



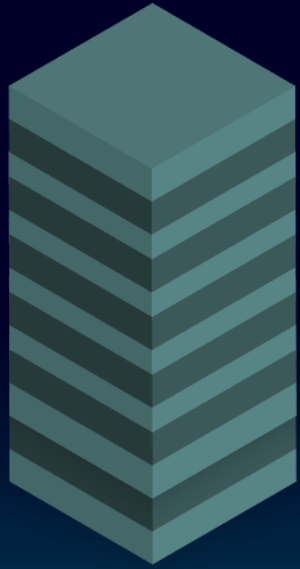
Siemens Building Products News

Kurt May, Thomas Eder

SIEMENS



- | **Was ist BACnet Secure Connect ?**
- | **Eine sichere Kommunikation für die Gebäudeautomation**



Gebäude in der Vergangenheit: **Lokal**

- Isolierte OT-Kommunikation
- Hauptsächlich lokaler Betrieb
- Geringe Angriffsfläche

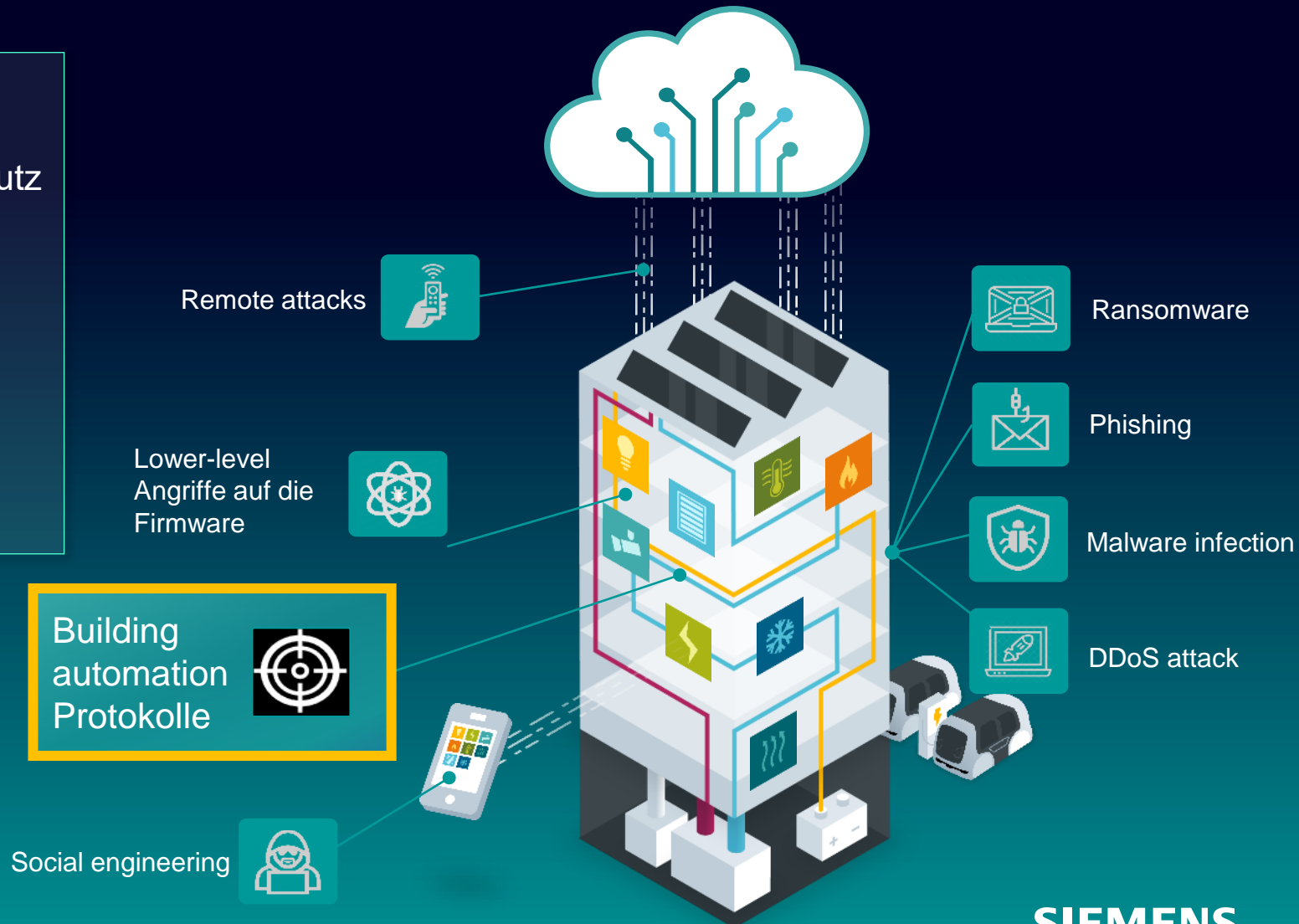
Gebäude heute: **Vernetzt**

- Konvergierte IT↔OT
- Betrieb mittels Cloud und mobilen Anwendungen
- Erhöhte Angriffsfläche

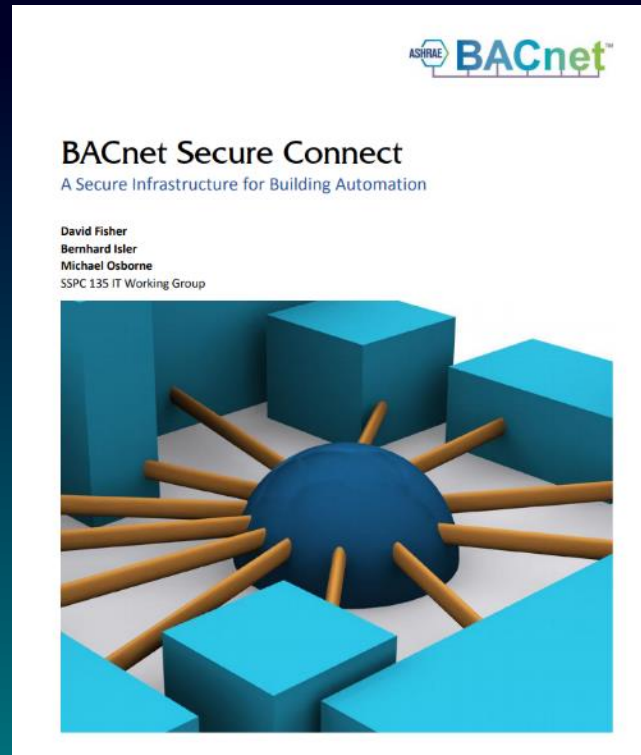


Viele Wege, ein Gebäude anzugreifen...

- BACnet stammt aus dem Jahr 1987:
- Keine Verschlüsselung → kein Datenschutz
- Keine Authentifizierung → nicht fälschungssicher
- Wird in etwa ~70% aller kommerziellen BACS verwendet
- Große installierte Basis → schrittweise Migrationsoption erforderlich



Viele Wege, ein Gebäude anzugreifen... ...und eine Möglichkeit, sich zu wehren



Genehmigt und freigegeben im November 2019

Verschlüsselte Kommunikation

Zertifizierte Geräte

Abwärtskompatibel

IT-freundlich

BACnet Secure Connect (“BACnet/SC”)

Was BACnet/SC ist

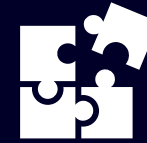
- Eine neuer BACnet **datalink** (wie BACnet/IP oder BACnet MS/TP)
- Eine verschlüsselte Kommunikation, um die M2M-Kommunikation gegen Manipulationen zu schützen
- Ein Authentifizierungsmechanismus, um den Zugriff auf ein Projekt zu beschränken
- Ein IT-freundlicher Weg für eine sichere Kommunikation in der Gebäudeautomation

Was BACnet/SC nicht ist

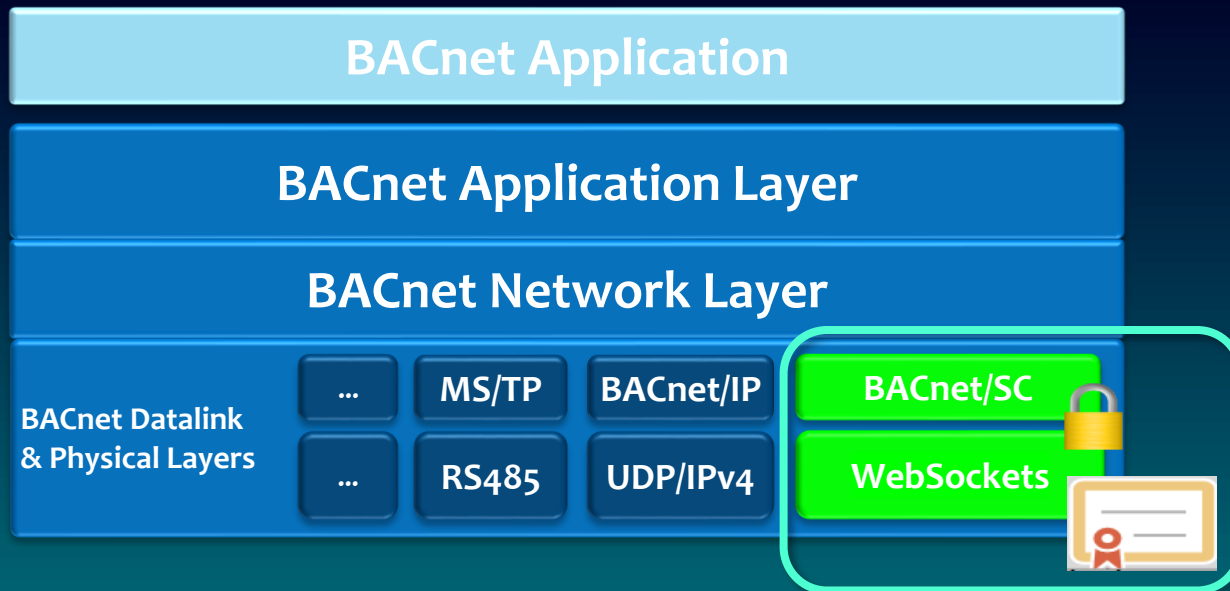
- Eine Wunderwaffe gegen alle Arten von Cybersecurity-Risiken
- Ein fein-granularer Autorisierungsmechanismus
- Etwas, das IT-Sicherheit "kostenlos" bietet...

BACnet/SC - Grundlegende Informationen

Abwärtskompatibilität

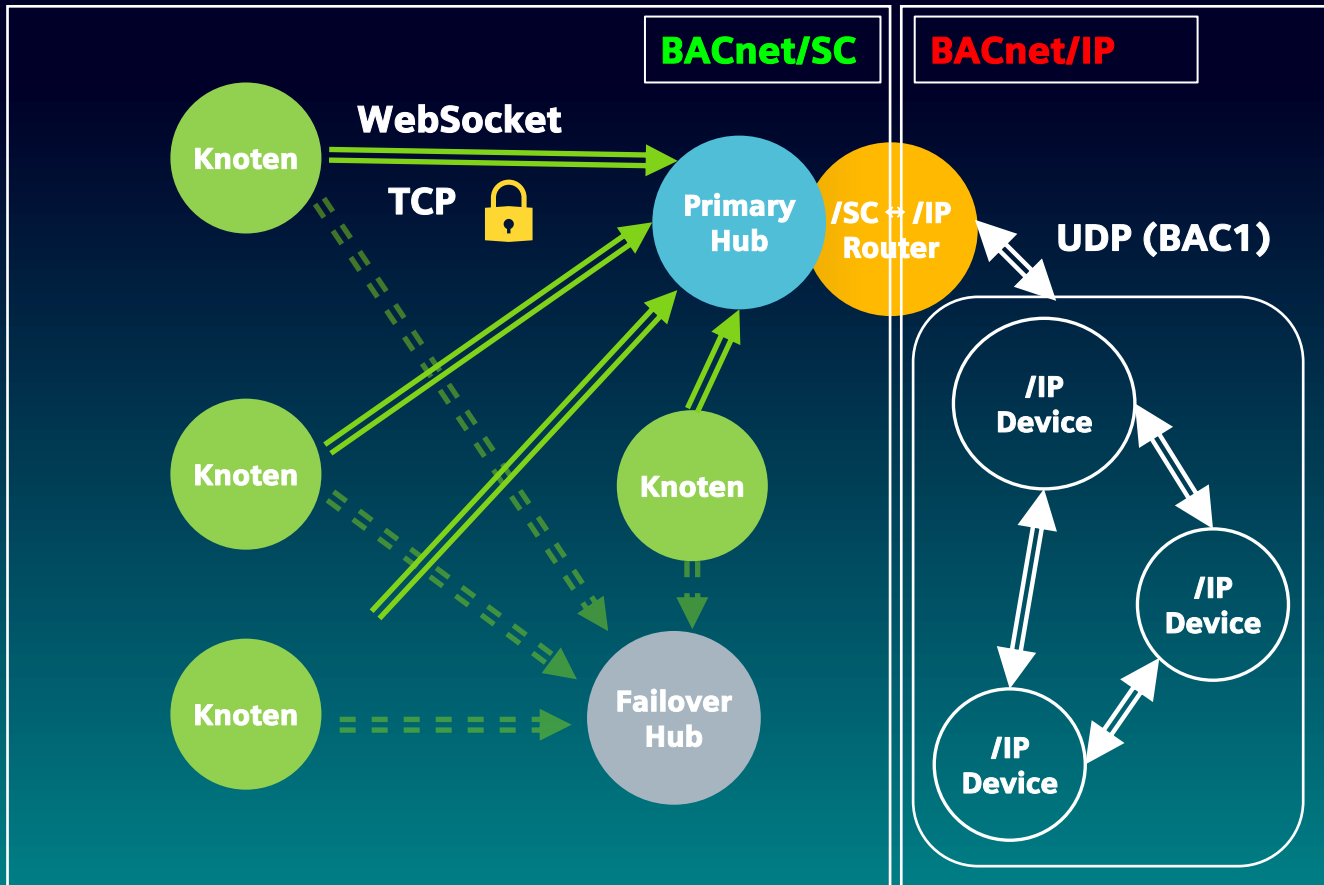


Take-Aways



- Keine Auswirkung auf die Anwendungsschicht
- Mix-and-match mit anderen BACnet Datenverbindungen
- "REMoB"
- Realisierung / Erweiterung / Migration immer auf Granularität "BACnet Netzwerk"
- Unabhängig von der BACnet Revision (zum ersten Mal in der Geschichte!)

BACnet/SC Grundlegende Informationen Topologie

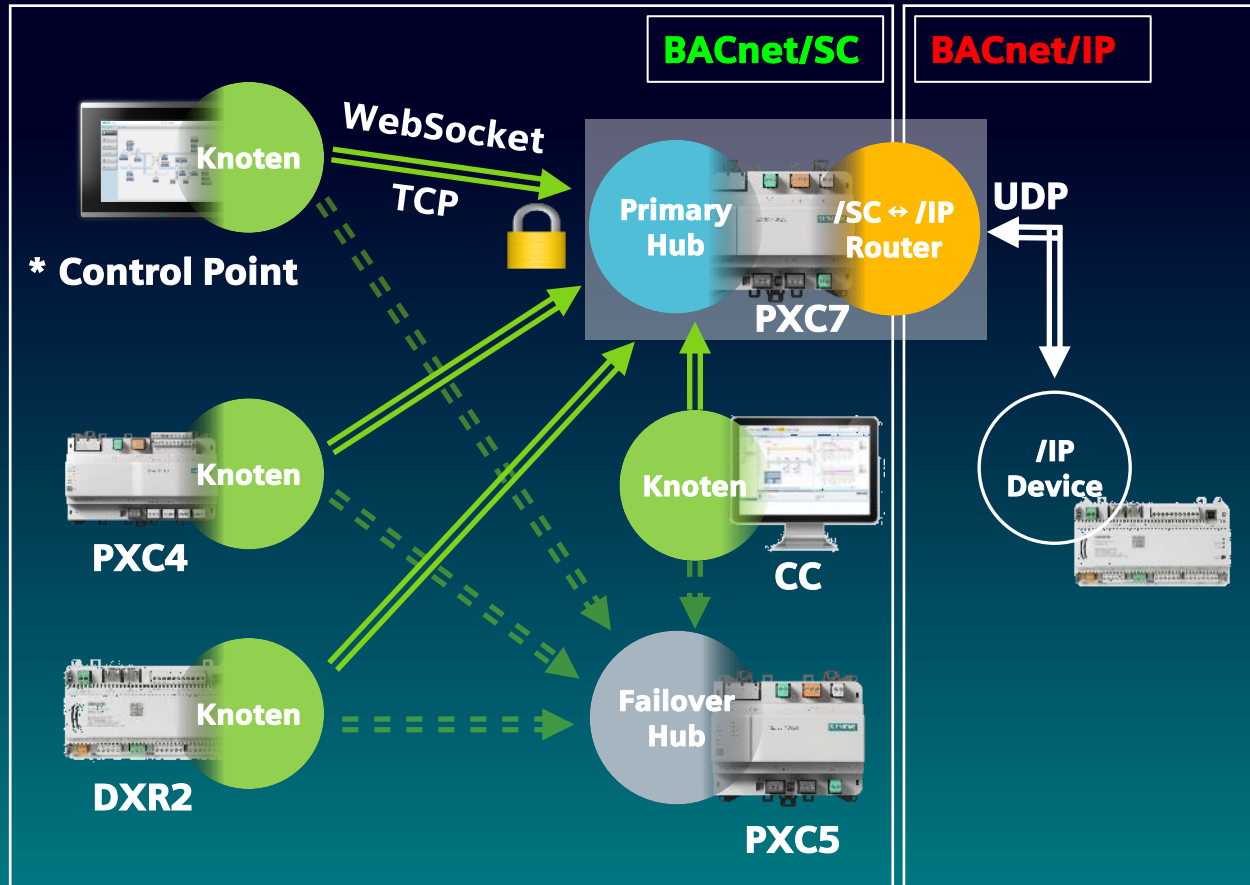


Take-Aways



- /SC setzt ein "Hub-and-Spoke"-Prinzip ein
 - **Knoten** = Endpunkte der Kommunikation
 - **Hubs** = zentrale Punkte zur Weiterleitung des Datenverkehrs
 - Failover-Hubs = Hot-Standby-Redundanz
 - Verschlüsselte Web-Sockets verwendet Hub ↔ Knoten
- /SC ist eine neue BACnet-Datenverbindung
 - verbindet sich durch BACnet-Routing mit /IP, /MSTP
 - "Hubs" sind in der Regel auch Host-"Router"

BACnet/SC Grundlegende Informationen Topologie



Take-Aways

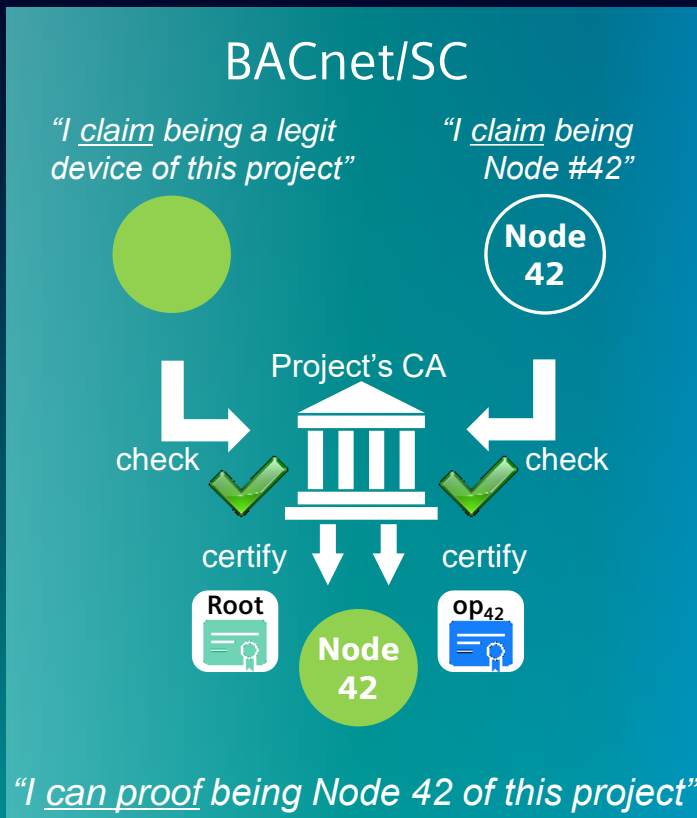


- Portfolios werden schrittweise auf BACnet/SC erweitert
- Projekte werden schrittweise zu BACnet/SC migriert
- Geräte sollen sowohl BACnet/IP als auch /SC unterstützen
- Herausforderung:
Skalierung /SC Interoperabilität in großen Netzen
Systemkonzept mit Kunden
-> Abstimmung -> Realisierung

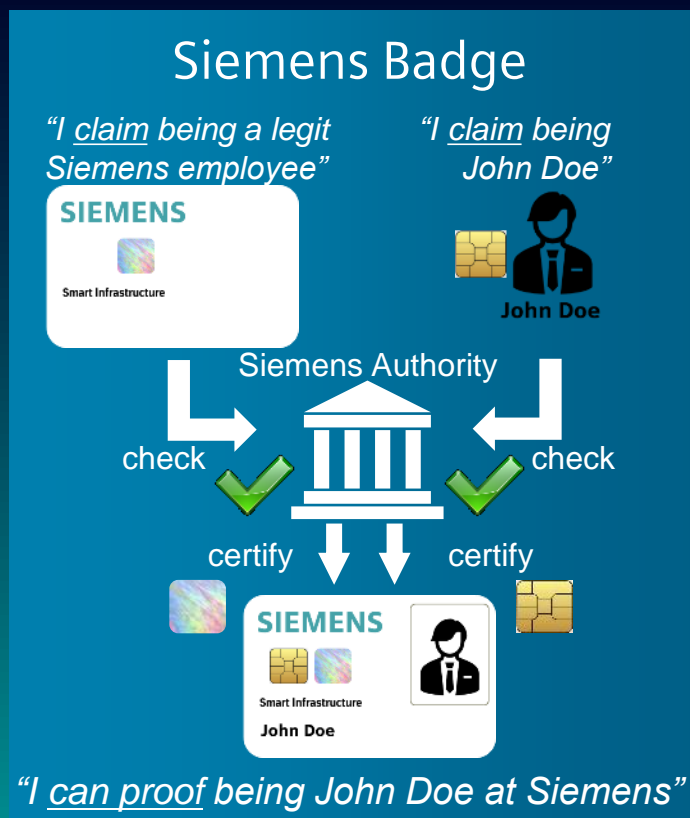
* Verfügbar für PXC und Desigo CC im ersten Schritt, die anderen Geräte sind auf der Roadmap

BACnet/SC Grundlegende Informationen Certification Authorities (“CA”)

Certification Authority



Real Life Analogy



Take-Aways

- CA ist eine vertrauenswürdige Instanz in einem Projekt
 - Stellt (gemeinsames) Root-Zertifikat aus
 - Stellt (individuelle) Betriebszertifikate aus
 - Es gibt genau eine solche CA in einem Projekt → Abstimmung erforderlich!
- Zertifikate sind verpflichtend für /SC
 - Werden für die Engineering & IBN benötigt
 - Regelmäßige Erneuerung während der Lebensdauer des Projektes erforderlich
 - IT-Best-Practices verwenden
"X.509", "TLS1.3", "WebSockets", ...

Fragen



| Kontakt

Herausgeber: Siemens AG Österreich

Kurt May

Siemensstraße 90
1210 Wien
Österreich

Telefon +43 664 80117 32783

E-Mail: kurt.may@siemens.com



- | **GAMMA instabus KNX IP Secure**
- | **Sichere KNX Kommunikation über IP**

Warum KNX-Secure-Geräte?

- Gewährleistet Schutz gegen unberechtigten Zugriff und Manipulation
- Höchster Datenschutz durch vollständig verschlüsselte Telegrammübertragung
- Nur befugte Personen erhalten Zugang zur KNX Anlage

Vorteile

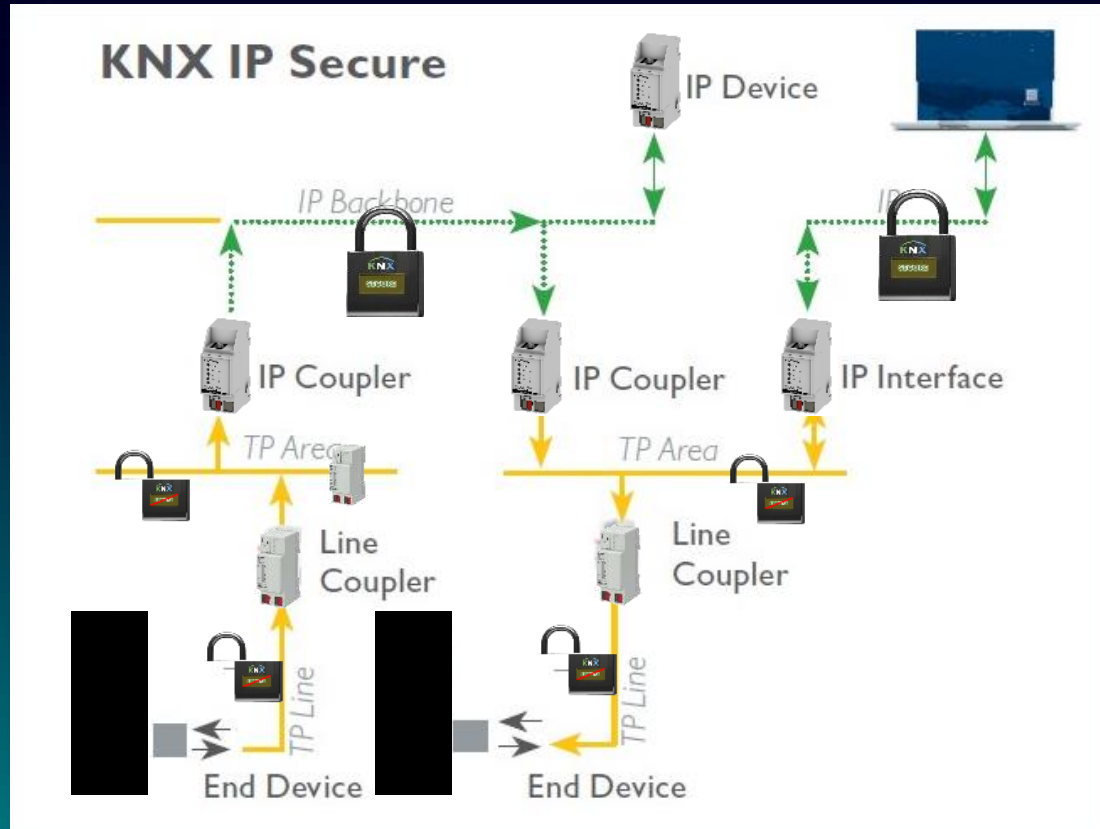
KNX IP Secure Geräte bieten im Vergleich zu herkömmlichen KNX-Geräten den Vorteil, dass Telegramme verschlüsselt werden können.

Dies gewährleistet eine zusätzliche Sicherheit für Ihre KNX-Anlage, sowohl bei Inbetriebnahme als auch während des Betriebs und das Risiko von unberechtigtem Zugriff durch Dritte wird minimiert.



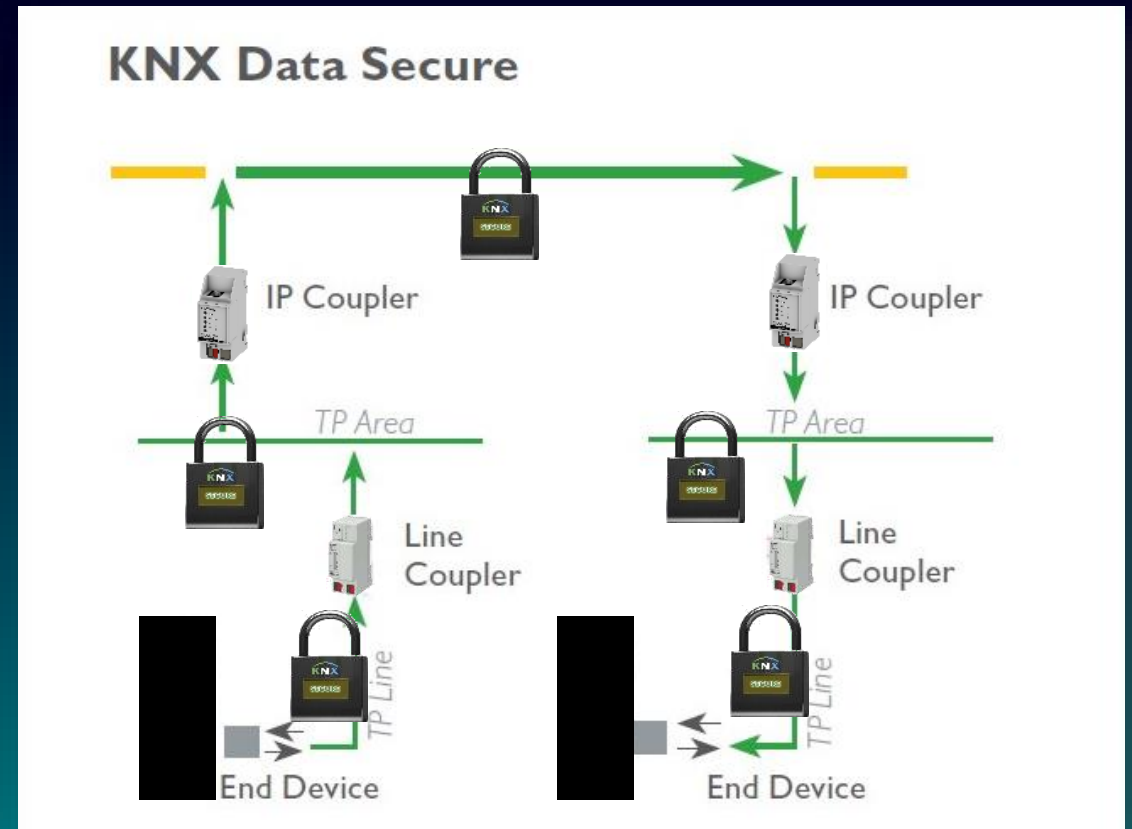
Was macht eine KNX-Installation sicher? KNX IP Secure Produkte

Gesicherte Kommunikation über KNXnet/IP



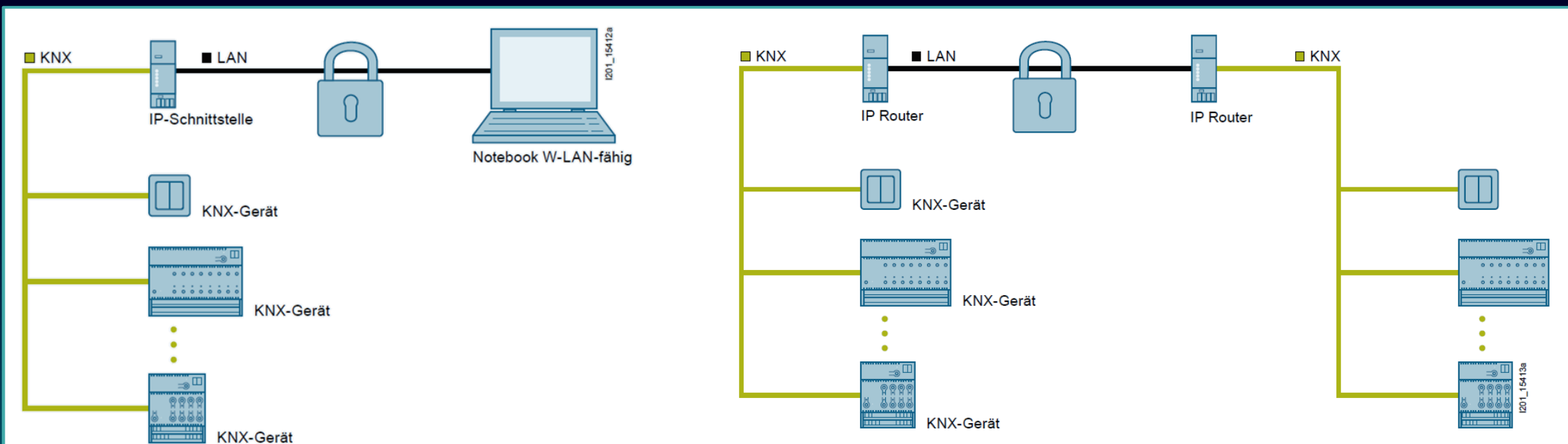
 ungesicherte Kommunikation

Gesicherte Kommunikation über KNXnet/IP und KNX TP



 gesicherte Kommunikation

KNX IP Secure Anwendungsfelder



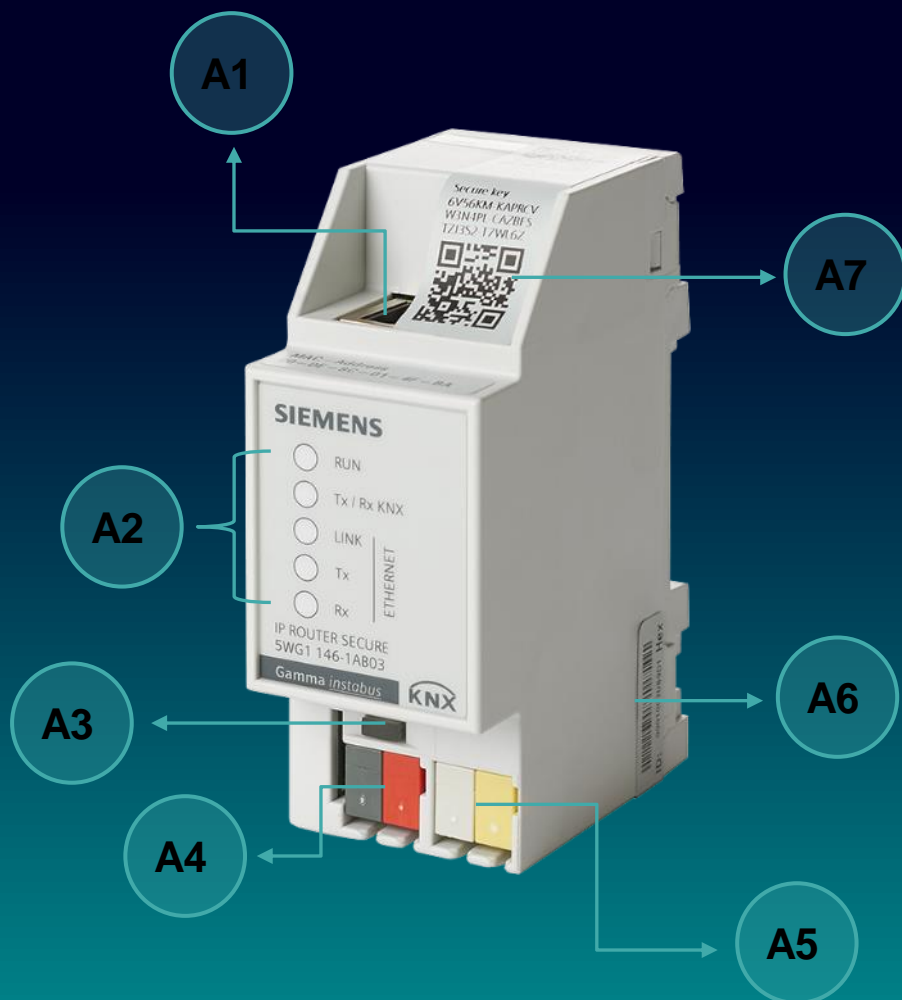
Schnittstellenfunktion zwischen PCs und KNX-Geräten für

- Inbetriebnahme und Diagnose (ETS, Zusatzsoftware,...)
- Anzeigen und Bedienen von Funktionen local oder aus der Ferne (lokales Display, Fernzugriff, Webzugriff, Smarte Geräte,...)

Datenübertragung zwischen KNX-Geräten

- Kommunikation zwischen Linien, Bereichen und Systemen
- Filtern von Telegrammen (Routing)

IP Secure-Produkte Komponenten

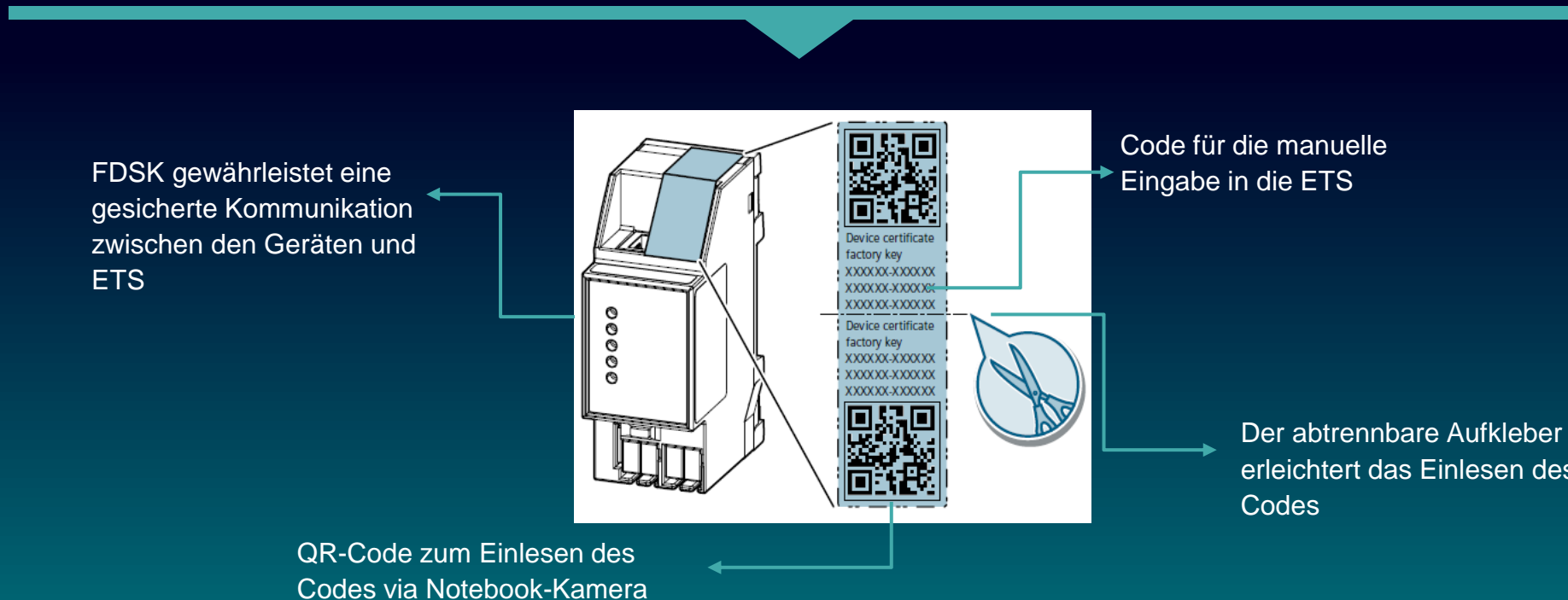


- A1** RJ45-Anschluss zur Ethernet-Anbindung; optional Power-over-Ethernet (PoE)
- A2** LEDs zur Anzeige des Betriebszustandes und Kommunikation
- A3** Programmier Taste / -LED fungiert als Lerntaste für physikalische Adressen, zum Zurücksetzen auf Auslieferungszustand sowie als LED für den Programmiermodus
- A4** KNX-Klemmen zum Anschluss an die KNX-Busleitung
- A5** Klemme zum Anschluss der Hilfsspannungsversorgung
- A6** KNX-Seriennummer zum Zuweisen der physikalischen Adressen mit der ETS
- A7** Gerätezertifikat (FDSK) zur Inbetriebnahme mit ETS im Modus KNXnet/IP Secure

IP Router Secure & IP Schnittstelle Secure

Einfache und sichere Inbetriebnahme

Gerätezertifikat (Factory Default Setup Key - FDSK) Für den gesicherten Betrieb*



* Die Inbetriebnahme im ungesicherten Modus erfolgt wie gewohnt

IP Router Secure Highlights

N 146/03 IP-Router Secure (Routing/Tunneling)

Filtern und Weiterleiten von verschlüsselten Telegrammen

Verbindung von KNX Linien mithilfe von Datennetzwerken unter Nutzung des IP

5 LED Anzeigen

Spannungsversorgung via Power-over-Ethernet



Verwendung des KNXnet/IP oder KNXnet/ IP Secure Protokolls

Einsatz als Linien-, Bereichs- oder Netzwerkkoppler

Bis zu vier KNXnet/IP Tunneling-Verbindungen für parallelen Buszugriff

Verwendung als KNX IP-Datenschnittstelle

IP Schnittstelle Secure Highlights

N 148/23 IP-Schnittstelle Secure (Tunneling)

Direkter Zugriff von jedem Punkt im IP Netzwerk auf die Installation

5 LED Anzeigen

Fernzugriff auf eine KNX-Installation

Spannungsversorgung via Power-over-Ethernet

Einfache Konfiguration über ETS

Verwendung des KNXnet/IP oder KNXnet/ IP Secure Protokolls

Einfache Anbindung von Visualisierungssystemen und Facility Management Systemen

Vernetzung von Liegenschaften



Fragen



| Kontakt

Herausgeber: Siemens AG Österreich

Thomas Eder

Siemensstraße 90
1210 Wien
Österreich

Telefon +43 664 8855 1820

E-Mail: thomas.a.eder@siemens.com

Building Product News XXII

Gesunde und produktive Räume



Erfahren Sie wie Sie mit unseren KNX Produkten und Human Centric Lighting für gesunde und produktive Räume in einer jeden Lebenssituation sorgen können.

Freitag, 25. Februar 2022, 10:00 Uhr



**Vielen Dank für Ihre
Aufmerksamkeit!**

Building Products News

SIEMENS