



MEHR SCHUTZ FÜR DIE GEBÄUDEAUTOMATION

# BACnet Secure Connect

[siemens.de/systeme-gebaeudeautomation](https://www.siemens.de/systeme-gebaeudeautomation)

**SIEMENS**

# Inhalte

Warum Gebäudeautomationssysteme besser geschützt werden müssen	3
Mehr Sicherheit und bessere IT-Anbindung für OT-Systeme	4
Einfache Bereitstellung und Geräteerkennung	5
Logische Netzwerkarchitektur von BACnet/SC	7
Das BACnet/SC-System von Siemens	8
BACnet/SC für Neubauten oder die Modernisierung von BACnet-Bestandssystemen	9
Ganzheitlicher Sicherheitsansatz für Gebäude	10
BACnet/SC-Zertifikatsverwaltung und -werkzeuge	11

# Warum Gebäudeautomations-systeme besser geschützt werden müssen

Gebäudeautomationssysteme (GA-Systeme) haben sich in den letzten Jahren technologisch weiterentwickelt. Durch die zunehmende Vernetzung in Gebäuden rücken die Betriebstechnologie (Operational Technology, kurz OT) und IT-Systeme immer weiter zusammen. Umso wichtiger ist es, beide Netzwerke ganzheitlich vor möglichen Cyberangriffen zu schützen. BACnet Secure Connect (BACnet/SC) ist ein wichtiger Bestandteil, um die höheren Sicherheitsanforderungen zu erfüllen.

Cyberbedrohungen betreffen schon längst nicht mehr nur IT-Systeme. Auch OT-Systeme, wie zum Beispiel Heizung, Lüftung und Klimatechnik (HLK), Beleuchtung, Energiezähler, Sicherheitstechnik oder Zutrittskontrolle, sind aufgrund der zunehmenden Konnektivität und der damit verbundenen größeren Angriffsfläche immer stärker gefährdet. Um das Angriffsrisiko dieser bisher oft vernachlässigten physischen Geräte zu minimieren, müssen diese stärker geschützt werden. OT-Systeme brauchen integrierte Sicherheitsfunktionen und einen manipulationssicheren Datenverkehr, um die Anlagenverfügbarkeit als wichtigstes Schutzziel zu erfüllen. Mit der Weiterentwicklung des weltweit standardisierten Netzwerkprotokolls BACnet (Building Automation and Control Network) zu BACnet/SC ist ein wichtiger Meilenstein erreicht. BACnet/SC enthält einen zusätzlichen Netzwerk-Layer für ein sicheres Datenkommunikationsprotokoll für Gebäudeautomations- und Steuerungsnetzwerke.

BACnet/SC basiert auf anerkannten und etablierten IP-Anwendungsprotokollen und auf in der IT-Branche üblichen Standardtechniken. Es integriert Sicherheit auf der Geräteebene direkt in das Kommunikationsprotokoll und verschlüsselt sämtliche Daten, die zwischen den Geräten ausgetauscht werden. Die gleiche Verschlüsselungstechnologie ist bereits zur Sicherung des Datenverkehrs im Online-Banking und anderen kritischen Anwendungen im Einsatz.

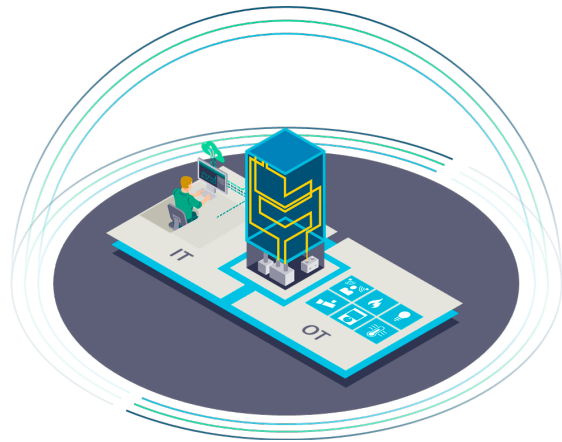
Wird die Sicherheit der OT-Systeme in einem ganzheitlichen Sicherheitsansatz mit mehrstufigen Abwehrmechanismen berücksichtigt, lassen sich nicht nur betriebliche Infrastrukturen schützen, sondern auch Angriffsvektoren schließen und das Risiko von Cyberbedrohungen aus dem OT-Bereich verringern.

Wenn vernetzte Systeme nicht ordnungsgemäß geschützt sind, können die Gebäudetechnik und die operativen Prozesse in Ihrem Gebäude gestört oder Steuerungsdaten Ihres Unternehmens manipuliert werden.

# Mehr Sicherheit und bessere IT-Anbindung für OT-Systeme

BACnet/SC ist ein wichtiger Schritt auf dem Weg zu einem integrierten und optimal geschützten GA-System, das den Anforderungen der fortschreitenden Digitalisierung im Gebäudesektor gerecht wird.

Die neue BACnet/SC-Datenverbindungsoption ist eine wichtige Erweiterung des BACnet-Standards und verbessert die Cybersicherheit und IT-Anbindung von BACnet-Systemen. Mit BACnet/SC-Systemen investieren Sie nicht nur in Cybersicherheit. Sie sorgen auch dafür, dass Ihr GA-System auf zukünftige Anforderungen vorbereitet ist und Innovationen im Bereich Smart-Building-Technologie nutzbar sind.



## Überblick über BACnet/SC ✓

BACnet/SC erweitert BACnet um eine weitere, **sichere Datenverbindungsoption**

**Verschlüsselung** des BACnet-Datenverkehrs zum Schutz der GA-Kommunikation vor Manipulation

**Authentifizierungsmechanismus** zur Einschränkung des Zugriffs auf ein Projekt

**Verbesserte IT-Anbindung** für die sichere Kommunikation in der Gebäudeautomation

## Vorteile von BACnet/SC 📊

**Investitionsschutz:** Kompatibilität mit heutigen und zukünftigen BACnet-Netzwerken und schrittweise Erweiterungs-/Upgrademöglichkeit

**Datenschutz:** Sichere End-to-End-Kommunikation auch in unsicheren Netzwerkumgebungen

**Schutz:** Ausschluss von unbefugten Geräten im Netzwerk und Man-in-the-Middle-Angriffen

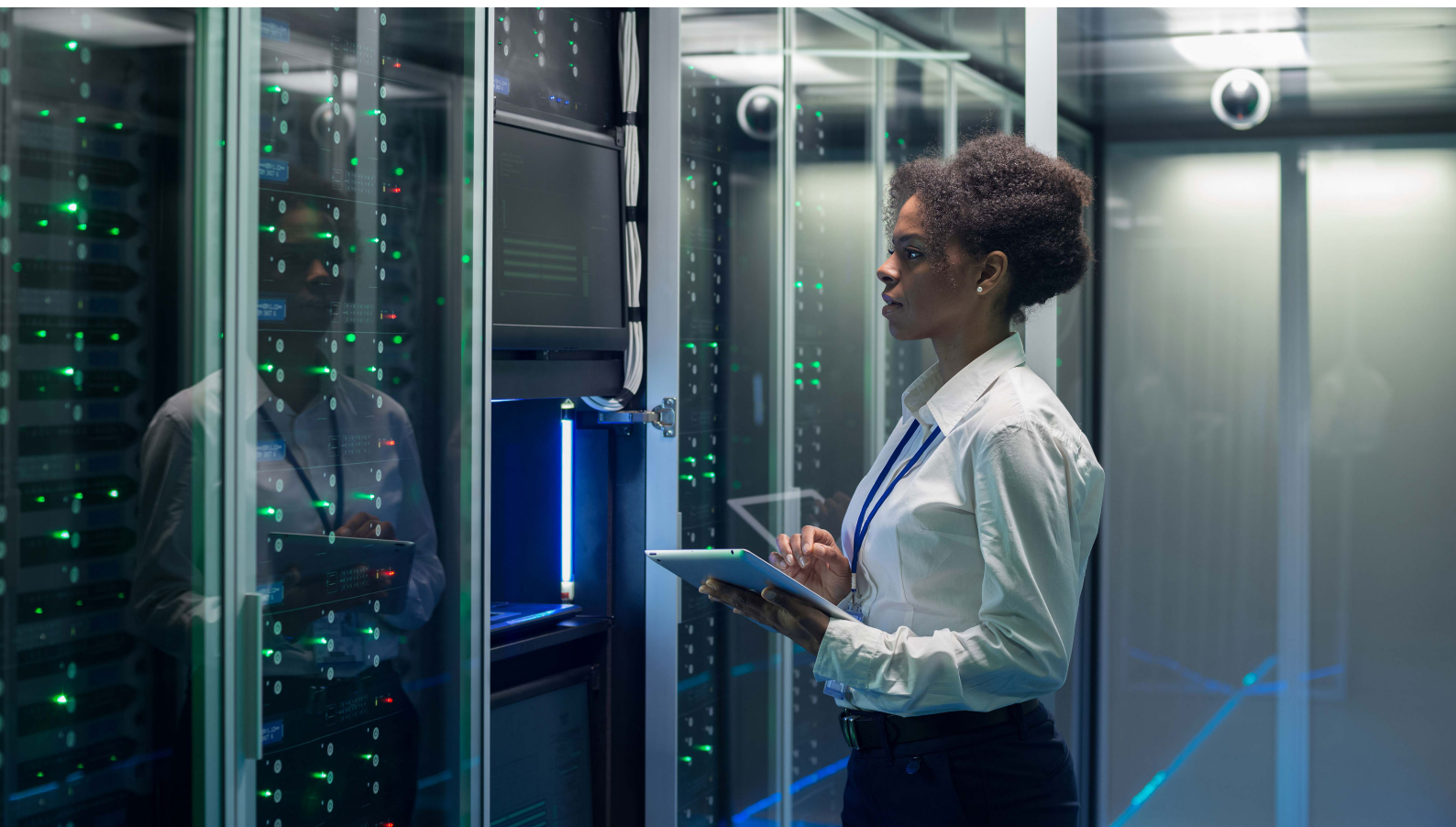
**Praktisch und kosteneffizient:** Fügt sich nahtlos in die bestehende IT-Landschaft ein

# Einfache Bereitstellung und Geräteerkennung

BACnet/SC bietet eine zusätzliche Verschlüsselung für die BACnet-Kommunikation und schreibt eine Geräteauthentifizierung anhand von Zertifikaten vor. Dadurch werden OT-Netzwerke weniger anfällig für Cyberangriffe.

Verwendet werden standardisierte und bewährte Technologien wie das WebSocket-Protokoll über HTTPS, das durch TLS v1.3 (gegenseitiger Handshake) und X.509-Zertifikate gesichert ist und mit denen IT-Expert\*innen bereits vertraut sind. Das UDP-Protokoll von BACnet/IP wurde durch das TCP-Protokoll ersetzt. BACnet/SC funktioniert problemlos mit IP-Firewalls und Network Address Translation (NAT). Zudem gibt es im IP-Netzwerk keine umfangreichen Broadcasts mehr.

Das bewährte WebSocket-Protokoll über HTTPS ersetzt UDP durch TCP.



## Leistungsmerkmale von BACnet/IP und BACnet/SC

	BACnet/IP	BACnet/SC
Standardisiertes Kommunikationsmodell	●	●
Interoperabilität zwischen Anbietern, die bei BACnet Testing Laboratory (BTL) gelistet sind und passenden BACnet Interoperability Building Blocks (BIBBs) im Protocol Implementation Conformance Statement (PICS)	●	●
Kompatibilität mit bestehenden und zukünftigen Versionen von BACnet	●	●
BACnet-Routing zwischen verschiedenen BACnet-Datenverbindungen (BACnet/IP, BACnet/SC)	●	●
Geräteinstanz-Nummern und Objektinstanz-Nummern zur Identifizierung von Geräten/Objekten	●	●
Skalierbarkeit und Flexibilität des Systems	●	●
Verbindungsloses UDP-Protokoll	●	
Verbindungsorientiertes TCP-Protokoll		●
Datenverkehr mit TLS v1.3 sicheren WebSockets Ende-zu-Ende Verschlüsselung		●
Alle Geräte werden mit X.509-Zertifikaten authentifiziert, bevor sie dem Netzwerk beitreten		●
Benötigt kein BACnet Broadcast Management Device (BBMD), um über IP-Subnetze zu gelangen		●
Funktioniert gut mit IP-Firewalls oder Netzwerk-Adressübersetzung (NAT)		●
Keine statischen IP-Adressen erforderlich		●

Da BACnet/SC lediglich eine weitere Datenverbindungsoption ist, kann es über BACnet-Routing auf bestehende BACnet-Datenverbindungen wie BACnet/IP und BACnet MS/TP zugreifen. BACnet/SC verwendet nach wie vor die gleiche Methode der Geräte-/Objektidentifikation (Geräte- und Objektinstanz-Nummern).

BACnet-Geräte der neuesten Generation unterstützen sowohl BACnet/IP als auch BACnet/SC. Viele BACnet/SC-fähige Geräte werden allerdings übergangsweise mit BACnet/IP betrieben. Bei der Umstellung der Netzwerkkonfiguration von BACnet/IP auf BACnet/SC oder beim Routing von bestehenden Datenverbindungen auf BACnet/SC ist es nicht erforderlich, eine erneute Geräte- und Objekt-erkennung durchzuführen oder Trends, Zeitpläne und Grafiken neu zu erstellen. Dadurch lässt sich bei Upgrade-Projekten viel Zeit sparen. Darüber hinaus bietet BACnet/SC weiterhin die bewährten BACnet-Leistungsmerkmale, wie zum Beispiel:

- Systemskalierbarkeit und -flexibilität
- Interoperabilität zwischen verschiedenen Anbietern, die BACnet-konform mit BTL-Listings und den entsprechenden BIBBs im PICS der Geräte sind, aus denen sich das System zusammensetzt.

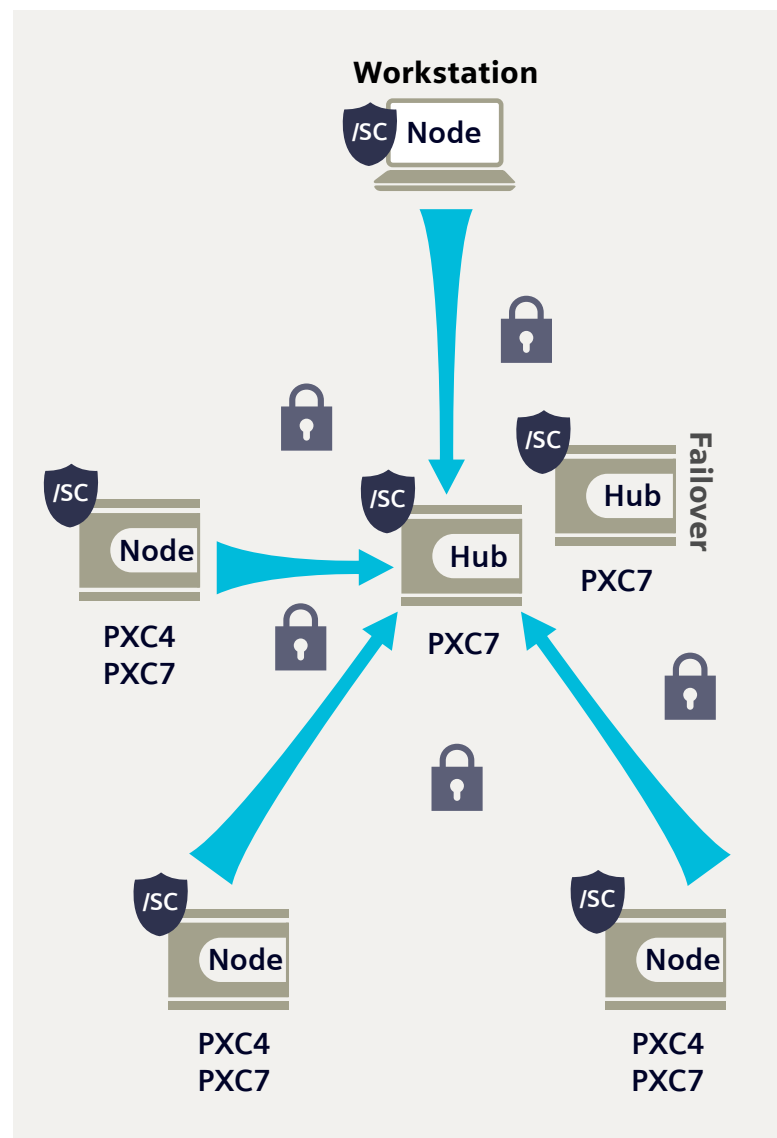


# Logische Netzwerkarchitektur von BACnet/SC

Hub und Node (Knoten) sind logische Funktionen in der Firmware von BACnet/SC-Geräten. Die Hub- und Node-Architektur von BACnet/SC erfordert mindestens ein BACnet/SC-Hub-Gerät im Netzwerk.

Der Hub ist die zentrale Stelle für die Geräteauthentifizierung. Alle anderen Geräte im BACnet/SC-Netzwerk sind Nodes. Nodes authentifizieren sich beim Hub. Der gesamte Knotenverkehr muss über den Hub laufen.

- Die Hub-Funktion wird von Systemcontrollern ausgeführt. Diese sind ausfallsicher und leistungsfähig genug, um zahlreiche gleichzeitige Knotenverbindungen sowie das BACnet-Routing zwischen verschiedenen Datenverbindungen zu unterstützen und gleichzeitig ihre Steuerungsaufgaben zu erfüllen.
- Da der Hub ein Single Point of Failure (SPOF) darstellt, wird ein zweiter Hub (ein Failover-Hub) für die Ausfallsicherheit des Netzwerks dringend empfohlen. Dies kann ein anderer Systemcontroller im Netzwerk mit BACnet/SC-Hub-Funktionalität sein.
- Wenn der primäre Hub ausfällt, sind die Nodes so konfiguriert, dass sie nach dem Failover-Hub suchen. Die Kommunikation wird ohne Unterbrechung fortgesetzt. Jedes Gerät mit Hub-Funktionalität ist standardmäßig auch ein Node und kann je nach Bedarf im Projekt verwendet werden.

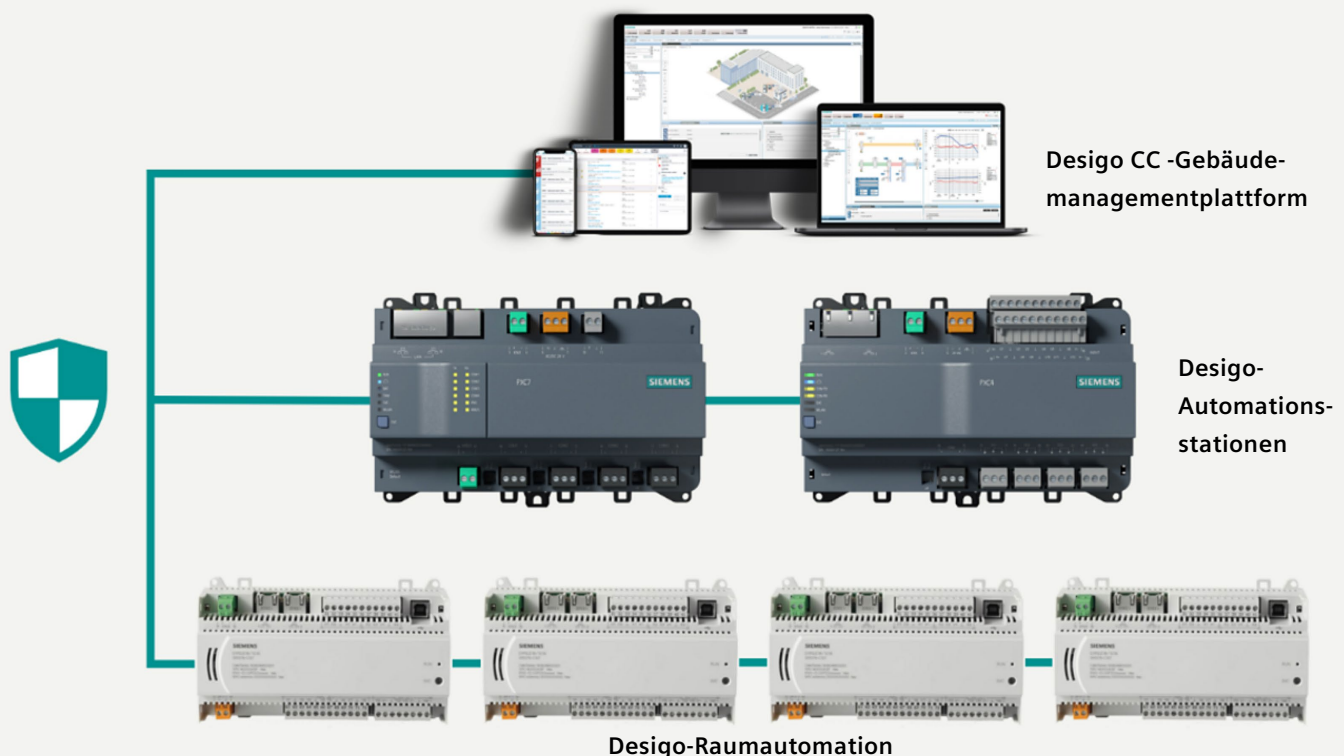


# Das BACnet/SC-System von Siemens

Mit den neuen [Desigo-Automationsstationen der PXC4..7-Reihe](#) und der [Desigo CC-Managementstation](#) bietet Siemens eine vollständige und BTL-zertifizierte Gesamtsystemlösung mit den Geräten der Profile B-BC und B-XAWS mit BACnet/SC. Werkzeuge für die Zertifikatsverwaltung mit BACnet/SC-Kommunikation runden das Siemens BACnet/SC-System ab.

Desigo PXC7 als Automationsstation ist ein Node, der bei Bedarf die Funktion des BACnet/SC-Hub oder Failover-Hub sowie BACnet/SC-Router übernehmen kann. Dank seiner vier EIA-485-Ports kann Desigo PXC7 Daten zwischen BACnet/SC- und BACnet/IP- bzw. BACnet MS/TP-Netzwerken weiterleiten. Die Desigo PXC4-Automationsstation und die Desigo CC-Managementstation fungieren als BACnet/SC-Nodes. Die PXC3- und DXR.E-Raumautomationsstation sind BACnet/SC-fähige Geräte, bei denen BACnet/SC durch ein Firmware-Upgrade aktiviert werden kann. Diese Produkte unterstützen Sie auf dem Weg zu einer sichereren GA-Infrastruktur – angefangen bei den wichtigsten Systemkomponenten.

**Eine durchgängige Komplettlösung, die Gebäudeautomation und Cybersicherheit vereint.**

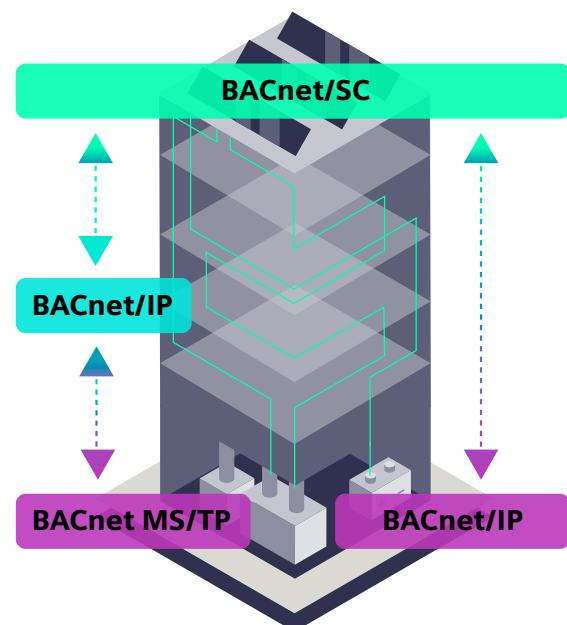


Unsere Topologie samt Beschreibungen finden Sie auf dieser Seite:  
<https://www.siemens.com/de/de/produkte/gebaeudetechnik/automation/desigo.html>

# BACnet/SC für Neubauten oder die Modernisierung von BACnet-Bestandssystemen

Für eine sichere Gebäudeinfrastruktur lohnt es sich, Produkte mit BACnet/SC-Funktion einzusetzen. Bei Neubauprojekten sollten BACnet-Systeme mit bereits verfügbaren nativen BACnet/SC-Produkten geplant werden oder Produkte eingesetzt werden, die leistungsfähig genug sind, um zukünftige Firmware-Upgrades auf BACnet/SC zu unterstützen.

Das Managementsystem und die Automationsstationen in mit der Cloud verbundenen Netzwerken oder in IT-Unternehmensnetzwerken sind die wichtigsten Komponenten, um mit BACnet/SC zu beginnen. Sie sind meist direkt zugänglich und damit am stärksten gefährdet. Es besteht weniger Bedarf, Netzwerke tief im Inneren von Gebäuden zu sichern. Ein weiterer Grund, warum es sich empfiehlt, mit BACnet/SC-Systemen bei den Automationsstationen anzusetzen: Sie bieten die erforderliche Leistung, um die BACnet/SC-Hub-Funktionalität und BACnet-Routing zwischen verschiedenen BACnet-Datenverbindungen zu unterstützen. Dank BACnet-Routing können auch bestehende BACnet/IP- und BACnet MS/TP-Produkte, die BACnet/SC nicht unterstützen, in Projekten eingesetzt werden, falls deren spezifische Funktionalität benötigt wird.



Bei BACnet-Bestandssystemen wird für Upgrade oder Erweiterung eine schrittweise Vorgehensweise empfohlen. Diese gewährleistet eine reibungslose Umstellung und sichert die bereits getätigten Investitionen der Gebäudeeigentümer in Automationsysteme und Sicherheit.

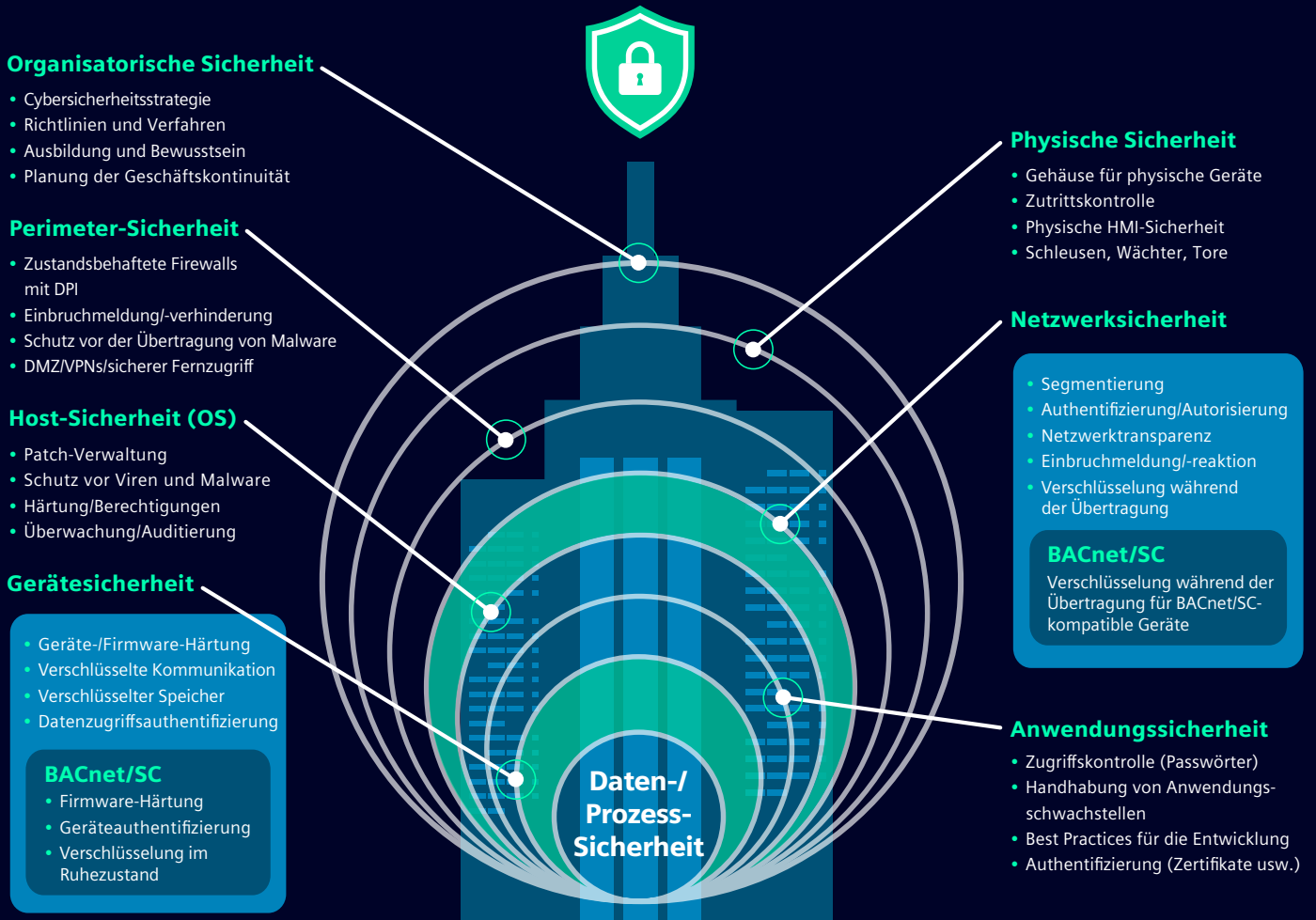
- BACnet/SC kann über BACnet-Routing (verfügbar in Desigo PXC7) an bestehende BACnet/IP- und BACnet MS/TP-Netzwerke/-Systeme angebunden werden. Bestandssysteme können bei Bedarf schrittweise und flexibel aufgerüstet werden.
- Um Upgrades durchzuführen können BACnet-Netzwerke/-Systeme in einzelne logische BACnet-Netzwerke mit unterschiedlichen Datenbindungstypen unterteilt und die logischen BACnet/SC-Netzwerkinseln über BACnet-Routing verbunden werden.
- Die verbleibenden unsicheren Netze können nachgerüstet werden, wenn die Geräte in diesen Netzwerken veraltet sind und Ersatzgeräte zur Verfügung stehen.
- Da die BACnet/SC-Kommunikation nur zwischen dem BACnet/SC-Hub und den Nodes (dem logischen BACnet/SC-Netzwerk) sicher ist, müssen Nicht-BACnet/SC-Netzwerksegmente unter Berücksichtigung der Gesamtsystemsicherheit angemessen geschützt werden.

# Ganzheitlicher Sicherheitsansatz für Gebäude

Ein effektives Verteidigungssystem ist mehrschichtig. Defense-in-Depth ist ein einfaches Prinzip: Kein Sicherheitsmechanismus kann allein vor möglichen Angreifern schützen. Gibt es allerdings mehrere unabhängige Abwehrmechanismen, ist es weitaus schwerer, in das System einzudringen. Angriffe werden so stark verlangsamt, dass sie sich für den Angreifer oftmals nicht mehr lohnen.

BACnet/SC bietet IT-Expert\*innen bereits etablierte Methoden, um OT-Systeme in ein ganzheitliches Sicherheitskonzept zu integrieren und so die Sicherheit Ihres Unternehmens zu gewährleisten. Ein sorgfältig konzipiertes und ordnungsgemäß konfiguriertes OT-Netzwerk mit BACnet/SC unterstützt einen proaktiven, mehrschichtigen „Defense-in-Depth“-Ansatz und kann bei einem Cyberangriff die letzte Verteidigungslinie eines Smart Buildings sein.

## BACnet/SC ist Teil des „Defense-in-Depth“-Konzepts

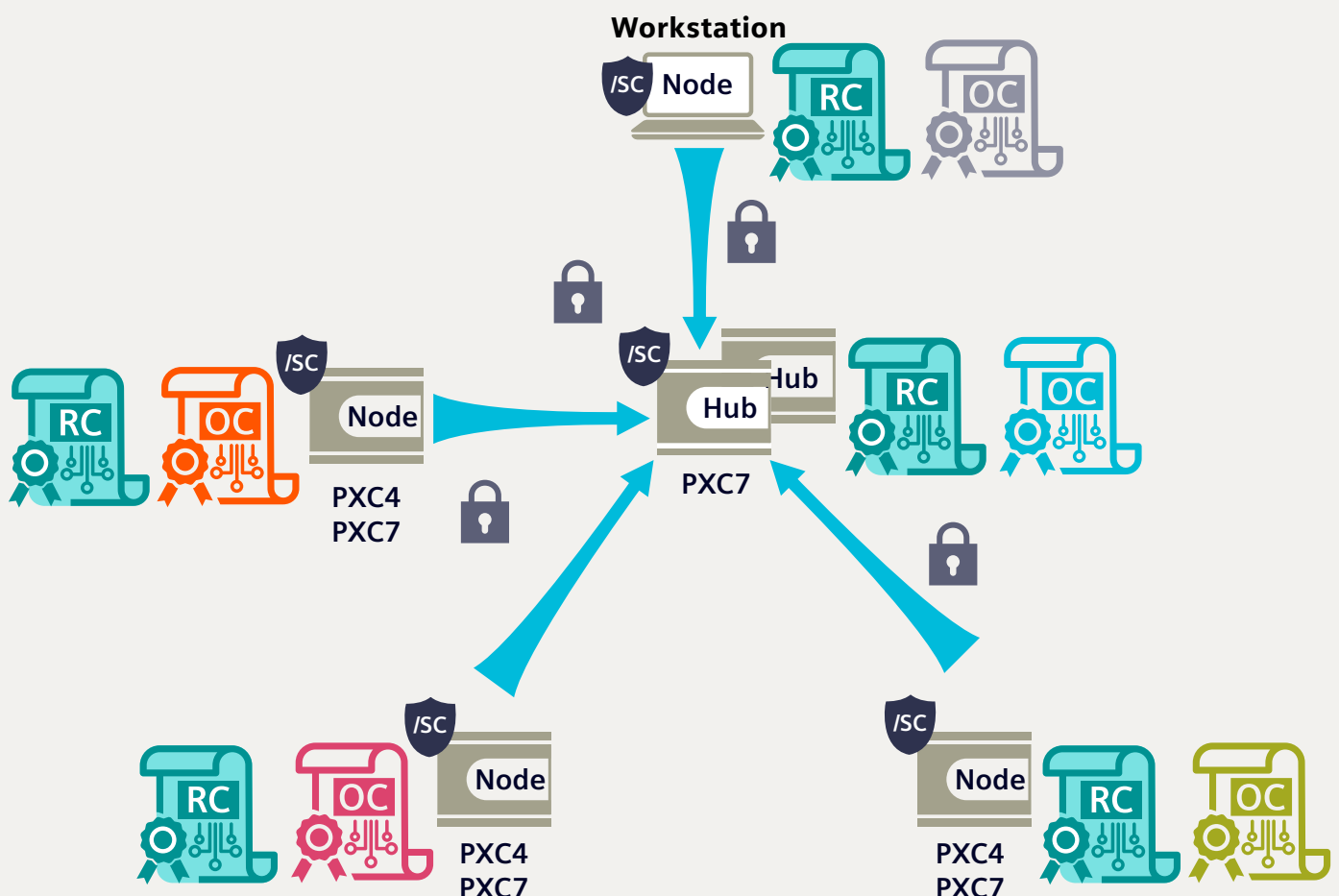


# BACnet/SC-Zertifikatsverwaltung und -werkzeuge

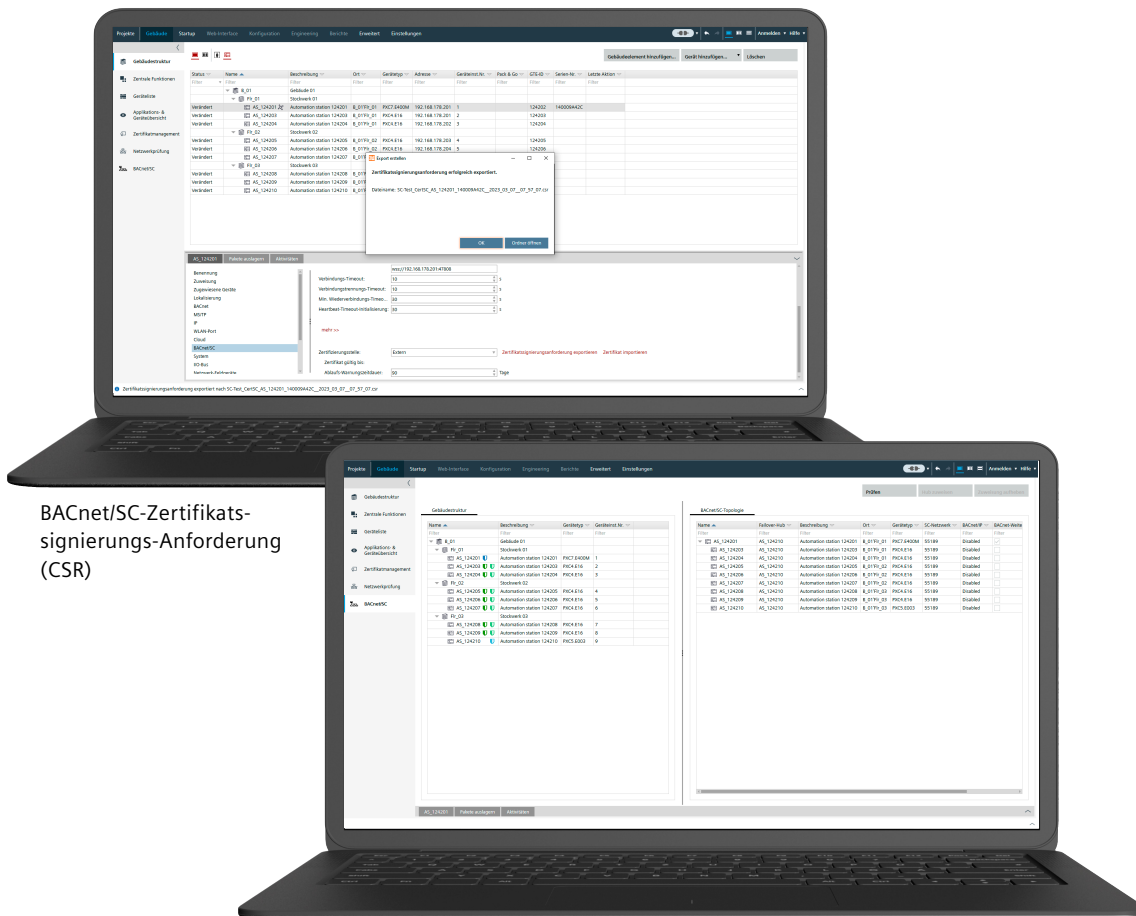
Bei BACnet/SC hängt die Geräteauthentifizierung von den richtigen Zertifikaten ab. Jedes Gerät benötigt zwei Zertifikate, um am BACnet/SC-Netzwerk teilzunehmen.

Das erste Zertifikat ist ein gemeinsames Stammzertifikat, das auf allen Geräten in einem Projekt identisch ist – unabhängig vom Gerätehersteller. Darüber hinaus gibt es die individuellen Betriebszertifikate, die pro Gerät eindeutig sind und die für die Authentifizierung von Geräten und für die Ver- und Entschlüsselung des Datenverkehrs verwendet werden. BACnet/SC verlangt, dass eine einzige Zertifizierungsstelle (CA) die Zertifikate für alle Geräte im Projekt signiert.

Siemens bietet Ihnen die kostenlose Anwendung ABT Site, deren einfache und intuitive Workflows alle Anforderungen an das BACnet/SC-Netzwerkmanagement erfüllen. ABT Site beinhaltet alle erforderlichen Funktionen, um Zertifikate auf Siemens-Geräten unter anderem zu generieren, zu signieren oder bereitzustellen. Zudem ist es möglich, BACnet/SC-Zertifikate auf Dateiebene zu importieren und zu exportieren, damit sie mit den Werkzeugen anderer Anbieter interoperabel sind oder als Vermittler zu einer von Ihnen bevorzugten Zertifizierungsstelle fungieren.



# Einfache Zertifikatsverwaltung mit ABT Site



BACnet/SC-Zertifikats-signierungs-Anforderung (CSR)

Logische Netzwerktopologie von BACnet/SC

## Vorgehen bei der Verwendung von ABT Site als Zertifizierungsstelle

Für viele Unternehmen ist es unter Umständen einfacher, die Siemens-Anwendung ABT Site als Zertifizierungsstelle zu nutzen. In diesem Fall wird ABT Site völlig eigenständig zum Erstellen, Signieren, Bereitstellen und Verlängern von Zertifikaten verwendet. So profitieren Sie von verschlüsselter Kommunikation und Geräteauthentifizierung ohne die Komplexität einer externen Zertifizierungsstelle.

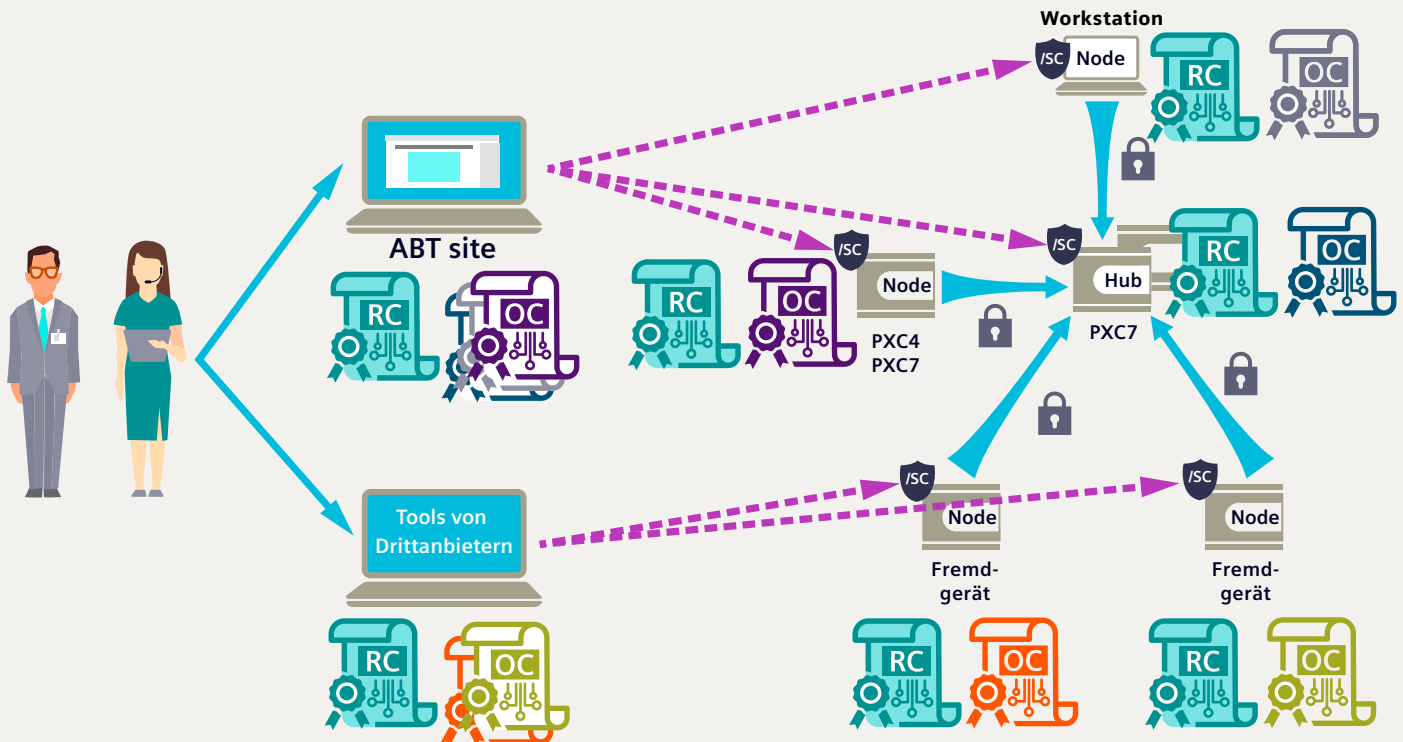
## Vorgehen bei der Verwendung einer kundenspezifischen Zertifizierungsstelle

Bevorzugen Sie eine eigene vertrauenswürdige Zertifizierungsstelle, sind zusätzliche Schritte für den Zertifikatsaustausch erforderlich. Dabei wird eine Zertifikatssignierungsanforderung (CSR) aus ABT Site exportiert und die Zertifikate werden von der bevorzugten Zertifizierungsstelle signiert. Sobald die Zertifikate von der vertrauenswürdigen Zertifizierungsstelle signiert sind, werden sie erneut in ABT Site importiert und auf Siemens-Geräten bereitgestellt.

## Enge Abstimmung zwischen IT und OT erforderlich

In beiden Fällen sollte das mit der Zertifikatsverwaltung beauftragte IT- oder Gebäudebetriebsteam die Use Cases und Verfahren definieren, die zur effizienten Sicherung des Netzwerks erforderlich sind. Ordnungsgemäß gesicherte Netzwerke erfordern eine sicherheitsbewusste Organisationskultur und engagiertes Personal, das für die Überwachung der Geräte, die Verlängerung der Zertifikate und die Koordinierung der jeweiligen OT-Anbieter am Standort zuständig ist. Diese Rolle bringt ein höheres Maß an Verantwortung mit sich, da das zuständige Team den Schlüssel zu diesem sicheren OT-Netzwerk besitzt. IT- und OT-Expert\*innen müssen somit eng zusammenarbeiten, um sicherzustellen, dass das OT-Netzwerk ordnungsgemäß überwacht und gemanagt wird.

## Workflow-Diagramm für die Zertifikatsverwaltung



Aufgrund der zunehmenden Digitalisierung und Vernetzung der Gebäudeautomation erhöht sich das Risiko für Cyberangriffe. Dies betrifft zunehmend auch den OT-Bereich. Daher ist Cybersicherheit für OT-Systeme schon längst keine Option mehr, sondern ein absolutes Muss. BACnet/SC ermöglicht die sichere Kommunikation und Authentifizierung zwischen GA-Geräten, um Cybersicherheit und eine bessere IT-Anbindung in OT-Netzwerken sicherzustellen.

BACnet/SC ist mit jedem BACnet-System kompatibel und bietet Flexibilität, Skalierbarkeit und Interoperabilität.

Siemens-Produkte und -Services erfüllen höchste Sicherheitsstandards, um die Gebäudeinfrastruktur vor möglichen Cyberangriffen bestmöglich zu schützen. Wir arbeiten stetig daran, weitere BACnet/SC-Produkte für verschiedene Gebäudeautomationsanforderungen auf den Markt zu bringen. Als zuverlässiger Partner für Cybersicherheit nehmen wir Cyberbedrohungen ernst. Unser ganzheitlicher Cybersicherheitsansatz hilft Ihnen, die Herausforderungen einer zunehmend digitalisierten Welt zu meistern.

Weitere Informationen über die Gebäudeautomationslösungen von Siemens finden Sie [hier](#).



### Wir bieten eine Reihe von Produkten und Services, die die Cybersicherheit über mehrere Systeme hinweg erhöhen:

- Cybersecurity-Services zur Bewertung der aktuellen Situation und Ausarbeitung eines Plans, um Cybersicherheitslücken zu schließen und gleichzeitig die getätigten Investitionen zu schützen
- Produkte und Systeme, die von Grund auf zur Gewährleistung der Cybersicherheit entwickelt werden, die die neuesten Technologien nutzen und durch umfassende Penetrationstests überprüft werden
- Informationstransparenz in Bezug auf Schwachstellen und Vorfälle mit zeitnahen Updates über die ergriffenen Maßnahmen
- Fachkenntnisse in den Bereichen Automation, Digitalisierung und Cybersicherheit, die internationalen Standards entsprechen und langfristigen Schutz bieten, auch wenn sich Technologien, Produkte und Systeme weiterentwickeln

Smart Infrastructure verbindet die reale mit der digitalen Welt über Energiesysteme, Gebäude und Industrien hinweg, um unsere Lebens- und Arbeitsweise durch mehr Effizienz und Nachhaltigkeit zu verbessern.

Gemeinsam mit unseren Kunden und Partnern schaffen wir ein Ökosystem, das sowohl intuitiv auf die Bedürfnisse der Menschen reagiert als auch Kunden dabei unterstützt, ihre Geschäftsziele zu erreichen.

Ein Ökosystem, das unseren Kunden hilft zu wachsen, das den Fortschritt von Gemeinschaften fördert und eine nachhaltige Entwicklung begünstigt, um unseren Planeten für die nächste Generation zu schützen.

**[siemens.de/smart-infrastructure](https://www.siemens.de/smart-infrastructure)**

**Herausgeber**

**Siemens AG**

Smart Infrastructure  
Lyoner Straße 27  
60528 Frankfurt am Main

Kundenbetreuungs-Center  
Tel. 0800 100 76 39  
[info.de.sbt@siemens.com](mailto:info.de.sbt@siemens.com)

Artikel-Nr. E10003-A38-H483 (Stand 03/2023)

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

© Siemens 2023