SIEMENS

Fachartikel

Fernzugriffsnetzwerke in IT oder OT

Fernzugriff mit Managementplattform für Remote Networks über Sprungserver und Private Cloud

Die Anforderungen an industrielle Sicherheit und den Schutz firmenvertraulicher Daten wächst kontinuierlich.

IT-Abteilungen und IT-Dienstleister übernehmen in Unternehmen immer öfter auch Aufgaben zur Absicherung des Fernzugriffs auf Anlagen und Maschinen für die Erbringung von Fernwartungs-Dienstleistungen durch Dritte. Hierbei gibt es spezielle Anforderungen bezüglich des Standorts und der Verantwortlichkeiten für den Server – von Hosting in der Unternehmens-IT bis zu Private-Cloud-Lösungen als Managed Service.

Die Anforderungen an einfache und gesicherte Fernwartungskonzepte wachsen weiter mit der steigenden Nachfrage nach Fernzugriffslösungen zur Erbringung von Remote Service Dienstleistungen im industriellen Umfeld.

IT-Infrastrukturen bei den Unternehmen wachsen zunehmend zusammen und Grenzen zwischen IT und OT werden in beide Richtungen je nach Anforderungslage verschoben.

Hier ergeben sich unterschiedliche Lösungsansätze und Angebote am Markt, um auf die verschiedenen Anforderungen einzugehen.

Im Vordergrund steht stets der Erhalt der Produktivität der Anlage. Dazu bedarf es von Zeit zu Zeit einer Wartung, die in diesem Fall über die Ferne erfolgen soll. Allerdings darf die Produktivität der Anlage nicht unter sporadischen Fernzugriffen leiden. Folglich müssen diese Fernzugriffe geplant und zuverlässig ausgeführt werden können.

Hierzu eignet sich also ein Konzept, in dem die Automatisierungszelle bei Bedarf und Verfügbarkeit in einen Fernwartungsmodus versetzt wird. Ist die Anlage nicht in dieser Betriebsart, kann und darf also kein Zugriff aus der Ferne erfolgen. Es empfiehlt sich, die Zelle so auszustatten, dass sie im Wartungsmodus die Verbindung initiiert – idealerweise zu einem vertrauenswürdigen und verfügbaren Partner.

Soll dies nun für eine Vielzahl von Zellen im Netzwerk erfolgen, bietet sich ein zentrales Konzept an, welches von allen Zellen auf die gleiche Art und Weise genutzt werden kann.

Auf der anderen, der zentralen Seite bietet sich dadurch die Möglichkeit, die entgegenzunehmenden Verbindungen zentral zu verwalten.

Der Servicetechniker, welcher die Zelle zur Wartung erreichen möchte, soll innerhalb kurzer Zeit verschiedene Zellen nacheinander oder gleichzeitig erreichen können. Dabei spielt es eine entscheidende Rolle, dass dies ohne großen Aufwand und IT-Fachkenntnisse möglich ist. Der Servicetechniker benötigt also ein einfaches Werkzeug, über welches er die Fernwartungs-Endpunkte (Automatisierungszelle im Netzwerk) erreichen kann. Da sich die Zellen zentral an einer Plattform melden (s.o.) ist es also naheliegend, dass der Servicetechniker diese Zentrale stelle ebenfalls bei Bedarf erreichen kann.

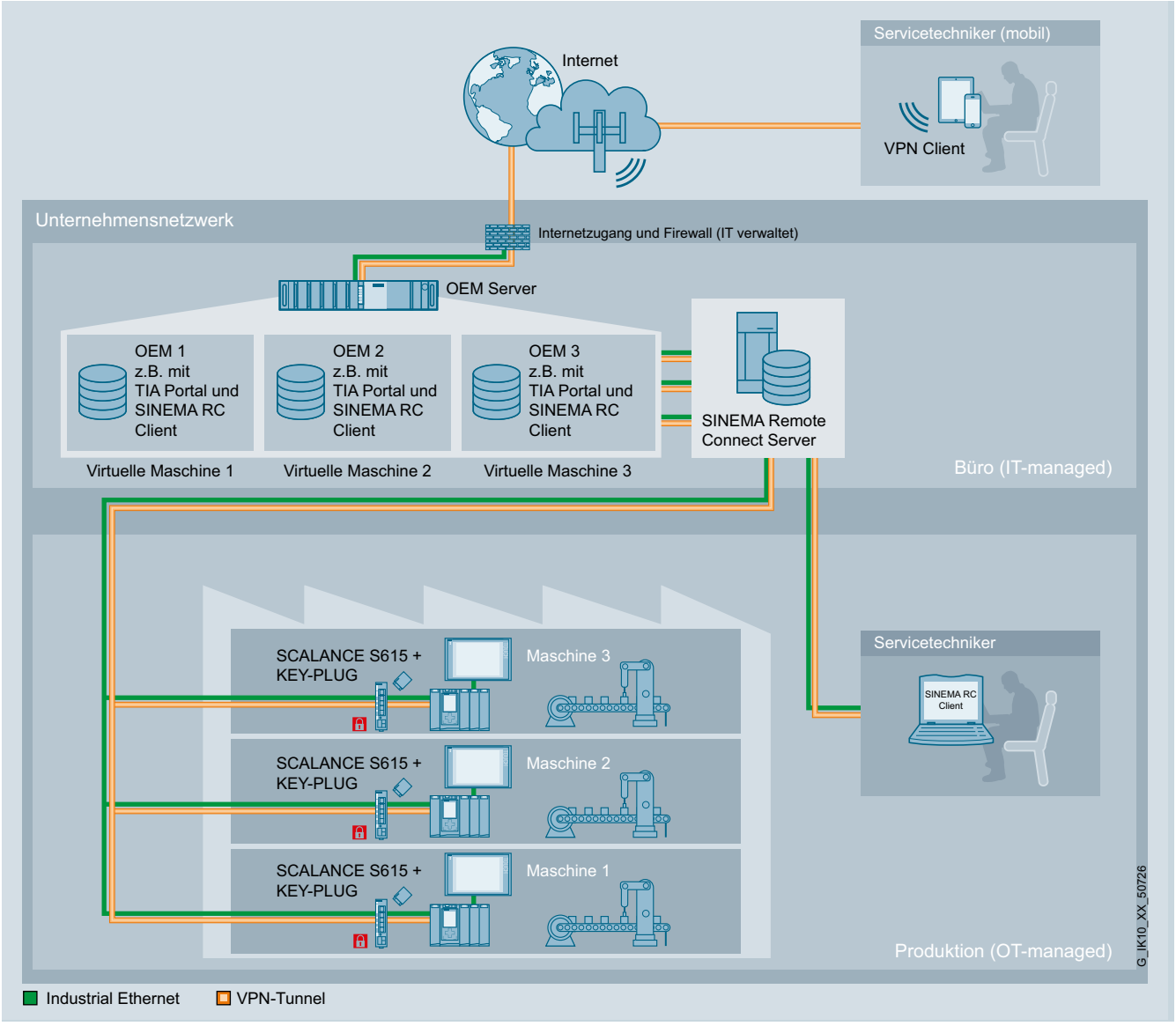
Für die Umsetzung dieses Konzepts, das auch als „Rendezvous Server" bezeichnet wird, muss die zentrale Managementplattform entsprechend der Security-Richtlinien der Unternehmen umgesetzt werden können. Dies schließt häufig cloud-gehosteted Lösungen auf fremden Servern aus.

Fernzugriff – aber bitte sicher und über meine IT!

Als führender Anbieter von Automatisierungs- und Netzwerkkomponenten für die Industrie hat Siemens stets die gesamte Sicht auf die Bedürfnisse der Anwender.

Neben den Geräten bietet Siemens auch Beratungsdienstleitungen und Services rund um das Kundennetzwerk und IT-Security an – und das weltweit. Stand der Technik bei Fernzugriffslösungen sind Systeme auf Basis zentraler Server, die Tunnelverbindungen von Maschinen und Servicepersonal entgegennehmen und je nach Berechtigung zusammenschalten. Dadurch kann eine der Kernanforderung des BSI (Bundesamt für Sicherheit in der Informationstechnik) an industrielle Fernzugriffsnetzwerke erfüllt werden: Ausgehende Verbindungen von den Anlagen, um die volle Kontrolle über Verbindungen nach außen lokal zu ermöglichen.

In nachfolgenden Beispielen wird verdeutlicht, wie ein solches Server-basiertes System - die Managementplattform für Remote Networks (SINEMA Remote Connect) – in Szenarien zum Einsatz kommen kann, bei denen der Endkunde ein Hosting außerhalb seines Einflussbereiches (Firmennetzwerks) nicht gestattet.



Fernzugriff – Zentraler Server in der Verantwortung der Unternehmens-IT

Im ersten Fall bietet die IT des Betreibers dem Servicetechniker einen Zugang über Remote Desktop auf einen Rechner, der in der Verantwortung der Betreiber-IT steht. Auf diesem Sprungrechner („jump-host") stellt der Betreiber dem Servicetechniker alle für den Wartungsfall benötigten Tools zur Verfügung (z.Bsp. TIA-Portal und TIA-Projekte).

Dadurch unterbindet die IT, dass ggf. unsichere Servicelaptops dazu führen, dass infizierte Daten in das Firmennetzwerk gelangen.

Beispiel für den Servicefall

Der Zugriff erfolgt über einen vorgelagerten Rechner im Firmen-Intranet, auf den sich die OEMs / Servicetechniker über von ihrer Office bereit gestellte Tools (Remote Desktop Anwendung) einwählen.

Ab dann sind sie im sicheren Bereich ihres Unternehmensnetzwerks und können über die Client-Applikation (SINEMA Remote Connect Client) auf dem vorgelagerten Rechner über das Intranet statt über das Internet auf den ebenfalls beim Betreiber im IT-Netzwerk gehosteten SINEMA Remote Connect Server zugreifen.

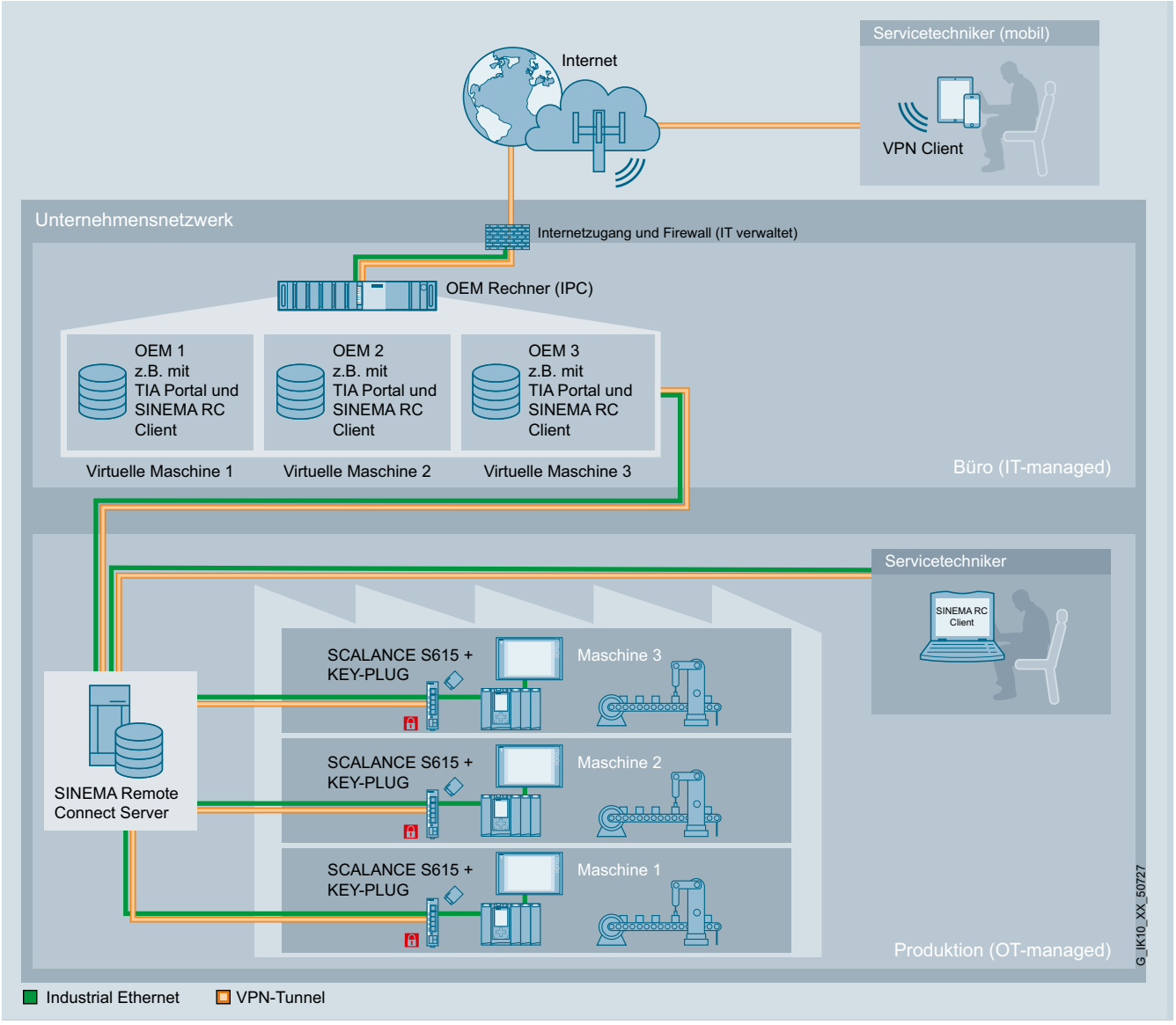
Ein weiteres Szenario ist, dass die Verantwortung des zentralen Fernwartungsservers (SINEMA Remote Connect) nicht in der IT, sondern im Fabriknetz des Kunden liegt.

Dies wird beispielsweise von Kunden gefordert, die aufgrund von Anforderungen an kurze Reaktionszeiten auf Veränderungen (User, Berechtigungen, Anlagen, ...) die Verwaltung des Servers selbst in der Hand haben wollen – ohne dabei von IT-Prozessen abhängig zu sein.

Das Grundkonzept ist wie bei dem zuvor beschriebenen Beispiel mit dem Sprungrechner, nur wird nun der SINEMA Remote Connect im Fabriknetzwerk betrieben.

Die Verwaltung der Remote Desktop Verbindungen von außen, sowie der dazu gehörigen, vorgelagerten Rechner liegt weiterhin bei der IT des Betreibers.

Interne Service-Techniker, die über das Factory-Intranet Zugriff auf den SINEMA Remote Connect haben, sind somit von der IT unabhängig.



Fernzugriff – Zentraler Server in der Verantwortung der Produktions-IT (OT)

Managed Services

Mit dem Angebot des „Managed Services“ bietet Siemens ein Komplettsystem basierend auf Server-Hardware, der quasi als „private cloud“ beim Kunden vor Ort eingesetzt werden.

Bestandteil des Angebotes ist neben der Hardware, Virtualisierungsumgebung und den bereits vorinstallierten virtuellen Maschinen für SINEMA Remote Connect sowie ein Windows-Betriebssystem, auf dem beispielsweise neben dem SINEMA Remote Connect Client ein TIA-Portal installiert sein kann.

Frei konfigurierbar nach den Bedürfnissen des Kunden steht somit ein Komplettsystem zur Verfügung, über welches der Kunde seinen Service abwickeln kann. Er benötigt lediglich die bereits dargestellten SCALANCE Router im Feld sowie die Möglichkeit, dass seine Servicetechniker remote Zugriff auf die virtuelle Maschine mit dem SINEMA Remote Connect Client (beispielsweise über eigene IT Lösung (VNC, Remote Desktop, ...).

Um den Betrieb der „private cloud“ kümmert sich in diesem Szenario Siemens – die Service-Ingenieure von Siemens haben selbst einen getrennten Remote-Zugang auf die Hardware und virtuelle Umgebung der „private-cloud“, um diese im Betrieb zu warten, bei der Optimierung, Erweiterung und ggf. Fehlerbehebung zu unterstützen. Stets getrennt von den Daten des Kunden, und ohne Zugriffsmöglichkeit auf die Anlagen des Kunden.

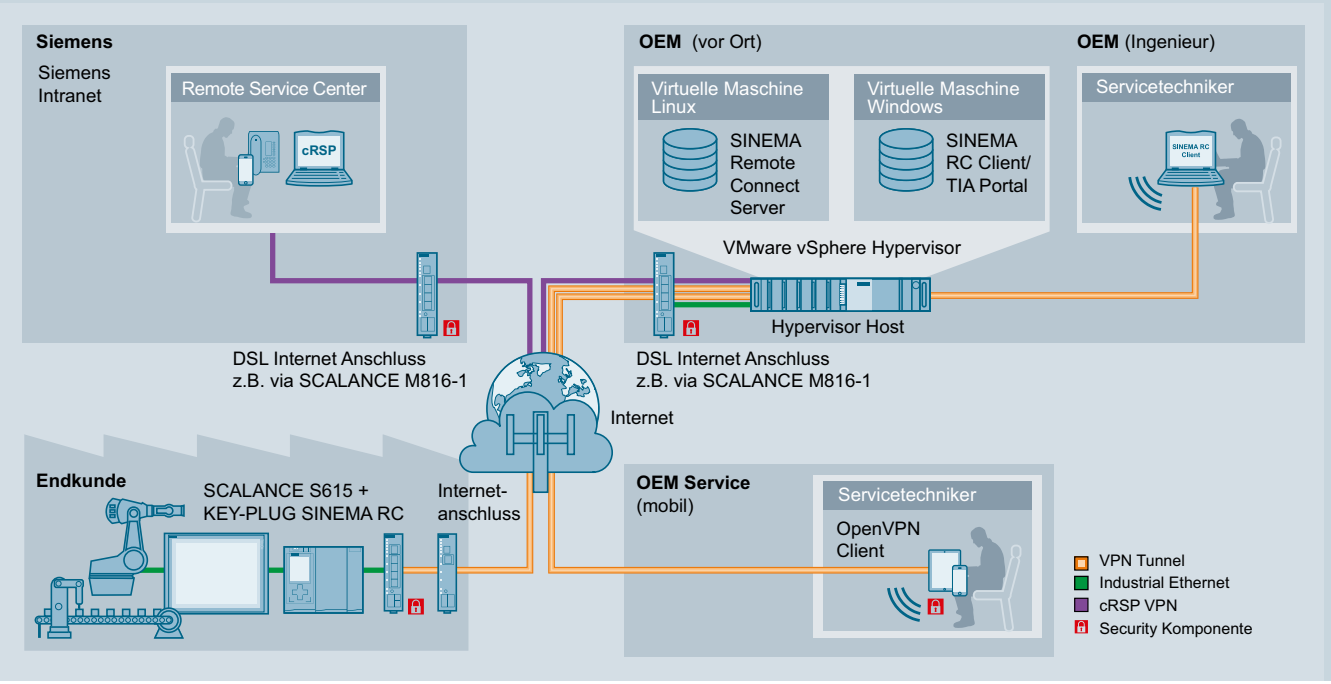
Eine rundum sichere Lösung, mit der die Kunden ihre Daten jederzeit im Griff (und entsprechend des Bedarfs innerhalb ihrer eigenen Firma!) haben, sich aber um Wartung und Betrieb der unterschiedlichen Treiber, Betriebssysteme und Software nicht zu kümmern braucht.

Einfach, transparent, gesichert

Die Dezentralisierung von Produktionsstätten und der schnelle wie auch gesicherte Zugriff auf diese ist für Unternehmen auch in Zukunft eine wichtige Maßnahme, um im globalen Wettbewerb Markanteile zu sichern, beziehungsweise auszubauen. Daher wird der Bedarf an immer performanteren Fernzugriffsszenarien weiter steigen.

Die Industrie-Router SCALANCE M-800 und SCALANCE S615 bilden die robuste Grundlage für das Fernzugriffsnetzwerk. Moderne Security-Mechanismen wie Firewall, IPsec und OpenVPN gehören ebenso wie die neuesten Mobilfunkstandards bis 4G (LTE) zu heutigen Lösungen aus dem Hause Siemens.

Abgerundet wird die Fernzugriffslösung durch SINEMA Remote Connect, der Managementplattform für Remote Networks. IP-basierter, transparenter Fernzugriff – einfach, gesichert – jederzeit und nahezu überall – mit SINEMA Remote Connect und SCALANCE-Industrie-Routern. Abgerundet wird die Fernzugriffslösung durch SINEMA Remote Connect, der Managementplattform für Remote Networks. IP-basierter, transparenter Fernzugriff – einfach, gesichert – jederzeit und nahezu überall – mit SINEMA Remote Connect und SCALANCE-Industrie-Routern



Fernzugriff – Zentraler Server als managed appliance (private cloud)

SCALANCE M –
Sicher. Flexibel. Grenzenlos.

Die Geräte sind im gängigen Industriedesign der Steuerung SIMATIC S7-1500 mit entsprechenden Aufnahmen für die Schienen der 300er/1500er-Serie sowie der 35-mm-DIN-Hutschiene ausgestattet.

Weiter ist der Temperaturbereich und die Anforderungen an die Spannungsversorgung und die digitalen Ein-Ausgänge an die SIMATIC-Automatisierungswelt angepasst – und erfüllt damit einen der höchsten Industriestandards am internationalen Markt.

Über ein weites Zubehörportfolio an Antennen und Kabel, sowie entsprechende Schaltschrankdurchführungen und Blitzschutzelemente sind auch die Mobilfunkgeräte einfach im Schaltschrank zu montieren und die zum Teil spritzwassergeschützten- und staubdichten (IP65) Antennen flexibel an der für einen sicheren Mobilfunkempfang besten Stelle zu installieren.

Aber auch in entlegenen Gebieten kann der Verbindungsaufbau von einem Mobilfunkrouter der Produktlinie SCALANCE M-800 aktiv angestoßen werden. Durch die integrierte SMS-Funktion ist es möglich, über den SINEMA Remote Connect den Versand einer „wake-up"-SMS an das Mobilfunkgerät anzustoßen.

Vorteile im Überblick

SINEMA Remote Connect, Managed Appliance und SCALANCE M

- **Erhöhte Anlagenflexibilität und Kosteneinsparung**
  - Fernzugriff verkürzt die Reaktionszeiten und reduziert die Kosten für Wartung und Service.
- **Investitionsschutz bestehender Anlagen**
  - Verbindung bestehender Anlagen, Anbindung neuer Anlagen – zukunftssichere Lösungen aus einer Hand.
- **Investitionsschutz zukünftiger Anlagen**
  - Zukunftssichere Technologien und kontinuierlicher Ausbau verfügbarer Produkte mit durchgängiger Kompatibilität.
  - Innovative Technologien, speziell für die Aufgaben im industriellen Umfeld.
- **Optimale Maschinen- und Anlagenverfügbarkeit**
  - Höchste Zuverlässigkeit der Produkte im Betrieb.
  - Darüber hinaus Service und Support rund um die Uhr (24/7), weltweit.
- **Planungssicherheit und Know-how-Schutz**
  - Lange Produktlebenszeit und Verfügbarkeit sichern langfristig angelegte Anlagenkonzepte und die Nutzung des Know-hows der Mitarbeiter.
- **Kompatibilität**
  - Durchgängige Produkte und Zubehör für die komplette industrielle Infrastruktur – vom Key-Plug über die Router bis zur Managementplattform
- **Weltweiter Einsatz**
  - Mobilfunkrouter mit Funkzulassungen für mehr als 50 Länder weltweit.
- Unsere Entwicklungsprozesse berücksichtigen schon bei der Planung spätere Anwendungen und Lösungen. Damit sind unsere Produkte stets leicht zu integrieren und auf die Bedürfnisse der Anwender und Endkunden zugeschnitten.
- **Produktqualität "Made in Germany"**
  - Entwicklung und Produktion an deutschen Standorten (Karlsruhe/Nürnberg). Deshalb geben wir fünf Jahre Gewährleistung auf die Geräte.

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-21-2017-PD-PA
BR 0617 / 5 De
Produced in Germany

siemens.de/remote-networks