl der Zugriff des Servicetechnikers auf das TIA Portal als auch der Verbindungsaufbau des Routers aus der Anlage heraus durchgängig über einen verschlüsselten VPN-Tunnel gesichert.

Stets den Überblick und die Kontrolle behalten

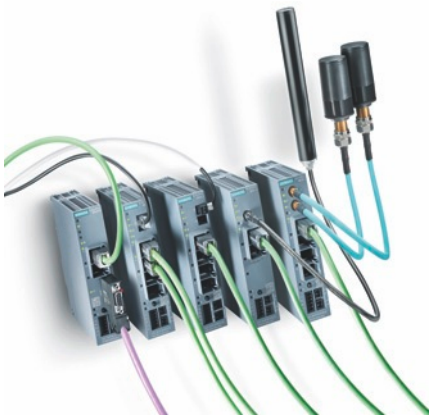
Die zentrale Managementplattform sorgt durch die Möglichkeit der zentralen Nutzer- und Geräteverwaltung für Transparenz und Übersichtlichkeit der Geräte und Nutzer. Die Kontrolle über den tatsächlichen Verbindungsaufbau zur Anlage kann bei Bedarf voll in die Verantwortung des Anlagenbetreibers vor Ort übergeben werden.
Hierbei kann der Betreiber die Möglichkeiten des Routers nutzen, den Aufbau des VPN-Tunnels nur nach Anforderung über einen lokalen Schlüsselschalter (digitaler Eingang) zu ermöglichen. Dadurch ist der Initiator stets auf der Anlagenseite.



Gesicherter Fernzugriff mit SCALANCE M804PB, STEP 7 und TIA Portal Cloud Connector.

Einfach, transparent, gesichert

Die Dezentralisierung von Produktionsstätten sowie der schnelle und gesicherte Zugriff auf Bestands- und neue Anlagen ist für Unternehmen eine wichtige Maßnahme, um im globalen Wettbewerb Markanteile zu sichern. Daher wird der Bedarf an einfachen – aber zugleich immer performanteren – Fernzugriffsmechanismen weiter steigen. Der Industrie-Router SCALANCE M804PB bildet die robuste Grundlage für das Fernzugriffsnetzwerk in Verbindung mit PROFIBUS-/MPI-Anlagen. Moderne Security-Mechanismen wie Firewall, IPsec und OpenVPN gehören dabei zu den etablierten Lösungen von Siemens.



Gesicherte Fernzugriffslösung aus einer Hand

Die Basis für einen funktionalen und gesicherten Fernzugriff ist ein professionelles industrielles Kommunikationsnetzwerk. Der Aufbau und die Pflege solcher Kommunikationsnetzwerke erfordert Erfahrung und umfassendes Anwendungs-Know-how.

Als Teil der Automatisierung werden industrielle Netzwerke immer von der Applikation ausgehend gestaltet. Deshalb empfiehlt es sich, in Sachen industrieller Netzwerke auf Partner zu setzen, die maßgeschneiderte und genau auf die jeweiligen Anforderungen zugeschnittene Netzwerk- und Remote-Konzepte entwickeln und umsetzen können.

Siemens als Partner der Industrie bietet ein zukunftsfähiges, umfassendes Portfolio an Netzwerkkomponenten. Darüber hinaus profitieren die Kunden von Professional-Services, die auf der langjährigen Erfahrung von Siemens aufsetzen, industrielle Netzwerke zu konzeptionieren, zu planen, zu implementieren und verantwortliche Mitarbeiter für den Betrieb der Netzwerke zu schulen und zu zertifizieren.

Securityhinweise

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts. Weitergehende Informationen über Industrial Security finden Sie unter **http://www.siemens.com/industrialsecurity**

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

PDF
Fachartikel
FAV-79-2018-PD-PA
BR 0318 / 3 De
Produced in Germany

www.siemens.de/remote-networks