

CRA-Ready: Technische Bausteine für eine zukunftssichere Serienfertigung

Leitfaden für den Maschinen- und Anlagenbau zur Unterstützung der CRA-Konformität mit dem IoT Gateway MC-NR

Executive Summary

Die fortschreitende Digitalisierung im Maschinen- und Anlagenbau erfordert eine lückenlose Vernetzung von Systemen im Feld. Gleichzeitig verschärft der Gesetzgeber die regulatorischen Anforderungen an die Cybersicherheit digitaler Produkte. Dieses Whitepaper beleuchtet die technischen Anforderungen des kommenden EU Cyber Resilience Acts (CRA) sowie der EN18031. Es zeigt auf, wie Maschinenbauer durch den strategischen Einsatz des IoT Gateways MC-NR die technische Grundlage für globale Konformität schaffen, die Hardware-Komplexität reduzieren und das Risiko von updatebedingten Ausfällen minimieren können.

Kapitel 1: Die regulatorische Herausforderung & EN18031-Unterstützung

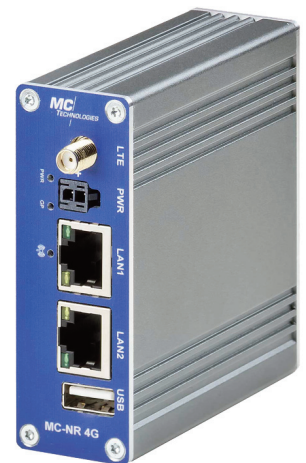
Sobald eine Maschine Daten sendet, empfängt oder verarbeitet, fällt sie unter die Bestimmungen des CRA. Die harmonisierte Norm EN18031 definiert dabei die konkreten technischen Schutzziele, bei deren Umsetzung unsere Hardware den Hersteller unterstützt:

- **Security by Design / Default:** Keine unsicheren Standard-Passwörter, standardmäßig geschlossene Ports und kryptografisch abgesicherte Kommunikationskanäle.
- **Patch-Management-Bereitschaft:** Die technische Möglichkeit, kritische Sicherheitslücken über die Betriebszeit hinweg sicher „Over-the-Air“ (OTA) zu adressieren.
- **Integritätsschutz:** Absicherung des Boot-Vorgangs, um das Einspielen manipulierter Firmware von Dritten zu erschweren.

Die IoT Gateway MC-NR Core Architektur:

Die Hardware wurde gezielt so konzipiert, dass sie Herstellern die Umsetzung der EN18031- und CRA-Anforderungen erleichtert. Das Herzstück bildet ein hochperformanter NXP i.MX91 Prozessor, der zusammen mit 512 MB RAM und 4 bis 8 GB Flash-Speicher ausreichend Leistungsreserven bietet, um anspruchsvolle Edge-Anwendungen, Docker-Container und lokales Datenlogging direkt auf dem Gerät auszuführen.

Durch hardwarebasierte Sicherheitsfeatures wie verschlüsselte Speicherbereiche und ein striktes, rollenbasiertes Zugriffsmanagement erhalten Sie eine robuste Plattform, die Ihren europäischen und globalen Vertrieb auf technischer Ebene absichert.



Rechtlicher Hinweis / Disclaimer: Dieses Whitepaper dient ausschließlich Informationszwecken und stellt keine Rechtsberatung dar. Die Erfüllung der Anforderungen des Cyber Resilience Acts (CRA) sowie der Norm EN18031 betrifft das jeweilige Gesamtsystem (die in Verkehr gebrachte Maschine/Anlage). Die MC Technologies GmbH übernimmt keine Haftung für die finale Konformität der Kundenapplikation. Das beschriebene IoT Gateway MC-NR ist ein technisches Hilfsmittel, das den Hersteller der Gesamtanlage bei der Umsetzung der Konformität unterstützen soll.

CRA-Ready: Technische Bausteine für eine zukunftssichere Serienfertigung

Kapitel 2: Wirtschaftlichkeit im Export durch weltweite Funkzulassungen

Im globalen Maschinenbau treiben länderspezifische Hardware-Varianten die Kosten im Engineering, in der Logistik und in der Ersatzteilhaltung nach oben.

Die IoT Gateway MC-NR Core Antwort:

- Globale Zulassung & Single-SKU: Das IoT Gateway MC-NR verfügt über umfassende, weltweite Funkzulassungen (u. a. CE, UKCA, FCC, IC, ANATEL, PTCRB, NAL, SRRC, Telec, NCC, SABER) und deckt alle global relevanten Frequenzbänder ab. Für Sie als Serienhersteller bedeutet das: Eine einzige Geräte-Variante (Single-SKU) für den Weltmarkt. Das vereinfacht die Logistik und das Ersatzteilmanagement dramatisch.
- LTE Cat.1bis & Single-Antenna: Durch den Einsatz eines modernen LTE Cat.1bis Moduls benötigt das IoT Gateway MC-NR nur noch eine einzige Mobilfunkantenne (Single-Antenna) statt der üblichen MIMO-Doppelantennen. Dies reduziert die reinen Hardware- und Kabelkosten und minimiert den mechanischen Montageaufwand (nur eine Bohrung am Schaltschrank) – ohne Einbußen bei der Signalqualität für industrielle Telemetrie- und Fernwartungsdaten.
- Ultrakompakter Formfaktor (Core-Variante): Mit ihren kompakten Abmessungen von 104×82×29" mm" lässt sich die Core-Variante extrem platzsparend auf der Hutschiene montieren. Sie verfügt zudem standardmäßig über ein integriertes GNSS-Modul (GPS, GLONASS, Galileo, BeiDou) für präzises Asset-Tracking und Geopositionierung ab Werk.

Kapitel 3: Maximale Verfügbarkeit (Dual Boot & Hardware Watchdog)

Ein Remote-Update bei einer Maschine im Ausland birgt im industriellen Alltag Risiken: Schlägt ein Firmware-Update fehl oder bricht die Mobilfunkverbindung ab, kann das Gateway unbrauchbar werden, was kostenintensive Serviceeinsätze vor Ort nach sich zieht.

Die IoT Gateway MC-NR Core Antwort:

- Dual Boot Architektur: Das IoT Gateway MC-NR verfügt über zwei autarke Software-Partitionen. Schlägt ein OTA-Firmware-Update im Feld fehl, erkennt das System dies, bricht den Vorgang ab und bootet selbstständig in das zuvor stabil laufende Backup-Betriebssystem. Ein unvollständiges Update blockiert somit nicht die Kommunikation zur Anlage.
- Hardware Watchdog: Ein dedizierter Hardware-Chip überwacht permanent die Vitalfunktionen des Hauptprozessors und führt bei Software-Hängern einen automatischen Hard-Reset durch. Zusammen mit einem weiten Betriebstemperaturbereich von -20°C bis +70°C wird so eine hervorragende Ausfallsicherheit an Remote-Standorten erzielt.



CRA-Ready: Technische Bausteine für eine zukunftssichere Serienfertigung

Kapitel 4: Praxisbeispiel – Globaler Verpackungsmaschinenhersteller

Ausgangslage: Ein Hersteller von Verpackungsmaschinen exportiert seine Anlagen weltweit. Bisher mussten im Engineering mehrere länderspezifische Router-Varianten gepflegt werden. Zudem fordern europäische Kunden vermehrt den Nachweis von Sicherheitskonzepten, die den CRA-Anforderungen entsprechen.

Die Umsetzung mit dem IoT Gateway MC-NR Core: Der Hersteller stellt seine Flotte auf das IoT Gateway MC-NR Core um. Da das Gerät über weltweite Funkzulassungen verfügt, wird im Standard-Schaltschrank nur noch eine einzige Hardware-Ausführung verbaut. Bei einem automatisierten Firmware-Update mitten in der Nacht bricht an einer Anlage in den USA die Mobilfunkverbindung ab.

Das Ergebnis: Dank der Dual-Boot-Architektur des IoT Gateways MC-NR bootet das Gateway autonom in den vorherigen, stabilen Zustand zurück. Die Maschine bleibt betriebsbereit, es entsteht kein ungeplanter Stillstand und kein teurer Technikereinsatz vor Ort. Gleichzeitig verfügt der Hersteller über ein technisch robustes Fundament, um die CRA-Konformität seiner Gesamtanlage erfolgreich zu dokumentieren.

(Dieses fiktive Anwendungsbeispiel dient der Veranschaulichung der technischen Funktionsweise.)

