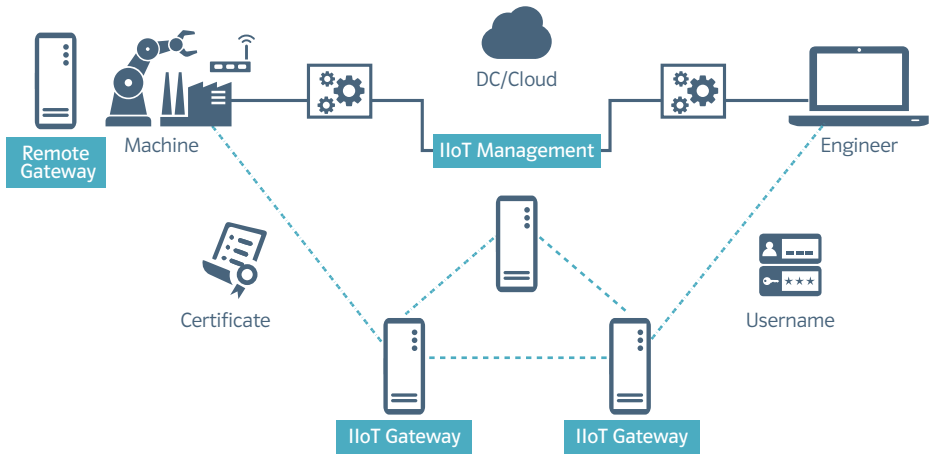
NCP Smart Maintenance

sichere Datenkommunikation im Umfeld von Maschinen und Systemen

Das Thema Industrie 4.0 und die zunehmende Vernetzung von Maschinen und Systemen haben vor allem im Jahr 2020 rasant an Fahrt aufgenommen. Der Digitalisierungsschub, den die Corona-Pandemie der deutschen Wirtschaft beschert hat, wird zunehmend stärker. Er bezieht sich nicht nur auf den Bereich privater oder schulischer Ausstattung, sondern auch auf die Produktion und die IT. Gerade im Umfeld der Produktion kann ein Lockdown schnell zu einer wirtschaftlichen Katastrophe werden. Maschinen stehen still oder die Kommunikation von angeschlossenen Systemen funktioniert nicht mehr. Der Umstand, dass ein Techniker das Unternehmen nicht betreten kann bzw. darf, führt somit zu einem hohen wirtschaftlichen Ausfall.



NCP Smart Maintenance unterstützt Sie optimal in dieser Situation.

Ein Techniker erhält in kürzester Zeit einen sicheren, zeitlich begrenzbaren Fernzugriff auf die gewünschte Maschine. Durch die schnelle Herstellung der Verbindung spart man viel Zeit und Kosten und ein möglicher Ausfall der Maschine/Anlage wird auf ein Minimum reduziert.

Konform nach dem Standard für sichere Fernzugriffslösungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) hat NCP für verschiedenste Industrie 4.0-Szenarien die passenden Softwarekomponenten für sichere Datenkommunikation:

- **Remote Gateways** für sichere Kommunikation von Anlagen, Maschinen oder Systemen
- **zentrales IIoT Gateway** in einem sicheren Bereich (z.B. DMZ) für die Verbindung zwischen „Innen" und „Außen"
- **zentrales IIoT Management** für Administration, Monitoring und sicherheitstechnische Steuerung

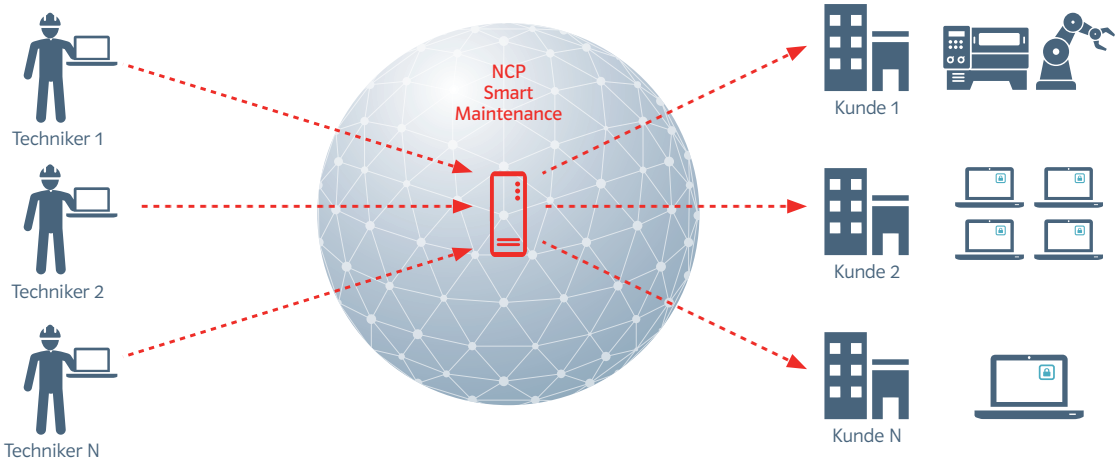
NCP Smart Maintenance branchenübergreifend für die Ansprüche „Fernwartung im industriellen Umfeld"

- zentrales Management (Cloud, OnPremise, Hybrid) zur Verwaltung und Steuerung aller User, Devices uvm.
- mandantenfähige, sicher getrennte Verwaltung vieler Kunden und Standorte
- granulare Zugriffsrechte
- Verbindungsaufbau dedizierter Maschine zu bestimmtem Techniker
- Szenarien in Cloud-Umgebungen oder Industrie 4.0-Strukturen
- Policy Enforcement und NAC im VPN/Fernwartungskontext
- state-of-the-art Verschlüsselung (z.B. IPsec IKEv2 mit ECC)
- starke Authentisierung (z.B. Zertifikate, TOTP oder andere)
- hochverfügbar und voll virtualisierbar
- zukunftsfähig (u.a. IPv4/IPv6-fähig)

hochsicher

skalierbar

ressourcenschonend



Neben dem Zugriff von Technikern auf Maschinen in der Produktion lassen sich weitere Szenarien abbilden. Dabei ist jeder Anwendungsfall individuell umsetzbar aber gleichzeitig einheitlich in der Lösung. Die Vernetzung von Technikern auf abgelegene Systeme, bspw. im Energiesektor (Kleinkraftwerke, Solarparks, uvm.) ist ebenso möglich wie der Zugriff von Technikern auf IT-Systeme in Kliniken oder Finanzinstituten. Hierbei dient als zentrales Element das Secure Enterprise Management (SEM) von NCP, das Herzstück von Smart Maintenance. Hiermit können alle Szenarien aus einer Hand administriert werden. Die Infrastruktur ist gleichermaßen geeignet für Kunden mit vielfältigen Szenarien wie auch für Managed Service Provider, die ihren Kunden individuell zugeschnittene Lösungen anbieten wollen.

Haben wir Ihr Interesse geweckt oder haben Sie noch weitere Fragen?

Dann wenden Sie sich gerne an Ihre Ansprechpartner:

Benjamin Isak
Senior Account Manager DACH
E-Mail: benjamin.isak@ncp-e.com
Mobile: +49 175 1901100

Sebastian Oelmann
Product Manager Industrie 4.0 | IIoT
E-Mail: sebastian.oelmann@ncp-e.com
Mobile: +49 175 4026805

NCP engineering GmbH | Dombühler Straße 2, 90449 Nürnberg | www.ncp-e.com