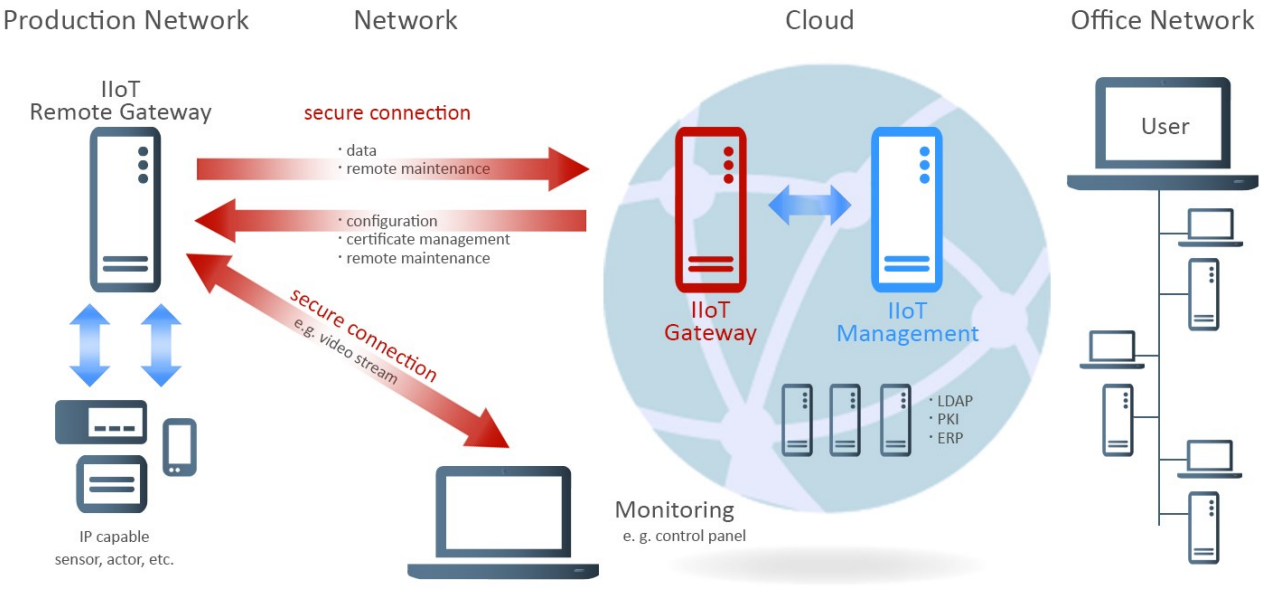
Security for the Industrial Internet of Things

In times where we are constantly online and do not think twice about revealing our personal status or making mobile payments, it is easy to forget security at the cost of convenience or to ignore potential risks. This applies to both the private and business markets.
Although we have only just become accustomed to this way of life, the next step is around the corner with the Industrial Internet of Things (IIoT) which will bring greater interconnectivity than ever before.

Just a few years ago, factories with production lines and control systems were serviced and monitored on site by qualified personnel. There were no direct links to the world outside the factory. In this scenario, staff were the only layer of security needed to protect the factory. As technology progressed, remote maintenance was carried out via dedicated lines and then through remote access via the Internet. Security risks have been increasing ever since the prevalence of remote access. A factory can be attacked from anywhere in the world anonymously and from a legal vacuum. Distributed denial of service attacks (DDoS) or easily discovered vulnerabilities and the subsequent introduction of malware are happening every day.



Overview: IIoT infrastructure

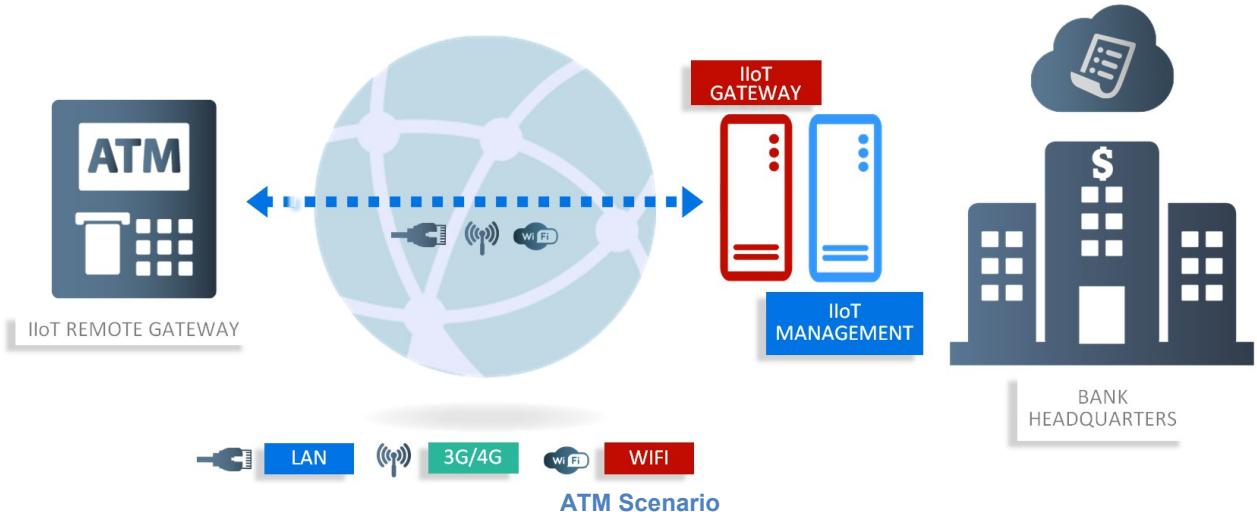
What is IIoT?

Industry needs have advanced beyond remote access to factories via the internet. IIoT involves networking all technical devices in a company for remote management and monitoring status. This means that even a

single device such as a temperature sensor can be access and controlled via a network. In addition to stationery applications, IIoT is increasingly being adopted for mobile applications such as vehicles, drones and shipping products.
Protocols for data exchange are just as varied as the hardware used in industrial applications. MQTT, CoAP, XMPP and even HTTP seem to be making their mark as the standard protocols of the future. In most cases, SSL/TLS is used for encryption. Most manufacturers use open source implementations of these protocols. There is no doubt that these implementations work in practice, yet questions must be asked in terms of scalability, redundancy and software fixes in production. The latter concerns updating software components on end devices rather than software fixes. Updating end devices can quickly become challenging with a large number of devices or if device locations are difficult to access.

NCP has decades of experience in the field of highly secure remote access. Companies who need to connect thousands of end users to the company network via a diverse range of media with many different authentication methods can also use NCP technology just as successfully in machine-to-machine projects. For example, NCP technology is used in ATMs. Customers who have implemented this solution benefit particularly from these features:

- NCP software on end devices can be updated centrally from the company's headquarters
- Certificates can be distributed centrally to end devices.
- Connection configuration data can be sent to end devices
- Advanced end-to-end encryption of all incoming and outgoing data
- High level of integration and automation of NCP components through central management



ATM Scenario

Security for the Industrial Internet of Things

The NCP solution does not replace the communication at the sensor level with IIoT protocols and adds an advanced security layer to data transport irrespective of how many IIoT sessions are held within the tunnel. The NCP solution can be implemented on diverse hardware ranging from low-cost ARM-based systems to high-performance server platforms. In addition to Linux which is often used in industry applications, NCP also offers IIoT Gateway and Management components for the Windows Server platform. Linux, Windows, Android (via API and a native implementation), macOS and iOS clients are supported. Features such as automated connection, selection of the most suitable connection medium, command line interface or the local API allow full automation of the NCP components.

The core of the NCP solution is the central management of all components. In addition to the management functions mentioned above, NCP central management offers the following interfaces for optimum integration into existing infrastructures:

- Connectivity to MS Active Directory or other directory services
- Integrated RADIUS server or connection option for external RADIUS server
- Connection to a Certificate Authority (Microsoft CA or others)
- Highly automated and flexible integration with scripting and batch files
- Easy commissioning of new devices through templates and automatic generation and distribution of configuration and certificates

Other Features

- Redundancy
- Multi-client capability
  including integration with client-specific MS Active Directory or LDAP

Close collaboration between NCP and the Federal Office for Security (BSI) ensures vast experience in handling highly-sensitive data and underpins NCP solutions as ideal for companies who need to process classified or confidential data securely.

Security for the Industrial Internet of Things

Disclaimer

The information contained in this document is subject to change without notice and does not represent any commitment to liability of NCP engineering GmbH. NCP engineering GmbH reserves the right to make changes to specifications for the purpose of technical progress.

Trademarks

All products mentioned are registered trademarks of their respective owners.

Version: January 2017

Next Generation Network Access Technology

www.ncp-e.com

Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299