

**BACnet SECURE CONNECT**

# OPTIMAL GESCHÜTZTE GEBÄUDEAUTOMATION



**BACnet/SC  
INSIDE**

## **BACnet/SC**

**Optimal geschützte Gebäudeautomation**

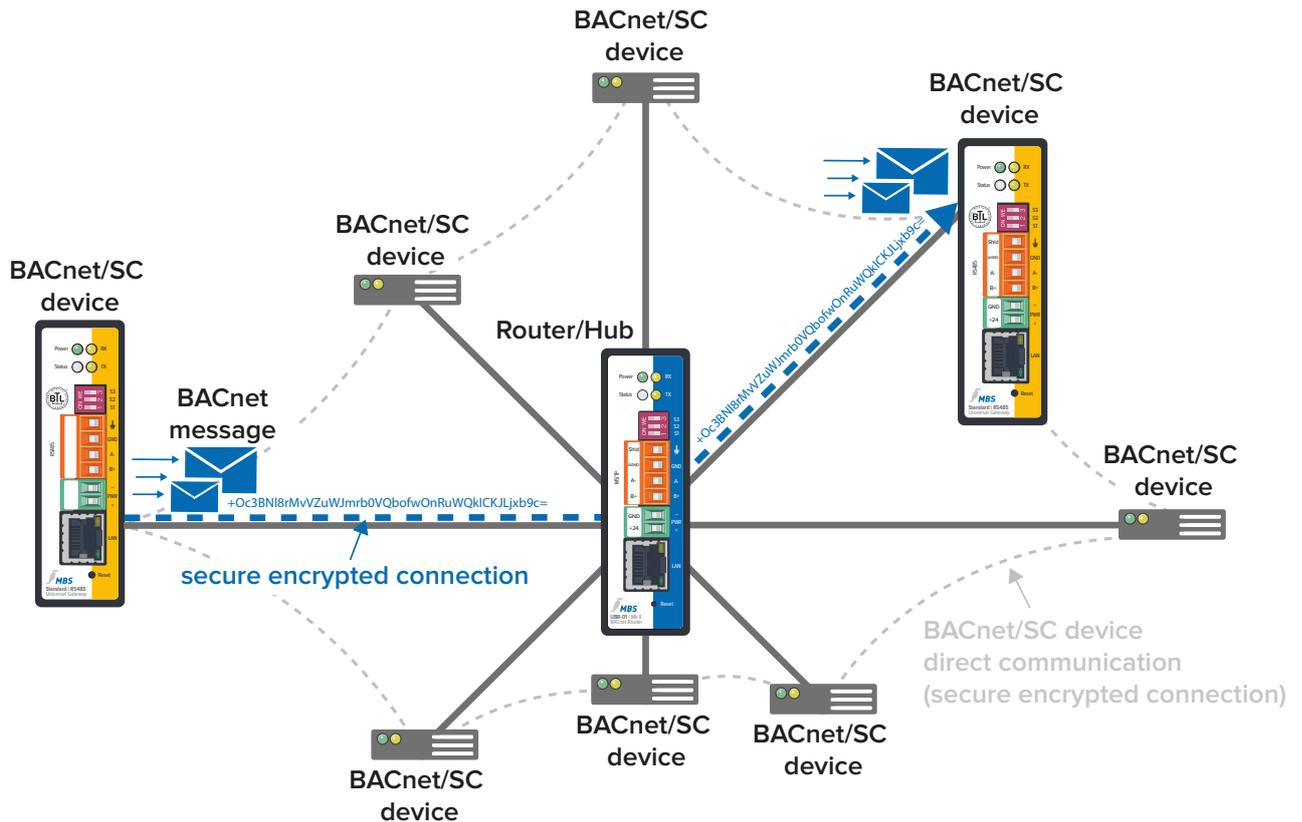
*Etwa 25 Millionen Geräte tauschen derzeit ihre Daten via BACnet aus, dessen erste Version 1995 veröffentlicht wurde. Nun besitzt der herstellerübergreifende Kommunikationsstandard seit kurzem eine eigene Sicherheitsinfrastruktur und ist damit fit für die Anforderungen der Digitalisierung.*

Abgeschlossene Netzwerke und lange Innovationszyklen – die Gebäudeautomation hatte zunächst ganz andere Anforderungen an die Betriebssicherheit als die Informationstechnologie (IT). Doch Internet-Technologien, das Zusammenwachsen von IT und Gebäudeautomation (GA) sowie Cloud-basierte Anwendungen erfordern ein hohes Maß an Schutz für die Kommunikation – wie Zugangsbeschränkung, Authentifizierung, Autorisierung und Verschlüsselung.

Weitere Informationen finden Sie unter [www.mbs-solutions.de](http://www.mbs-solutions.de)

# BACnet/SC

Optimal geschützte Gebäudeautomation



## Risiken minimieren

Hinzu kommt die KRITIS-Strategie der Bundesregierung. Sie hat sich zum Ziel gesetzt, die kritischen Infrastrukturen zu schützen, die Staat, Wirtschaft und Gesellschaft mit zentralen Gütern bzw. Dienstleistungen versorgen. Ob Flughafen, Chemiefabrik oder kommunale Liegenschaft – immer mehr GA-Betreiber müssen nachweisen, dass sie Versorgungssicherheit gewährleisten können. Dies betrifft auch BACnet-Netzwerke, die bisher aber nur mit hohem Aufwand entspre-

chend abgesichert werden konnten. Mit BACnet Secure Connect (BACnet/SC) gibt es nun eine Technologie, um sichere Kommunikationsverbindungen mit vergleichsweise geringem Aufwand herzustellen. Denn was in der IT üblich ist, sorgt künftig ebenfalls für die Netz- und Informationssicherheit der Gebäudeautomation.

Um diesen Prozess erfolgreich abzuschließen, sind einige Herausforderungen zu meistern. So ist das Sicherheitsbewusstsein in der Gebäudeautomation längst noch nicht so

ausgeprägt wie in der IT. Wer etwa das Internet auf der Suche nach ungesicherten BACnet-Netzwerken durchforstet, wird schnell – und oft – fündig. Gleichzeitig lässt sich die Gebäudetechnik nicht ohne weiteres an die Security-erprobte IT-Administration übergeben, ohne die Gewährleistung der Gerätehersteller aufs Spiel zu setzen. Gefragt sind deshalb pragmatische Wege, um den neuen Standard so zu implementieren, dass die Betreiber ihn problemlos anwenden können. Dementsprechend verwendet er jetzt mehrere Mechanismen, die sich in der Informationstechnologie bewährt haben.

### Vom Hub zum Knoten

Zunächst einmal verändert sich die Netzwerk-Topologie mit BACnet/SC sichtbar. Bisher wurde der initiale Verbindungsaufbau im BACnet mit Broadcasts vollzogen, teilweise dann mit Unterstützung von sogenannten BACnet Broadcast Management Devices (BBMD) – eine Methode, die in der IT nicht üblich ist. Deshalb wurde für die Konfiguration nun ein anderer Ansatz gewählt: Jedes Netzwerk erhält einen zentralen Punkt, den sogenannten Hub. Er steuert den Datenverkehr zwischen einer beliebigen Anzahl von Nodes (Endgeräten). Darüber hinaus übernimmt er die Analyse des Datenverkehrs, um festzustellen, ob Informationen an einen einzigen oder alle Nodes weitergeleitet werden sollen. Für die direkte Kommunikation zwischen zwei Nodes lässt sich außerdem eine direkte Verbindung schalten.

Zugleich enthält BACnet/SC einen Failover-Mechanismus, der sicherstellt, dass das System auch dann funktionsfähig bleibt, wenn der Hub ausfällt oder zwecks Wartung ausgeschaltet ist. Diese neue Topologie vereinfacht Konfigura-

tion, Inbetriebnahme und Verwaltung erheblich. Gleichzeitig werden BBMD sowie deren Konfiguration überflüssig. BBMD sowie deren Konfiguration überflüssig.

### Verschlüsselung und Zertifikate

Für die geschützte Datenübertragung wird TCP (Transmission Control Protocol) mit WebSocket verwendet – zwei zuverlässige Mechanismen auf Basis des Internet-Protokolls IP, das in der IT nahezu flächendeckend genutzt wird. TCP/IP löst die bisher von BACnet verwendete Netzwerkprotokollschicht UDP (User Data Protocol) ab und für eine abhörsowie fälschungssichere Kommunikation wird TLS eingesetzt. TLS (Transport Layer Security) ist als Grundlage für den sicheren Webzugriff (https) in der IT ebenfalls weit verbreitet.

Bei der Verschlüsselung ist zu beachten, dass für die notwendigen digitalen Zertifikate ein unternehmensweites Procedure angelegt werden muss. Die für das Internet im Rahmen von Public-Key-Infrastrukturen zuständigen Zertifizierungs- und Registrierungsstellen sind in BACnet/SC nicht vorgegeben. Damit kann ein GA-Betreiber seinen individuellen Netzwerkstrukturen Rechnung tragen.

Für die problemlose Implementierung in vorhandene Netzwerke wurden die Sicherheitsmechanismen als zusätzlicher Data Link Layer in BACnet definiert. Zudem ist der neue Standard in der aktuellen Revision 22 abwärtskompatibel. Das hat den Vorteil, dass die bereits vorhandene Ausstattung über entsprechende Router grundsätzlich mit neuen BACnet/SC-Geräten kommunizieren kann. Für Investitionssicherheit ist also gesorgt.

**Wer die eher langfristigen Innovationszyklen in der Gebäudeautomation auch auf die Einführung von Secure Connect projiziert, unterschätzt den Handlungsdruck, der durch aktuelle Trends wie Cloud-Services oder Internet of Things befeuert wird.**

## BACnet/SC

Optimal geschützte Gebäudeautomation

### Jetzt beginnen!

BACnet/SC ist noch jung. Es dauert sicherlich einige Jahre, bis der Standard in Deutschland und Europa flächendeckend ausgerollt ist. Erst einmal abzuwarten, ist dabei aber keine Option. Vielmehr sollten Betreiber jetzt aktiv werden, denn Sicherheit wird nicht allein dadurch geschaffen, dass man ein Netzwerk mit BACnet/SC-fähigen Geräten aufbaut oder ergänzt. Vielmehr ist es notwendig, ein Sicherheitsbewusstsein zu schaffen, das alle mit einem BACnet-Netzwerk befassten Personen einschließt.

Betreiber sollten sich zudem mit den Details der Revision 22 vertraut machen, um den Umstieg zu planen: Was bedeutet es, von UDP auf auf IP mit TLS umzusteigen? Was ist aus technischer Perspektive notwendig, um den Übergang möglichst reibungslos zu gestalten? Sind zusätzliche Geräte oder Leitungsstränge nötig? Was ist zu tun, um digitale Zertifikate zu erstellen, zu unterzeichnen und auf die Feldgeräte zu laden? Welche Tools stehen für den Wechsel zur Verfügung? Wo kann man von den Mechanismen der bestehenden IT profitieren?

Was die neue Produktpalette betrifft, so ist BACnet/SC eine Technologie, die die meisten GA-Hersteller künftig implementieren werden. Kleinere Unternehmen sind dabei möglicherweise schneller mit neuen Produkten am Markt als große. Vielleicht lohnt es sich auch, nach Herstellern Ausschau zu halten, die an der aktuellen Revision mitgearbeitet haben. Außerdem kann es für Liegenschaftsbetreiber sinnvoll sein, sich in allgemeinen oder unternehmensspezifischen Schulungen Beratung einzuholen. Auf diese Weise wird es gelingen, BACnet/SC in der eigenen Liegenschaft erfolgreich anzuwenden.



Sie benötigen Unterstützung zu BACnet/SC?

Sprechen Sie uns an!

+49 21 51 72 94-0  
vertrieb@mbs-solutions.de

Imprint: **Managing Director:** Martin Brust-Theiß, Gerhard Memmen-Krüger, Nils-Gunnar Fritz  
**Register court:** Krefeld HRB 3337, USt-IdNr.: DE 270 148 529, Headquarters: Krefeld  
**Responsible for contents according to § 6 MDSV:** Martin Brust-Theiß, Gerhard Memmen-Krüger, Nils-Gunnar Fritz

\*Dieses Produkt ist CE-Zertifiziert

\*Änderungen der Technischen Daten vorbehalten



**PLUGFEST**  
BACnet/SC

### EINLADUNG ZUM VIRTUELLEN PLUGFEST MIT BACnet/SC

Eine Testumgebung für die sichere Kommunikation mit BACnet/SC, die auf Initiative von Delta Controls mit der MBS GmbH aufgesetzt wurde, steht nun für alle Hersteller bereit. „Sie sind herzlich eingeladen, sich kostenfrei mit unserer virtuellen Plattform zu verknüpfen“, sagen die beiden BACnet/SC-Pioniere.

<https://www.mbs-solutions.de/bacnetsc-plugfest>

