FABOS

# Factory and Process Automation

## Ausgangssituation

Die wachsende Zahl von IIoT-Geräten erhöht das Risiko von Sicherheitsbedrohungen. Geräte können während ihrer Lebensdauer den Besitzer wechseln, was es für Backend-Dienste schwierig macht, die Berechtigung des Geräts zu überprüfen. Viele IIoT-Geräte sind so konzipiert, dass sie mehrere Jahre lang im Einsatz sind. Dennoch müssen Gerätehersteller und Dienstanbieter die Sicherheit ihrer Geräte während ihres gesamten Lebenszyklus auf dem neuesten Stand halten. Der unbefugte Zugriff auf nur ein Gerät kann einen Dominoeffekt auslösen, der weitreichende Netzwerkschäden verursacht und sogar die öffentliche Sicherheit bedroht, da zahlreiche IIoT-Geräte in Anwendungen wie der Gebäudeautomatisierung, dem Transportwesen, der Energieversorgung und dem Gesundheitswesen eingesetzt werden, die einen direkten Einfluss auf Menschen und ihre Gesellschaft haben. Die Anwendung eines ganzheitlichen Security-by-Design-Prinzips für den gesamten Lebenszyklus von IIoT-Geräten wird daher zu einer entscheidenden Anforderung für Gerätehersteller.

Eine weitere Herausforderung, mit der industrielle OEMs bei der Entwicklung von Lösungen für Industrie 4.0 konfrontiert sind, ist die Notwendigkeit, den Bereich der Betriebstechnologie (OT) mit ihrer IT-Infrastruktur zusammenzuführen. OT-Netzwerke erfordern jedoch eine garantierte und rechtzeitige Zustellung von Paketen und nicht den typischen Best-Effort-Ansatz, der heute in IT-Netzwerken verwendet wird.

## Lösungsansatz

Time Sensitive Networking (TSN) unterstützt bestehende IT- und OT-Geräte im selben Netzwerk und ermöglicht Gigabit-Bandbreiten bei gleichzeitiger Vereinfachung der Netzwerkbereitstellung und -verwaltung.

TSN-Funktionen erweitern das Ethernet-Switching, um planmäßigen Datenverkehr, spontanen Datenverkehr mit hoher Priorität und Best-Effort-Datenverkehr auf derselben Leitung zu unterstützen.

Feste Latenzen und minimaler Jitter in TSN-Netzwerken helfen beim Aufbau verteilter Kontrollsysteme. Echtzeit-Verkehr funktioniert zuverlässig auf demselben Kabel wie regulärer Verkehr. TSN-Funktionen funktionieren in einer einzigen Zelle und können ganze Anlagen umfassen. Mithilfe der Scheduling-Funktionen können mehrere industrielle Protokolle über dasselbe Netz betrieben werden.

OPC UA ermöglicht eine vollständige Transparenz der Fabrik bis hin zu Geräten auf Feldebene wie Sensoren und Antriebe. Es wurde mit Blick auf Vielseitigkeit und Sicherheit entwickelt.
Das gebrauchsfertige Secure Element für IIoT-Geräte bietet eine Vertrauensbasis auf IC-Ebene und bietet echte End-to-End-Sicherheit, ohne dass Sicherheitscode geschrieben werden muss. Es ist so konzipiert, dass es Industriestandards erfüllt und dem Security-by-Design-Ansatz folgt.

Darüber hinaus unterstützt das Secure Element eine späte Gerätekonfiguration im Feld, die es Geräteherstellern und Dienstanbietern ermöglicht, ihre IIoT-Geräte dynamisch mit mehreren Clouds und Dienstanbietern zu verbinden.

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

DLR Projektträger

aufgrund eines Beschlusses des Deutschen Bundestages

Da die Gerätehersteller nicht mehr mit Schlüsseln oder Zertifikaten hantieren müssen, ermöglichen Secure Elements die Aufrechterhaltung der Sicherheit von IIoT-Geräten im Feld sowie die Aktualisierung, den Widerruf oder das Hinzufügen neuer Geräteanmeldeinformationen. Dies vereinfacht die Verwaltung großer Flotten von IIoT-Geräten.

## Unser Leistungsangebot

Um die Sicherheit von IIoT-Geräten während ihres gesamten Lebenszyklus im FabOS-Kontext zu gewährleisten, wird ein Konzept für einen On- und Offboarding-Dienst für die Provisionierung von digitalen Zertifikaten vorgestellt. Darüber hinaus werden Hardware-Bausteine, die den Security-by-Design Prinzipien folgen, einschließlich Secure Elements, TSN-fähiger industrietauglicher Anwendungsprozessoren für KI-Anwendungen auf der Edge sowie TSN-Switches zu einer vollständigen Systemarchitektur für die sichere Fabrik- und Prozessautomatisierung kombiniert. Die Systemarchitektur wird anhand einer TSN-basierten verteilten Echtzeit-Motorsteuerung in Kombination mit einer bildverarbeitungsbasierten KI-Anwendung auf der Edge zur Steuerung der Motoren mit Handgesten demonstriert. Darüber hinaus wird eine hardwaregesicherte OPC UA Pub/Sub-Kommunikationsverbindung zwischen den Hardwarekomponenten verwendet, um Performancedaten der Motorsteuerung sicher anderen Netzwerkteilnehmern zur Verfügung zu stellen.

## Einordnung ins Gesamtprojekt FabOS

Die vorgestellte Lösung zeigt Ansätze für ein sicheres und echtzeitfähiges System. Durch die Verwendung von anerkannten Standards kann eine Vereinheitlichung der Kommunikation hergestellt werden und vereinfacht so die Integrationsarbeit des Inbetriebnehmers.

## Ihr Nutzen

Die verwendeten Komponenten bieten folgende Vorteile:

- Verwendung von OPC UA vereinheitlicht die Kommunikation von heterogenen Geräten
- Root of Trust durch Verwendung eines Secure Elements
- Kosteneinsparung durch Vereinfachung der Integrationsarbeit
- Kritische und unkritische Datenströme können über die gleiche Schnittstelle gesendet werden

## Zielgruppe

Produzierende Unternehmen mit heterogenen Systemlandschaften

### Werden Sie Teil der FabOS-Community

Ein Betriebssystem für die Produktion klingt interessant für Sie? Entweder weil Sie es gerne bei sich einsetzen würden oder Sie gerne bei der Entwicklung mitwirken würden?

Dann melden Sie sich für die FabOS-Community an und begleiten Sie unser Projekt:

www.fab-os.org/werde-partner

- Regelmäßige Informationen zu Neuigkeiten aus dem Projekt
- Kostenlose und bevorzugte Teilnahme an unseren Workshops
- Direkte Möglichkeit, Anforderungen und Feedback einzubringen
- Zugang zu Datensätzen und Vorlagen für Verwaltungsschalen
- Frühzeitige Erprobung entwickelter Projektsoftware

Wir freuen uns auf den Austausch und hoffen, Sie bald als assoziierten Partner im Projekt willkommen heißen zu dürfen.

Folgender Projektpartner ist an dem Exponat beteiligt:

**Ansprechpartner:**

Factory and Process Automation
NXP Semiconductors Germany GmbH
Troplowitzstraße 20 | 22529 Hamburg | Deutschland

Julia Tremp
Tel.: +49 151 40793167
Julia.tremp@nxp.com

info@fab-os.org | www.fab-os.org