



Kubernetes auf dem Shopfloor: Sichere und zukunftsfähige Geräte- und App-Verwaltung mit netFIELD

Uwe Schnepf
Leiter Produktmanagement IIoT Solutions

Hilscher auf einen Blick

Zuverlässiges Geschäft



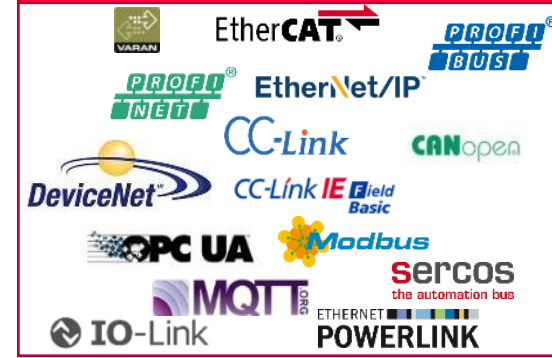
Finanzielle Stabilität



Qualität



Unsere Expertise



netX Chips & Module



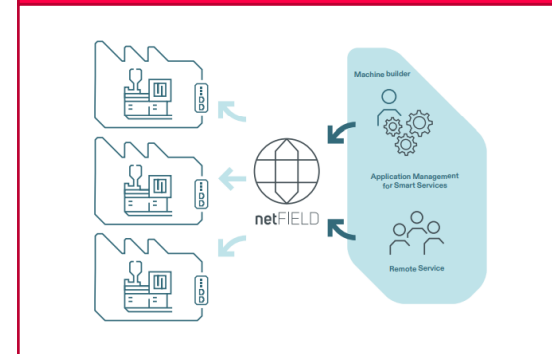
PC-Karten



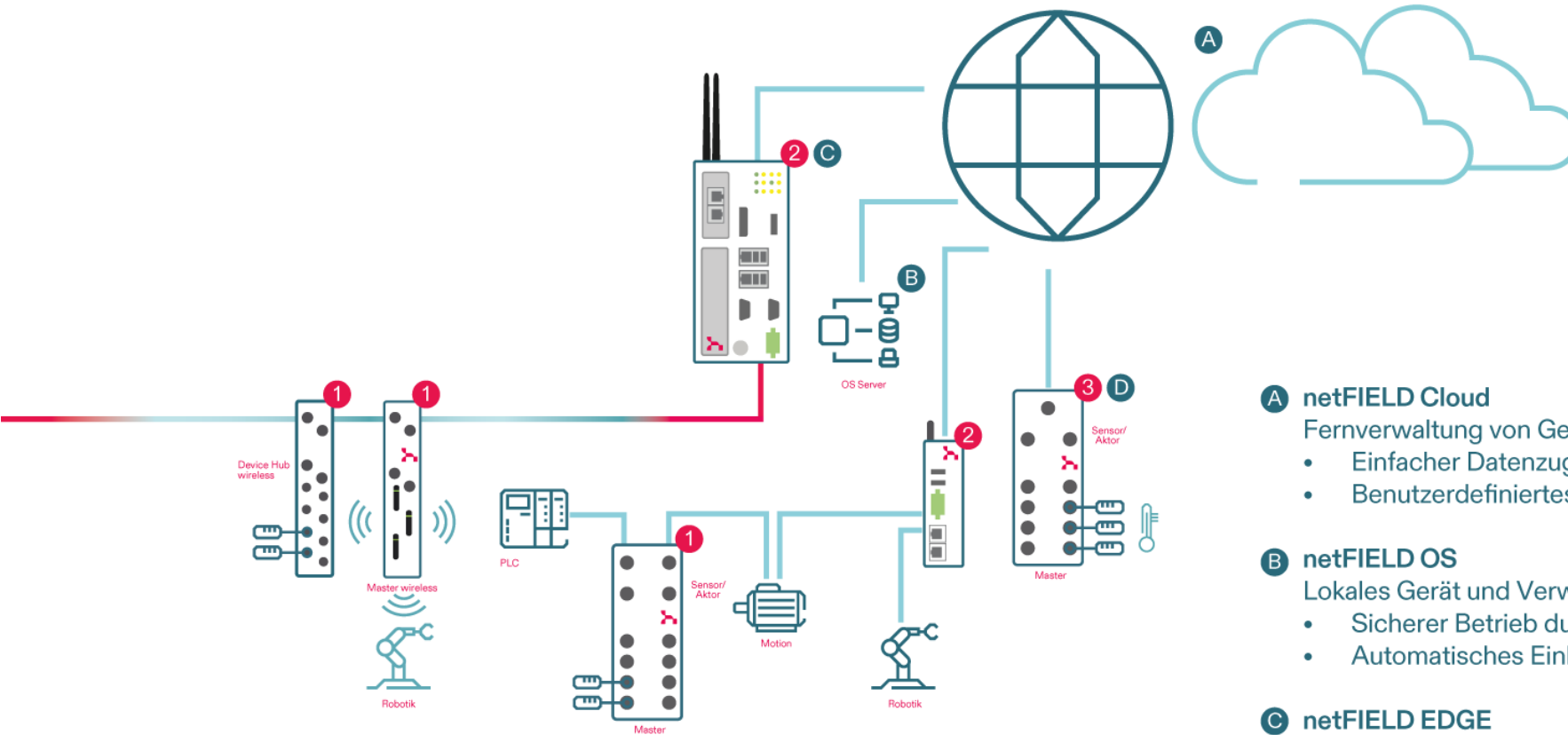
Gateways



netFIELD



MILLIONEN GERÄTE ÜBERALL VERWALTEN. netFIELD.



- A netFIELD Cloud**
Fernverwaltung von Geräten und Anwendungen
 - Einfacher Datenzugriff über RestAPI
 - Benutzerdefiniertes White-Labeling verfügbar
- B netFIELD OS**
Lokales Gerät und Verwaltung (opt.)
 - Sicherer Betrieb durch virtuelle Maschine
 - Automatisches Einbinden von Geräten in die **netFIELD Cloud**
- C netFIELD EDGE**
Schließen Sie die Lücke zwischen OT und IT
 - Abgestimmte Lösungen für verschiedene Leistungsklassen
 - Real-Time Ethernet Unterstützung
 - Perfekt integriert in **netFIELD OS** und **netFIELD Cloud**
- D sensorEDGE**
Verbindet bis zu 8 IO-Link-Sensoren direkt mit der Cloud
 - Schnelle und einfache automatische Konfiguration
 - Dashboard-Visualisierung für Sensordaten

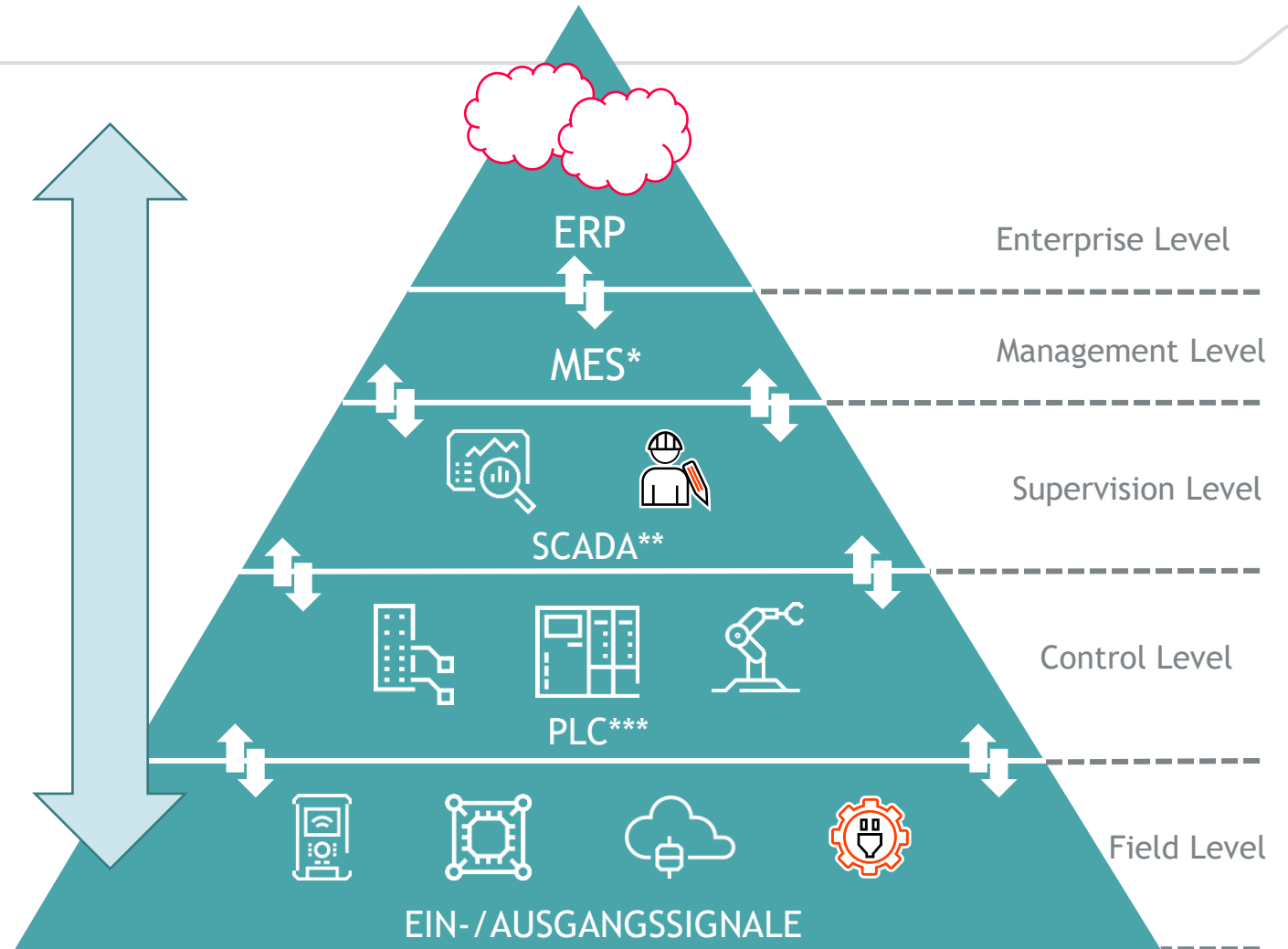


Edge Computing als Werkzeug der Industrie 4.0

Vertikale Integration für:

- Condition Monitoring
- Remote Service
- Predictive Maintenance
- Machine Learning
- Smart Control
- Smart Service
- Pay-per-Use

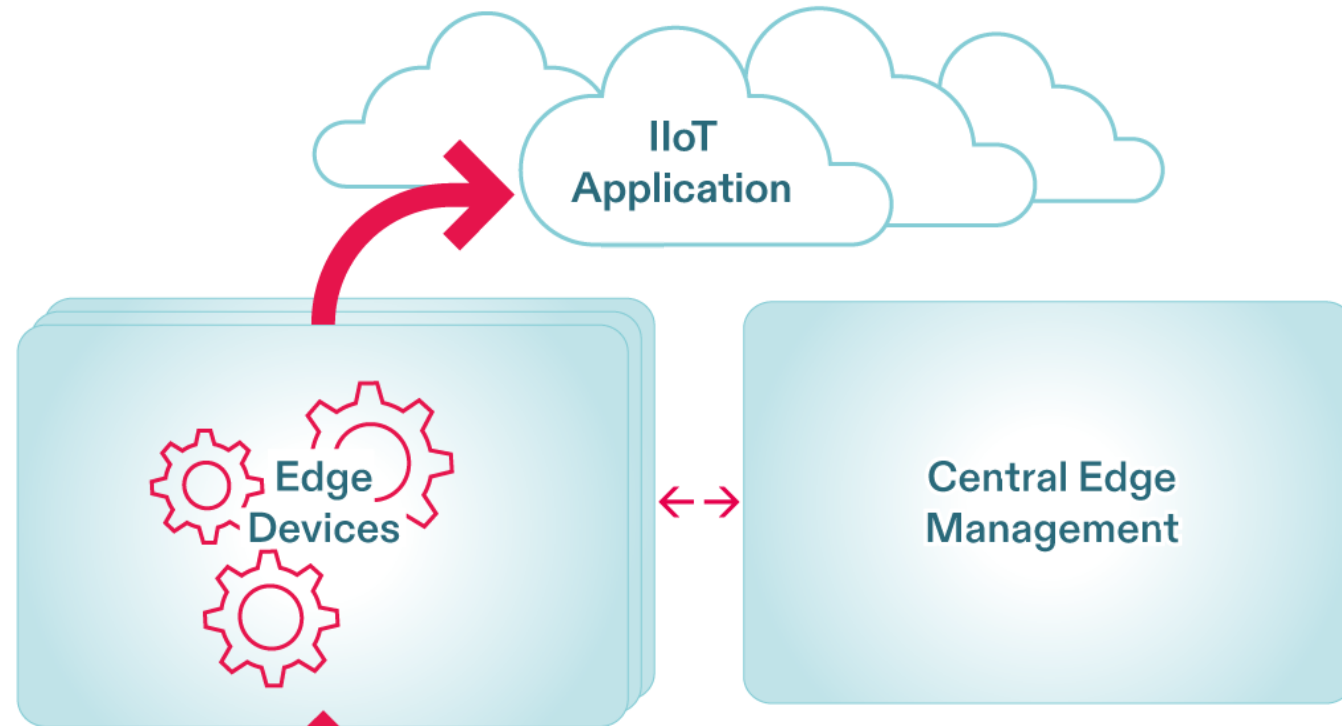
Edge Computing



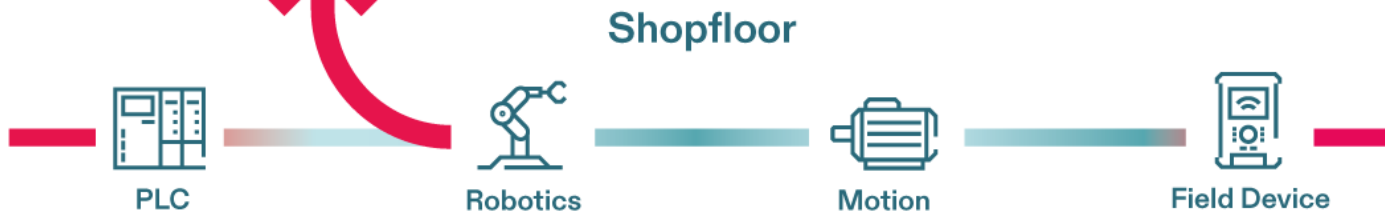
* Manufacturing Execution System

**Supervisory Control And Data Acquisition

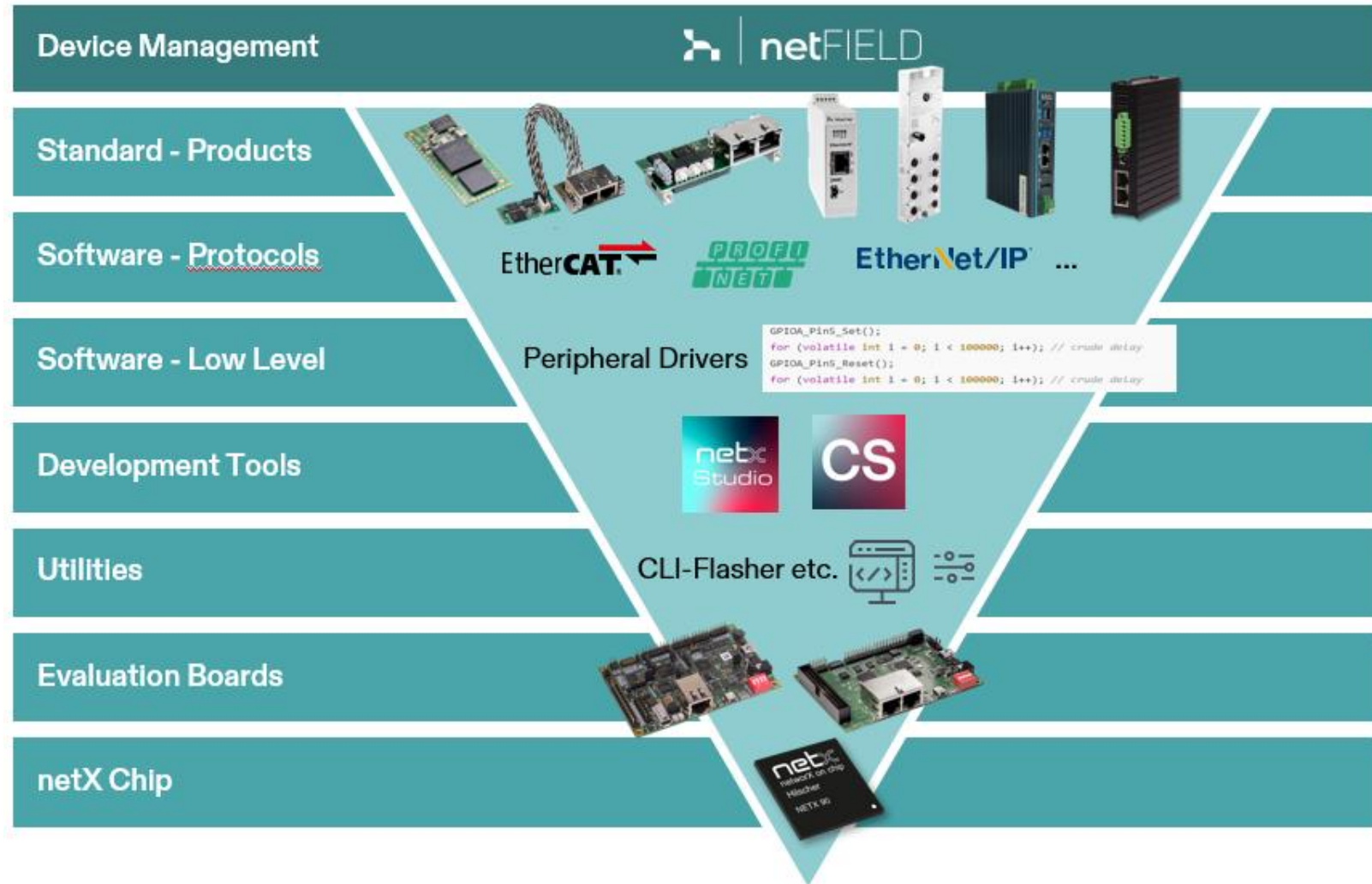
***Programmable Logic Controller



Sicheres Device Management



Sicherheit bis auf Chip-Ebene: das netX-Ecosystem



BEDROHUNGSLAGE & RELEVANZ



266,6 Mrd.€

Schaden durch
Cybercrime (2024)



81%

Unternehmen
betroffen



1.220

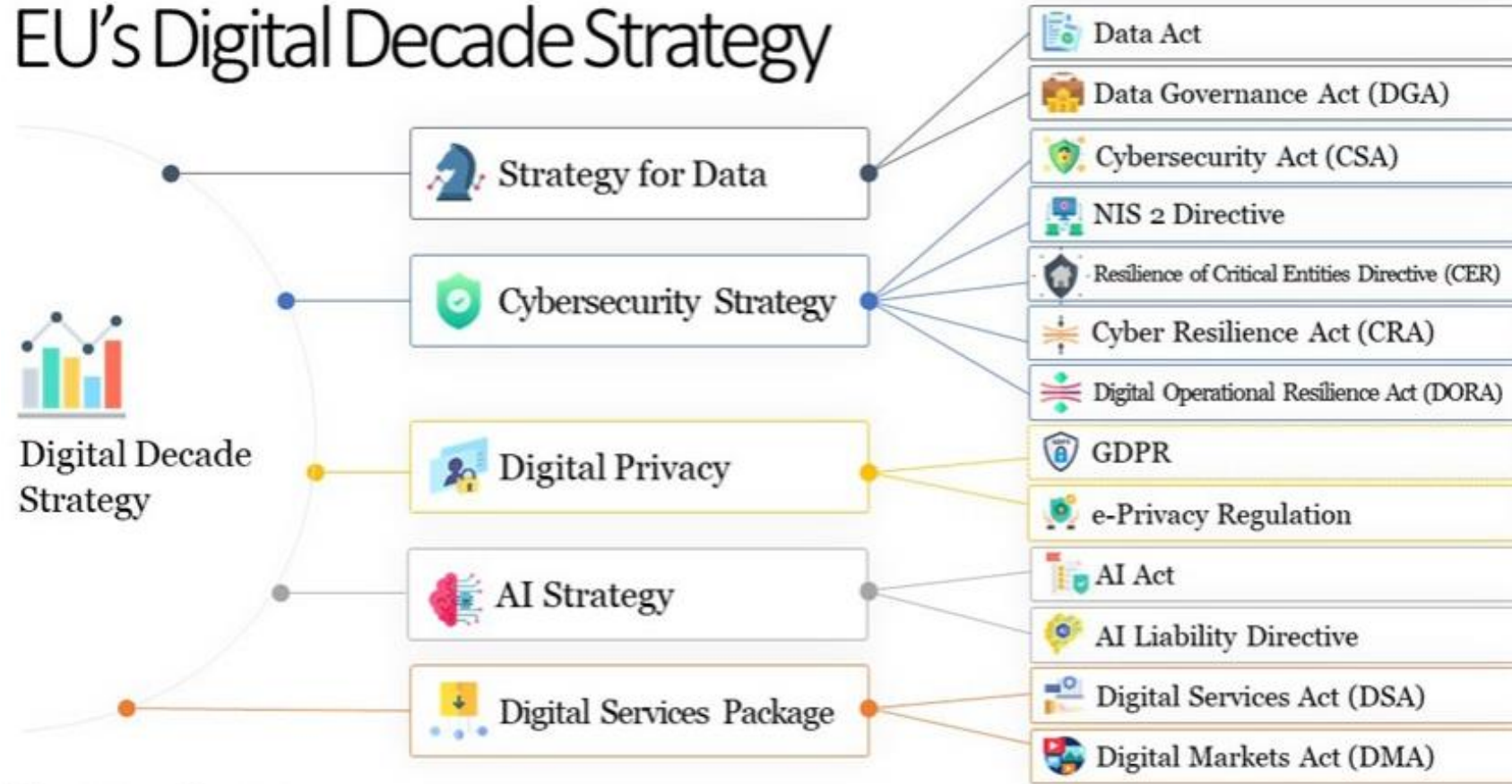
Angriffe/Woche
in DE

Maschinen:

vernetzt, automatisiert, angreifbar



EU's Digital Decade Strategy



While Others Innovate, Europe Regulates ;-)

Wo spielt Cyber Security eine Rolle auf dem Shopfloor?

Nur autorisierte Benutzer erhalten Zugang zu Geräten und Daten

Autorisierung



Schutz vor Daten-manipulation

Integrität



Unbefugtes Lesen von Daten verhindern, Daten geheim halten

Vertraulichkeit



SPS



Verfügbarkeit

Sicherstellen, dass das System die definierte Funktion erfüllt

Authentizität

Sicherstellen, dass die Kommunikation nur mit vertrauenswürdigen Geräten erfolgt

Anforderungen an Maschinenbauer, Anlagenbetreiber und Lösungsanbieter



→ NIS-2 Richtlinie

→ CRA

→ Maschinenverordnung

NIS-2-Richtlinie – Umsetzungspflichten für mittlere und große Maschinenbauer



		Risikobewertung		
Wahrscheinlichkeit	Hoch	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Mittel	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
	Niedrig	Niedriges Risiko	Niedriges Risiko	Mittleres Risiko
		Selten	Mittel	Hoch



Was ist NIS-2?

- EU-Richtlinie für kritische und wichtige Einrichtungen zur Verbesserung der Cybersicherheitslage

Anwendungsbereich

- Betrifft Unternehmen mit > 50 Mitarbeitenden oder > 10 Mio. € Umsatz, sofern im produzierenden Gewerbe

Timeline

- Nationale Umsetzung sollte eigentlich bis Oktober 2024 (NIS2UmsuCG) erfolgen
- Umsetzung asap (und dann unverzüglich in Kraft)

Kernpflichten

- Einführung eines ISMS
- Benennung eines Sicherheitsverantwortlichen
- Risikomanagement-Maßnahmen
- Incident-Reporting binnen 24 h an BSI
- Technische & organisatorische Maßnahmen

Konsequenzen bei Nicht-Einhaltung

- Bußgelder bis 10 Mio. € oder 2 % Umsatz

Herausforderungen

- Meldepflichten greifen auch bei Zulieferkettenproblemen (z. B. durch Softwarekomponenten von Dritten)

Notwendige Voraussetzungen zur Umsetzung im Unternehmen



Interne Sicherheitsstrukturen

- Einrichtung eines dedizierten Teams oder einer Abteilung für Cybersecurity
- Klare Zuständigkeiten und Verantwortlichkeiten definieren



Schulung und Sensibilisierung

- Regelmäßige Schulungen für Mitarbeiter in Bezug auf Cyberbedrohungen und Sicherheitspraktiken
- Sensibilisierungskampagnen zur Förderung einer Sicherheitskultur



Technologische Infrastruktur

- Investitionen in moderne Sicherheitslösungen (Firewall, Antivirus, Intrusion Detection Systeme)
- Implementierung von regelmäßigen Sicherheitsüberprüfungen und Updates

		Risikobewertung		
		Selten	Mittel	Hoch
Wahrscheinlichkeit	Hoch	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Mittel	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
	Niedrig	Niedriges Risiko	Niedriges Risiko	Mittleres Risiko

Risikobewertung

- Durchführung einer umfassenden Risikobewertung zur Identifizierung von Schwachstellen
- Entwicklung und Implementierung von Notfallplänen und Reaktionsstrategien

Weitere Empfehlungen für Compliance Maßnahmen



Berichterstattung

Meldepflicht

- Wesentliche Systeme sollten an ein SOC (Security Operation Center) angebunden werden.
- Das SOC übernimmt die automatisierte Anomalie-Erkennung
- Für den Fall einer Anomalie Erkennung, können erfahrener Techniker die Analyse fortsetzen und bei Bestätigung zusammen mit der internen IT geeignete Maßnahmen ergreifen



BSI IT-Grundschatz Zertifizierung

- Zertifizierung nach BSI IT-Grundschatz mit integrierter ISO 27001 Zertifizierung



Schutz der Produktion und der IT

- Assetmanagement implementiert
- Überarbeitung der Zugangskontrollen
- Überarbeitung des gesamten Sicherheitskonzepts der Produktions-IT und der IT

Der Cyber Resilience Act (CRA) – Verpflichtungen & Chancen



		Risikobewertung		
Wahrscheinlichkeit	Hoch	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Mittel	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
	Niedrig	Niedriges Risiko	Niedriges Risiko	Mittleres Risiko
		Selten	Mittel	Hoch



Was ist der CRA?

- Erste EU-weite Cybersicherheitsverordnung für Produkte mit digitalen Komponenten
- Gilt für Hersteller, Inverkehrbringer, Händler, Importeure und Betreiber

Timeline

- Veröffentlichung im EU-Amtsblatt am 24.11.2024
- Umsetzung Artikel 14 „Meldepflicht der Hersteller“ bis 11.09.2026
- Vollständige Umsetzung bis 11.12.2027

Kernpflichten

- Risikoanalyse durchführen
- Sichere Entwicklung, Authentifizierung, Zugriffskontrolle
- Sicherheitsupdates über gesamte Lebensdauer
- Meldepflichten für Schwachstellen (24h-Regel)
- CE-Kennzeichnung: Cybersicherheit als Konformitätskriterium

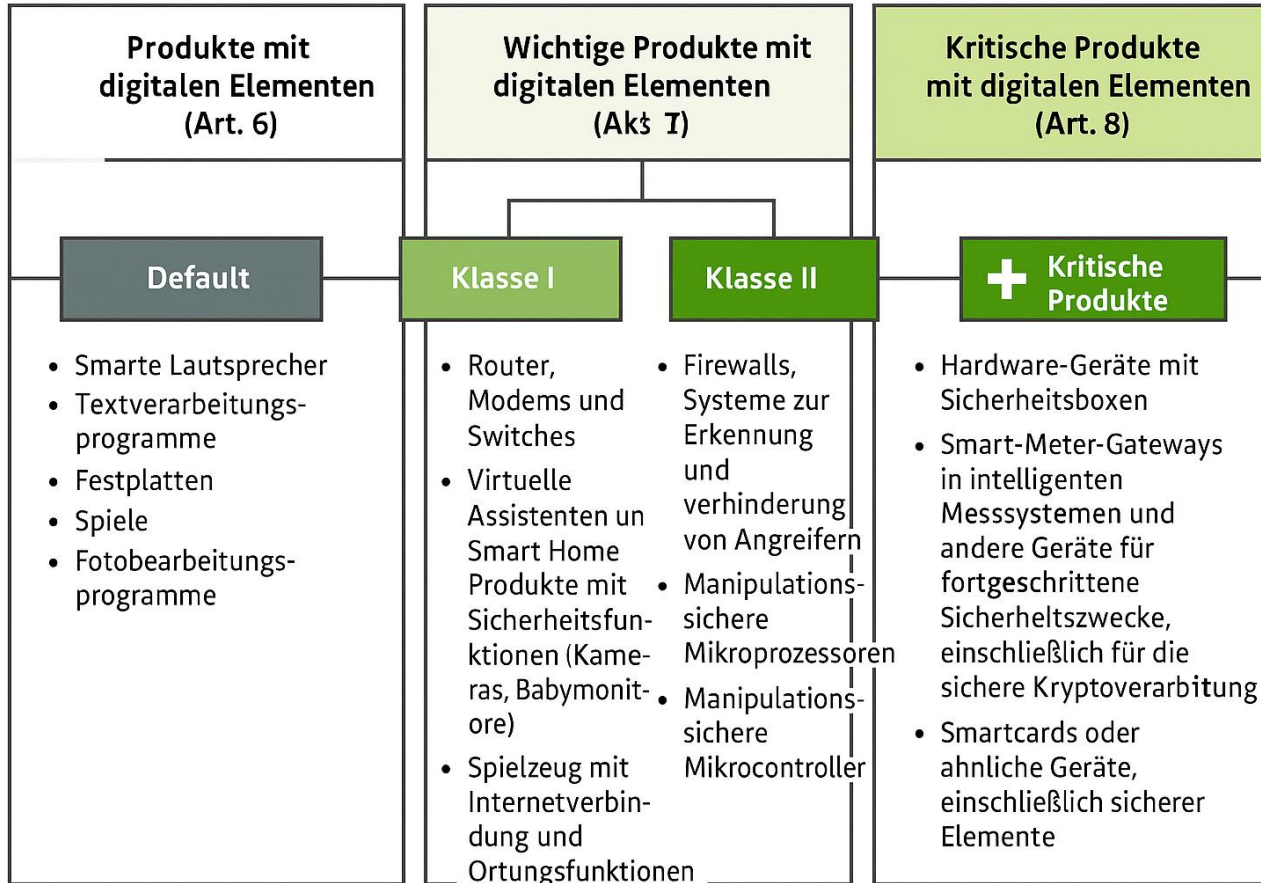
Konsequenzen bei Nicht-Einhaltung

- Marktverbot
- Rückruf
- Geldstrafen bis 15 Mio. € oder 2,5 % Jahresumsatz

Chancen

- Wettbewerbsvorteil durch "Secure-by-Design"
- Vertrauensgewinn bei Kunden

Anwendungsbereich



- Default: Self-Assessment für Sicherheitsstandards
- Klasse I: Self-Assessment anhand von Normen, wenn vorhanden, oder Assessment durch Dritte
- Klasse II und kritische Produkte: Assessment durch Dritte
- (Verpackungs-) Maschinen je nach Funktion und Risiko in den Klassen I oder II.

Praktische Empfehlung für Compliance Maßnahme



IEC 62443-4-1

- Fit/Gap Analyse durchführen für die Entwicklungsprozesse
- Start Dokumentation und Implementierung
- Zertifizierung



BSI IT-Grundschutz

- Zertifizierung nach BSI IT-Grundschutz inklusive ISO 27001



Produktvorprüfungen CRA

- In 2025 werden die Zertifizierungskriterien in der EU-Kommission verabschiedet
- In Kooperation mit den Zertifizierungsstellen beginnen, die ersten Produkte / Produktfamilien prüfen lassen
- Erstellung von SBOMs



Produktzertifizierungen

- Aus den Vorprüfungen Maßnahmenkataloge für die endgültigen Produktzertifizierungen erstellen.
- Die Maßnahmen dann einplanen und umsetzen

Maschinenverordnung (EU) 2023/1230 – Relevanz im Kontext

- Gilt ab: 20. Januar 2027
- Führt erstmals explizit Anforderungen an Cybersicherheit in Maschinen ein
- Ergänzt CRA aus Sicht der Maschinenfunktional- und -bediensicherheit

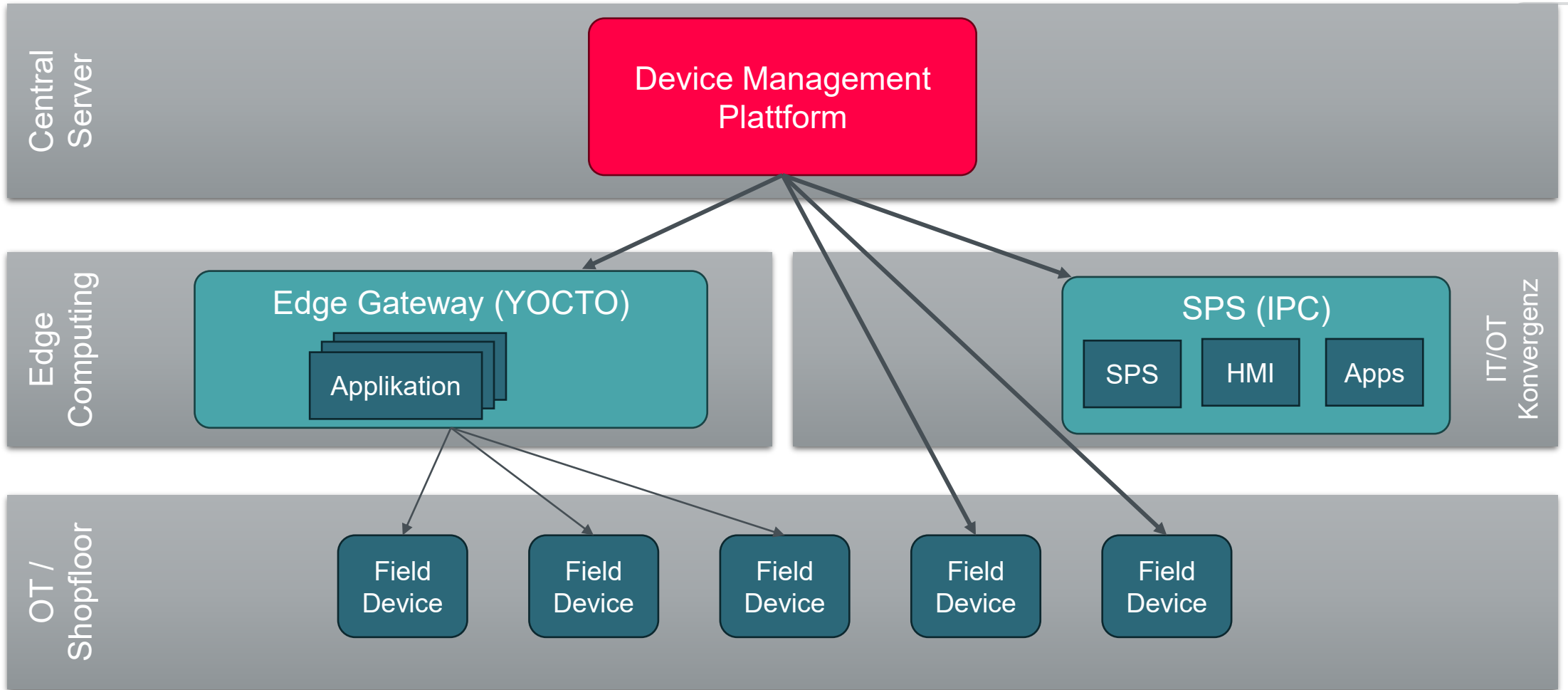
Das bedeutet konkret:

- Sichere Konnektivität
- Schutz kritischer Hardware
- Schutz kritischer Software und Daten
- Kenntlichmachung sicherheitsrelevanter Software
- Aufzeichnung von Änderungen



Daraus abgeleitet:
OT-Systeme müssen explizit
gemanagt und cybersicher
gehalten werden

Die netFIELD Device Management Plattform Entwicklung



Enterprise Device and Container Management for Industry 4.0

Bring intelligence to your field devices with netFIELD.io, a hybrid cloud and edge solution for the Industrial IoT.



The netFIELD.io Difference

Containers are revolutionizing connected IoT devices, and netFIELD.io is the perfect match to manage and run them.



INTELLIGENT EDGE

Run intelligence for data acquisition & analytics by deploying containers to your field devices.



OPEN PLATFORM

Manage your field devices from a single-point with end-to-end security and powerful open APIs.

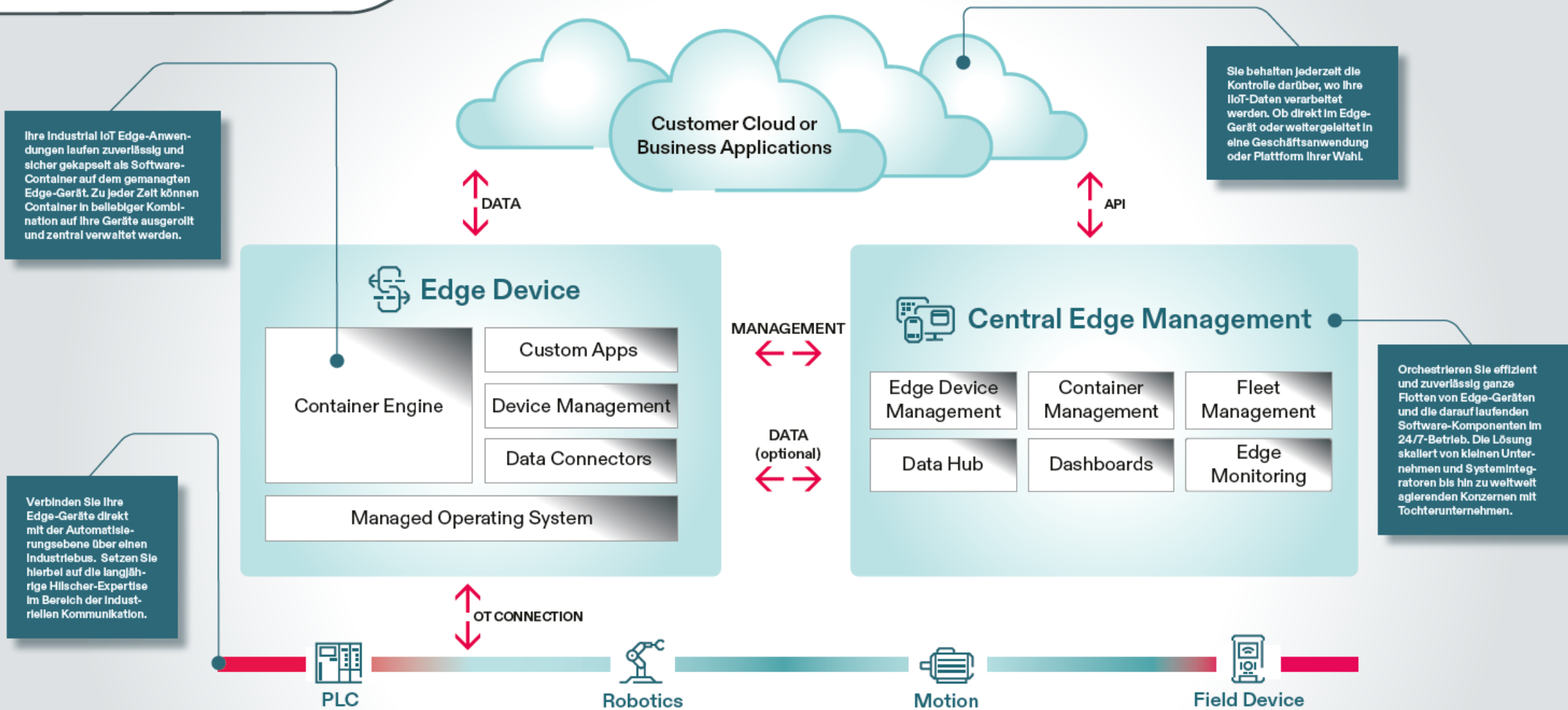


APPLICATIONS

Use our self-service portal to manage your devices at scale while maintaining ownership.

IIoT Edge Management

netFIELD Cloud



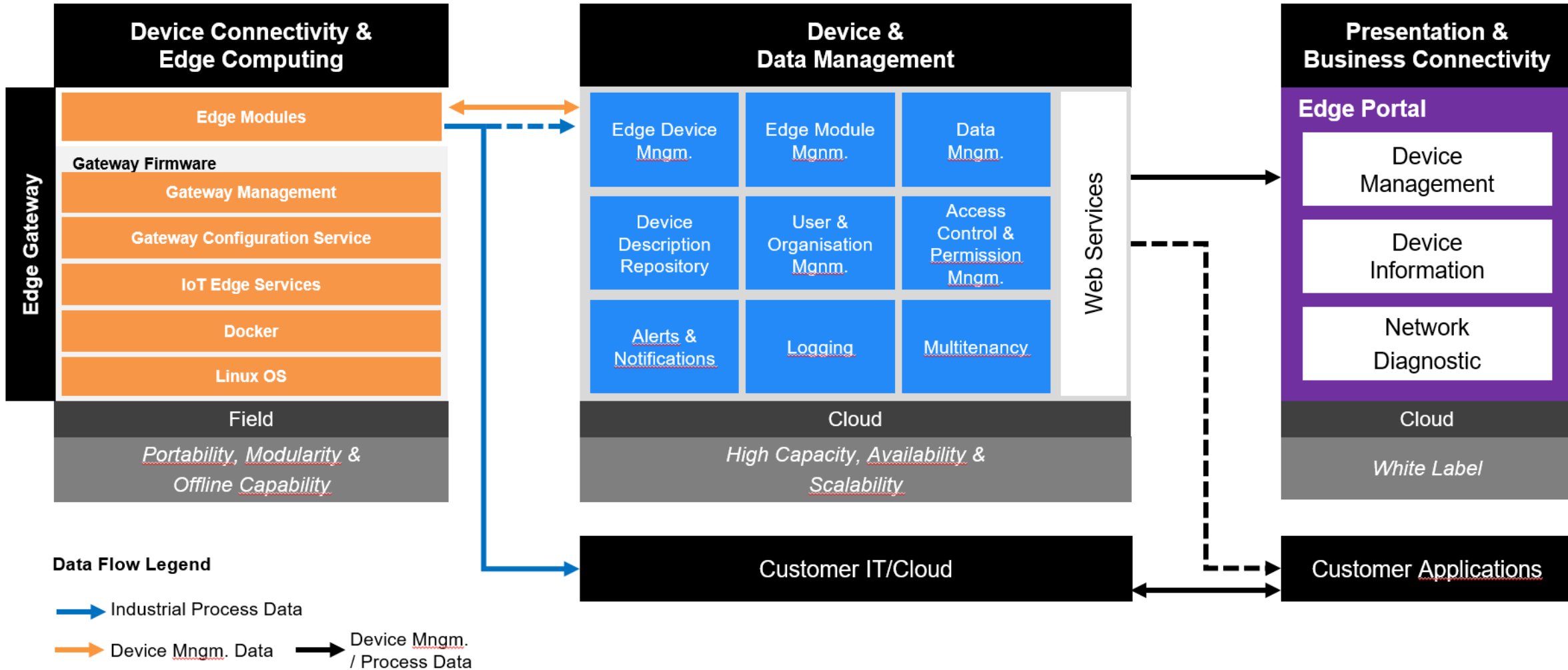
Ihre Industrial IoT Edge-Anwendungen laufen zuverlässig und sicher gekapselt als Software-Container auf dem gemanagten Edge-Gerät. Zu jeder Zeit können Container in beliebiger Kombination auf Ihre Geräte ausgerollt und zentral verwaltet werden.

Verbinden Sie Ihre Edge-Geräte direkt mit der Automatisierungsebene über einen Industriebus. Setzen Sie hierbei auf die langjährige Hilscher-Expertise im Bereich der industriellen Kommunikation.

Sie behalten jederzeit die Kontrolle darüber, wo Ihre IIoT-Daten verarbeitet werden. Ob direkt im Edge-Gerät oder weitergeleitet in eine Geschäftsanwendung oder Plattform Ihrer Wahl.

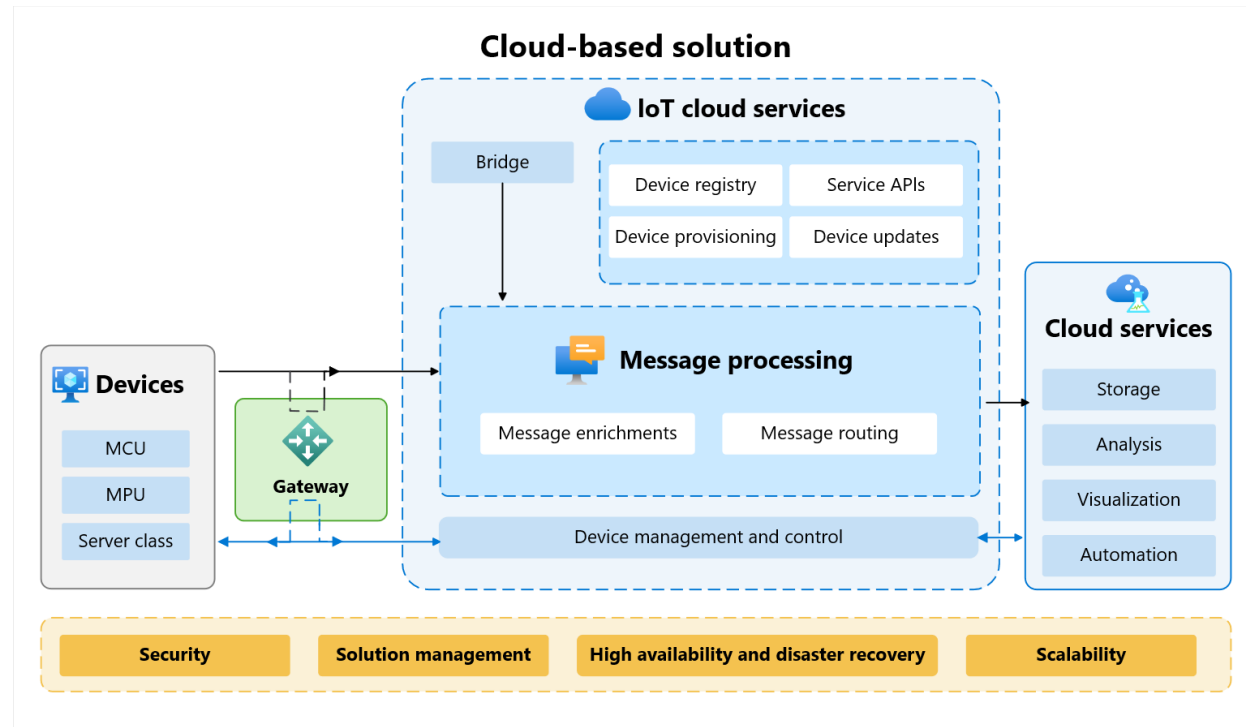
Orchestrieren Sie effizient und zuverlässig ganze Flotten von Edge-Geräten und die darauf laufenden Software-Komponenten im 24/7-Betrieb. Die Lösung skaliert von kleinen Unternehmen und Systemintegratoren bis hin zu weltweit agierenden Konzernen mit Tochterunternehmen.

System-Übersicht Geräte- und App-Verwaltung



Realisierung mit Azure IoT: The Beginning

- **Azure IoT** ist eine Sammlung von verwalteten Clouddiensten, Edge-Komponenten und Software Development Kits (SDKs) von **Microsoft**, die entwickelt wurden, um **Geräte** mit dem Internet der Dinge (IoT) in großem Maßstab zu **verbinden, zu überwachen und zu steuern**.
- Es ermöglicht die **Erfassung und Verarbeitung von Daten** von physischen Geräten, um Geschäftserkenntnisse zu gewinnen, die sowohl in der Cloud als auch am "Edge" (nahe den Geräten) verarbeitet werden können.
- Wichtige Bestandteile sind **Azure IoT Hub** (die Kommunikationsbrücke) und **Azure IoT Edge** (für die Verarbeitung am Edge).



Quelle: Microsoft Corp.

Dashboard

Devices ^

Edge devices

Plants

Software and artifacts ^

Applications

Operating systems

Manifests

Fleet management ^

Groups

Jobs

Rollouts

Remote access profiles

Organization settings ^

Users and roles

Organizations

Metrics and audit

Subscriptions

Auth providers

API access

netFIELD / Edge devices / 68caa26bd10235a5c2c07223

Automatisierungstreff 2025 ^

← automatisierungstreff-2025-sensorEDGE-01

[Edit device](#)

Device Information

Apps

Properties

Remote control

Device Stats

Docker

MQTT messages

Installed Apps

Add Apps

Search

Apps installed on automatisierungstreff-2025-sensorEDGE-01 (8)

Show system apps

Restart

Update

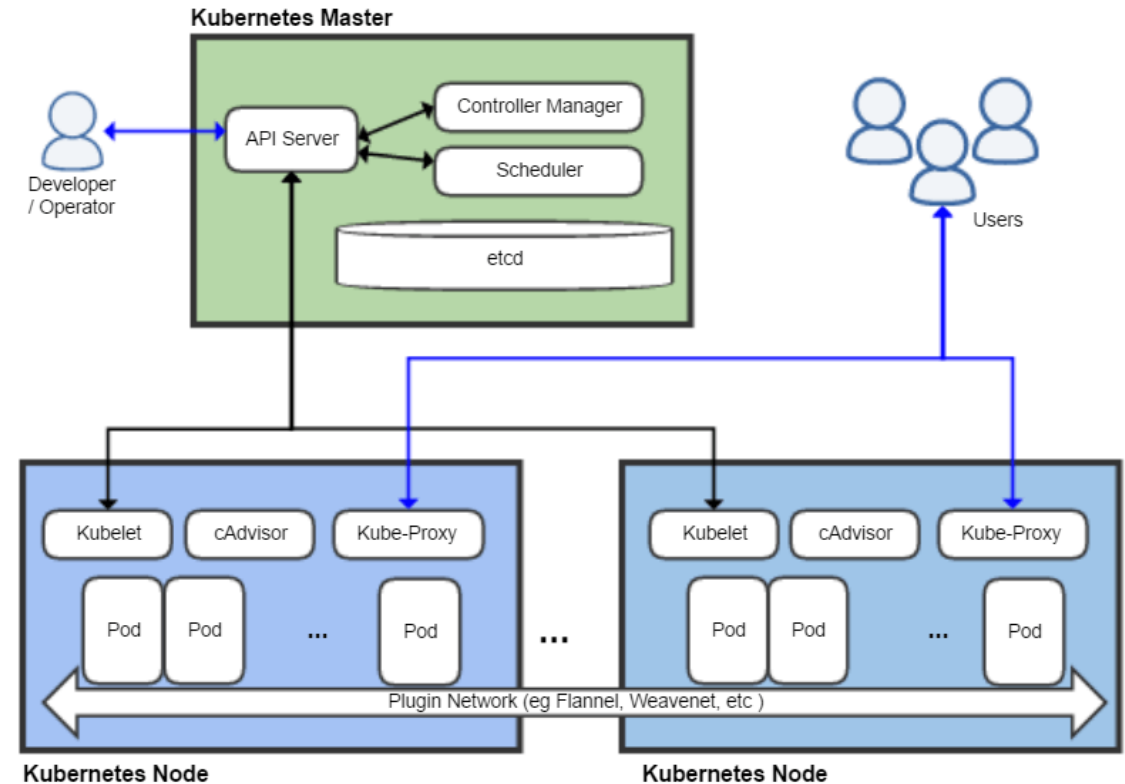
<input type="checkbox"/>	App name	Status	Version	Category	View
<input type="checkbox"/>	edgeAgent	Running	Reported: 1.5.27 Desired: 1.5	System	
<input type="checkbox"/>	edgeHub	Running	Reported: 1.5.27 Desired: 1.5	System	
<input type="checkbox"/>	netFIELD App IO-Link Configurator ...	Running	Reported: 1.2.5 Desired: 1.2.5	Applications	
<input type="checkbox"/>	netFIELD App License Server	Running	Reported: 1.0.2 Desired: 1.0.2	Services	
<input type="checkbox"/>	netFIELD App MQTT Broker	Running	Reported: 2.0.14 Desired: 2.0.14	IT/Cloud Connectors	

Nachteile Azure IoT

- Abhängigkeit von einem einzelnen Anbieter, sowohl kommerziell als auch technologisch
- Unklare Situation beim Datenschutz, evtl. hat die US-Regierung Zugriff auf Systeme im Bedarfsfall
- In diesem Sinne fehlende Daten-Souveränität
- Ebenso Gefahr von „Kill Switch“ bei politisch nicht-konformen Verhalten eines Staates oder Gesellschaft
- Darüber hinaus: Azure IoT gibt es nur als „Cloud-only“ – Vorbehalte seitens Industrie

Die Alternative: Kubernetes

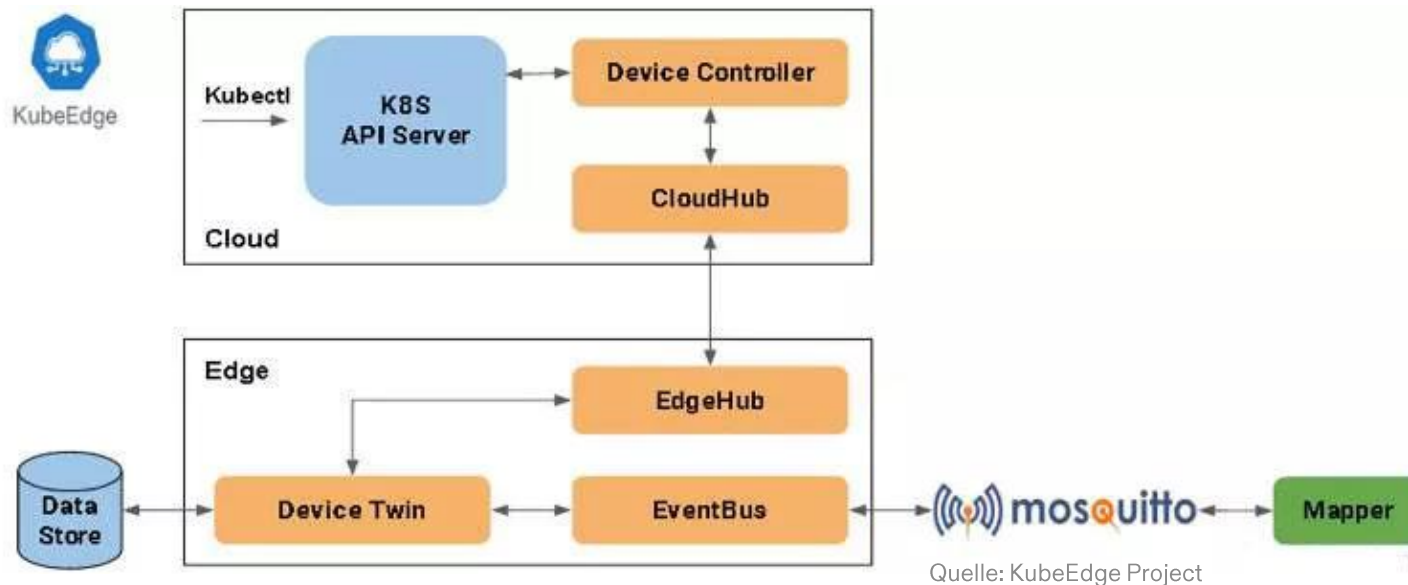
- Kubernetes ist eine **Open-Source-Plattform** zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen.
- Sie gruppiert **Container** zu logischen Einheiten, um die **Verwaltung** zu vereinfachen, automatisiert Prozesse wie die Anwendungskonfiguration und die Ressourcenzuweisung und stellt sicher, dass Anwendungen selbstheilend und hochverfügbar sind.
- Ursprünglich von Google entwickelt, wird sie heute von einer **großen Community** gepflegt und von der **Cloud Native Computing Foundation** verwaltet.
- Aber was ist mit der „**Edge**“? Diese Geräte sind nicht permanent online und potenziell weltweit verteilt.



Quelle: Cloud Native Computing Foundation

KubeEdge

- **KubeEdge** ist ein Open-Source-System zur Erweiterung der nativen Containerisierungsfunktionen für **Anwendungen** auf Hosts am Edge.
- Es basiert auf Kubernetes und bietet grundlegende **Infrastrukturunterstützung** für Netzwerk, Anwendungsbereitstellung und Metadatensynchronisation zwischen **Cloud und Edge**.
- KubeEdge ist unter Apache 2.0 als **Open Source** lizenziert und für den privaten oder kommerziellen Gebrauch völlig kostenlos und ebenfalls ein Projekt der Cloud Native Computing Foundation.



FAZIT:

Kubernetes & KubeEdge als sichere Basis für netFIELD Geräte & App Verwaltung

- Unabhängig von einzelnen Infrastruktur-Anbieter, diesem Sinne zukunftssicher
- Lizenzkostenfrei, Open Source ermöglicht günstige Infrastrukturkosten
- Läuft auf quasi jeder aktuellen Cloud Hosting Infrastruktur, z.B. StackIt der Schwarz-Gruppe
- On-Premise-Installation und -Betrieb möglich
- Stetige Weiterentwicklung durch große Community
- Beliebig Skalierbar
- Von NIS-2 und CRA geforderte Cyber Security durch Standard-IT Security-Funktionen abgebildet, z.B. Firewalls, Secure Boot, TPM, PKI, SSO/TFA, gehärtetes Edge OS auf Basis Linux u.v.m.
- **Die Zukunft gehört Open Source – trotz oder gerade wegen der geforderten Cyber Security-Anforderungen durch NIS-2 und CRA der EU!**

Vielen Dank für Ihre Aufmerksamkeit!

Hilscher Gesellschaft für Systemautomation mbH

Intelligente Lösungen für die Industrielle Kommunikation

Uwe Schnepf

Leiter PDM Industrial IoT Lösungen

Telefon: +49 6190 9907-607

Mobil: +49 157 387 40 337

E-Mail: uschnepf@hilscher.com

Web: www.hilscher.com

Rheinstraße 15 | 65795 Hattersheim

