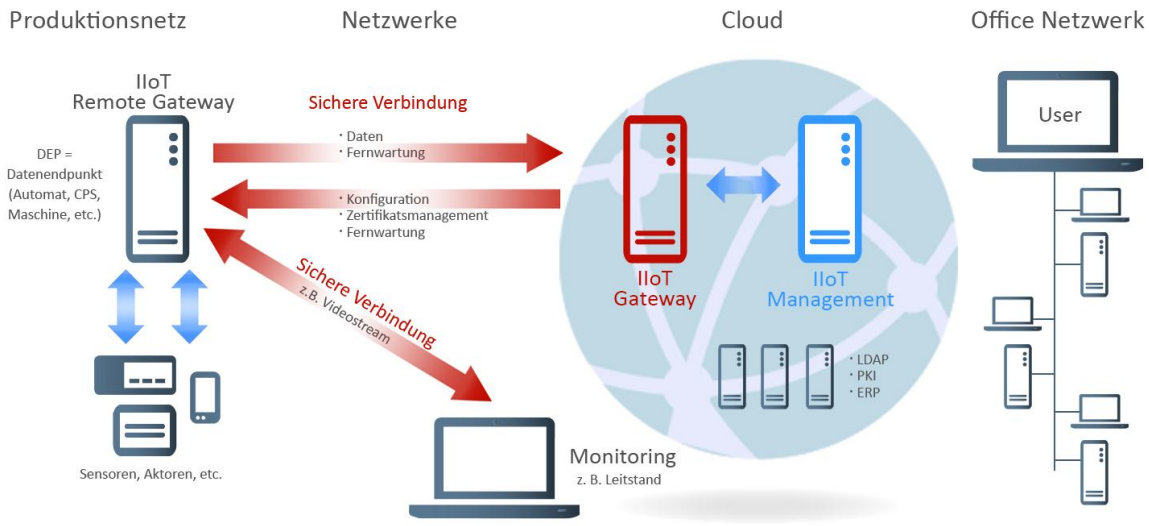
Security für das Industrial Internet of Things

In Zeiten, in denen jeder ständig und überall online ist, seinen Status preis gibt und auch Geldgeschäfte mobil getätigt werden, vergisst man gerne den Nutzungskomfort ausreichend abzusichern bzw. die möglichen Risiken. Dies gilt sowohl im privaten als auch im geschäftlichen Umfeld.
Kaum haben wir uns an diese Lebensweise gewöhnt, steht nun der nächste Schritt an, das **I**ndustrial **I**nternet **o**f **T**hings (IIoT) – alles wird miteinander vernetzt, wirklich alles.

Wie war es noch vor Jahren: Eine Industrieanlage mit Ihren Fertigungsstraßen und Steuerungen wurde vor Ort von Fachpersonal gewartet und betreut. Der informationstechnische Kontakt zur Außenwelt war nicht direkt vorhanden. Der Mensch agierte in diesem Umfeld als die natürliche Barriere, die Firewall zum Schutz vor schädlichen Einflüssen. Fernwartung mit Standleitungen kam später hinzu und schließlich der Zugriff von extern über das Internet. Spätestens seit diesem Zeitpunkt potenzierte sich das Risiko. Angriffe auf eine Industrieanlage können von überall auf der Welt erfolgen – geschützt durch Anonymität und rechtsfreien Raum. Angriffe in Form von Distributed Denial of Service Attacks (DDoS) oder das Ausspähen von Sicherheitslücken und das anschließende Einbringen von Schadsoftware sind fast an der Tagesordnung.



Übersicht einer IIoT Infrastruktur

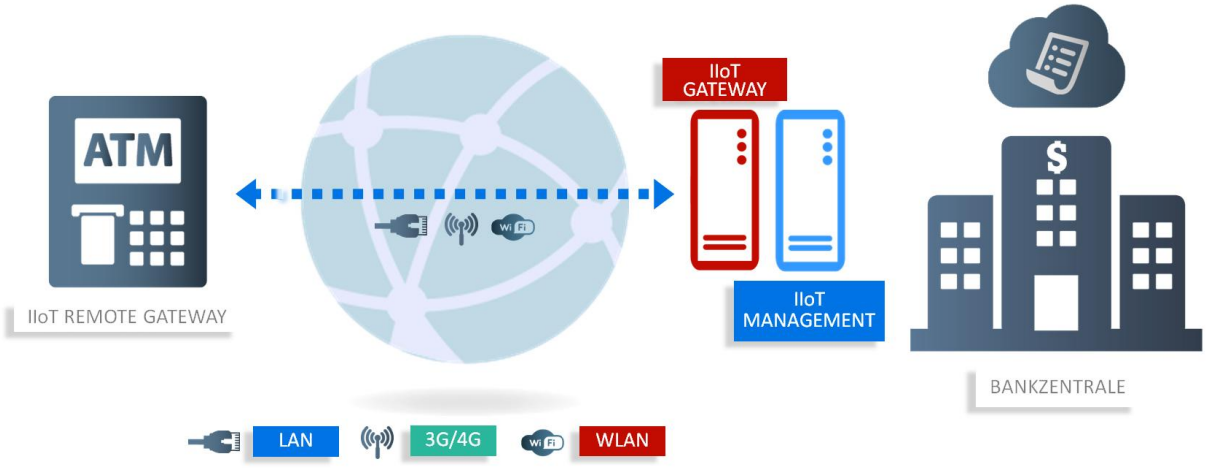
Was bedeutet IIoT?

Es geht nicht mehr darum, auf eine industrielle Anlage Zugriff über das Internet zu haben. Es geht darum, auf jede technische Komponente innerhalb des Betriebes steuernd zugreifen bzw. den Status abfragen zu können. Der Zugriff kann also bis hin zum einfachen Sensor, z.B. einem Temperaturfühler, erfolgen. Derartige Zugriffe sind beim IIoT nicht nur auf stationäre Objekte

beschränkt, vermehrt kommen auch bewegliche Objekte wie z.B. Automobile, Drohnen, Versandartikel usw. hinzu.
So vielfältig im industriellen Umfeld die eingesetzte Hardware sein kann, so vielfältig sind die bisher in diesem Umfeld anzutreffenden Protokolle für den Datenaustausch. MQTT, CoAP, XMPP und sogar das altbewährte HTTP scheinen sich als Standardprotokolle der Zukunft herauszubilden. Für die Verschlüsselung wird meist SSL/TLS verwendet. Hier bedient sich der jeweilige Hersteller meist im Open Source-Umfeld. Dass derartige Implementierungen funktionieren steht außer Frage. Wie sieht es jedoch mit der Skalierung, Verfügbarkeit an Sammelknoten (Redundanz) und Fehlerbehebung vor Ort aus? Bei letzterer ist nicht die Fehlerbehebung in der Software gemeint, sondern auch der Austausch betroffener Softwarekomponenten am Endgerät vor Ort. Diese Aufgabe wird schnell zu einer echten Herausforderung, wenn es sich um eine große Anzahl von Endgeräten handelt und diese sich an schwierig zugänglichen Orten befinden.

Die Firma NCP hat seit Jahren Erfahrung auf dem Gebiet des hochsicheren Remote Access. Geht es klassisch um die Anbindung von bis zu mehreren tausend Endanwendern an die Firmenzentrale über verschiedenste Einwahlmedien und mit unterschiedlichsten Authentisierungsvarianten, so werden mit NCP-Technik ebenso erfolgreich Projekte im Bereich von Machine-2-Machine umgesetzt. Beispielsweise kommt diese in Bankautomaten zum Einsatz. Den Betreibern dieser Lösung sind die folgenden Funktionalitäten besonders wichtig:

- die Updatefähigkeit der NCP-Software auf dem Endgerät aus der Firmenzentrale heraus
- die zentrale Verteilung von Zertifikaten auf die Endgeräte
- die Verteilung einer neuen Konfiguration zum Verbindungsaufbau auf das Endgerät
- eine ausgereifte Komplettverschlüsselung aller ein- und ausgehenden Daten
- eine hohe Integrationsfähigkeit und Automatisierbarkeit des Managements der beteiligten NCP-Komponenten auf der zentralen Seite



Szenario Bankautomat

Security für das Industrial Internet of Things

Die NCP-Lösung ersetzt nicht die Kommunikation auf Sensorebene mit oben genannten IIoT-Protokollen. Jedoch stellt sie diesen Protokollen einen ausgereiften Sicherheitslayer zum Transport bereit. Dabei spielt es keine Rolle wie viele IIoT-Sessions innerhalb des transparenten Datentunnels stattfinden. Die NCP-Lösung kann auf unterschiedlichster Hardware integriert werden, angefangen von einer kostengünstigen ARM-basierten Hardware bis hin zur Hochleistungsserverplattform. Neben dem im IIoT-Umfeld häufig anzutreffenden Linux-Betriebssystem bietet NCP seine zentralen Produkte – Gateway und Management – auch für die Windows Server-Plattform an. Clientseitig werden Linux, Windows, Android (via API und als native Implementierung), macOS sowie iOS unterstützt. Automatismen wie ein automatischer Verbindungsaufbau, die Auswahl des am besten geeigneten Verbindungsmediums oder Schnittstellen via Kommandozeile oder lokale API ermöglichen eine umfassende Automatisierung des Betriebes.

Das Herzstück der NCP-Lösung stellt das zentrale Management aller beteiligten Komponenten dar. Neben den oben genannten Verwaltungsfunktionen bietet das Management der NCP-Lösung folgende Schnittstellen für eine bestmögliche Integration in bestehende Infrastrukturen:

- Anbindungsmöglichkeit an MS Active Directory oder andere Verzeichnisdienste
- integrierter RADIUS-Server bzw. Anbindungsoption an externen RADIUS-Server
- Anbindung an eine Certificate Authority (Microsoft CA oder andere)
- hoher Automatisierungsgrad und flexible Integration durch Skriptsprache/Batchdateien
- einfache Inbetriebnahme neuer Endgeräte durch Vorlagen und automatische Generierung von Konfiguration und ggf. Zertifikaten mit anschließender Verteilung

Weitere Merkmale:

- ausfallsicheres Konzept
- Mandantenfähigkeit
  inkl. Anbindung an mandantenspezifisches MS Active Directory oder LDAP

Aufgrund der engen Zusammenarbeit von NCP und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der sich daraus ergebenden Erfahrung im Umgang mit hochsensiblen Daten, sind NCP-Lösungen für geheimschutzbetreute Unternehmen bzw. für den Transport hochsensibler Daten geradezu prädestiniert.

Haftungsausschluss
Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen
Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Stand Januar 2017

Next Generation Network Access Technology

www.ncp-e.com

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com