BACnet Secure Connect

Der Umstieg auf BACnet/SC

Um BACnet Secure Connect (BACnet/SC) in der Gebäudeautomation (GA) zu nutzen, könnte ein Liegenschaftsbetreiber natürlich flächendeckend eine Infrastruktur aus BACnet/SC-fähigen Geräten aufbauen. Führt man sich aber vor Augen, dass derzeit circa 25 Millionen Endgeräte ihre Daten via BACnet übertragen, wird schnell deutlich, dass deren kompletter Austausch einen erheblichen Aufwand bedeuten würde.

Wer stattdessen vielleicht auf ein – derzeit noch nicht absehbares – Update für seine Bestandsgeräte hofft, sollte bedenken, dass die vorhandene Hardware möglicherweise nicht für die Rechenleistung ausgerüstet ist, die BACnet/SC benötigt.

Deshalb ist es sinnvoll, eine Transition zu planen: mit einer Kombination aus der vorhandenen BACnet/IPv4-Infrastruktur (Internet Protocol Version 4) plus BACnet/SC-fähiger Hardware. In die herkömmliche Infrastruktur integriert, stellt diese nicht nur eine Brücke zwischen BACnet und BACnet/SC her. Vielmehr lässt sich damit der Datenaustausch via BACnet/IP physikalisch abkapseln. Auf diese Weise kann in der Gebäudeautomation für sichere, verschlüsselte Datenkommunikation gesorgt werden.

Die folgenden drei Grafiken stellen gängige Netzwerk-Topologien für die Gebäudeautomation mit BACnet dar und sollen Anregungen geben, wie der Umstieg auf BACnet/SC gelingen kann.

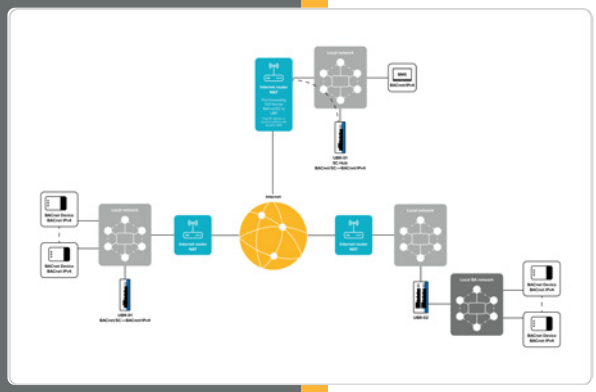
Grundsätzlich gilt: Um ein herkömmliches Netzwerk fit für BACnet/SC zu machen, muss seine Topologie verändert werden. Dafür erhält jedes Netzwerk bei der Konfiguration einen zentralen Punkt, den sogenannten Hub. Dieses Zentrum

- steuert den Datenverkehr zwischen einer beliebigen Anzahl von Endgeräten und
- übernimmt die Analyse des Datenverkehrs, um zu überprüfen, an wie viele Endgeräte die Informationen weitergeleitet werden sollen.

Der Universal-BACnet-Router (UBR) von MBS kann diese Rolle übernehmen.
Im lokalen Netzwerk der Leittechnik angesiedelt, wird das Gerät bereits seit längerem für die Umsetzung der BACnet-Netzwerk-Topologien ISO 8802-2 (auch als BACnet/Ethernet bekannt), BACnet/IP und MS/TP (serielle BACnet-Netzwerke auf der Basis von RS485) verwendet. Mittlerweile unterstützt es auch die aktuelle BACnet Revision 22 und ist damit für den Aufbau der innovativen Sicherheitsstruktur BACnet/SC geeignet. Der UBR-01 enthält eine Netzwerkkarte, der UBR-02 zwei. Welches Gerät zum Einsatz kommen kann, hängt von den konkreten Gegebenheiten ab.

MBS®

Anlagenübergreifend via Internet mit BACnet/SC verbinden



Die Ausgangssituation

Eine Zentrale mit weltweit verteilten Standorten, die via Internet miteinander vernetzt sind. Derzeit wäre der Datenaustausch in der Gebäudeautomation über BACnet/IPv4 nur möglich, wenn alle Standorte über VPN verbunden würden. Anwendungsbeispiele sind etwa ein Unternehmen mit weltweit verteilten Standorten, eine Behörde mit angeschlossenen Schulen und Turnhallen oder eine Supermarktkette mit ihren Filialen.

In der Zentrale befindet sich die Gebäudeleittechnik (GLT), die auf die gebäudetechnischen Anlagen zugreifen soll. Die Schnittstelle zum World Wide Web bildet ein Internet-Router mit einer Firewall.

Die Herausforderung

Der Datenaustausch über IPv4 läuft unverschlüsselt ab. Zudem wird das Steuerungsprotokoll DHCP (Dynamic Host Configuration Protocol) für den automatischen Bezug von IP-Adressen – vorteilhaft bei der Verwaltung großer Netzwerke – nicht unterstützt. Um solche GA-Netze abzusichern, war bisher der aufwändige Aufbau von VPNs (Virtual Private Network) erforderlich.

Was tun?

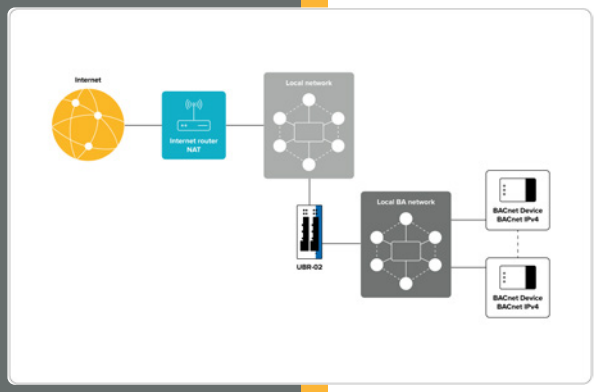
In diesem Beispiel übermittelt der Internet-Router die Daten an den UBR-01, der mit seiner integrierten Netzwerkkarte zum einen als Medienkonverter das Datenprotokoll BACnet/IPv4 in BACnet/SC übersetzt. Zum zweiten verschlüsselt er die Datenkommunikation.

Der Anschluss der Zentrale

Der Internet-IP-Router der Zentrale verfügt zum Internet hin entweder über eine statische IP-Adresse, oder seine dynamische Adresse ist über dynamisches DNS auflösbar. Eingehende Datenpakete werden über einen festgelegten Port an einen UBR-01 weitergeleitet (Port Forwarding). Der UBR-02 fungiert hier als SC-Hub und als BACnet-Router, um eine GLT mit BACnet/IPv4 weiter verwenden zu können.

Der Anschluss der Standorte

Unterhalb der zentralen Leitstelle sind zwei Versionen dargestellt, wie in diesem Szenario die gebäudetechnischen Anlagen an den verteilten Standorten an die Leittechnik angeschlossen werden können.



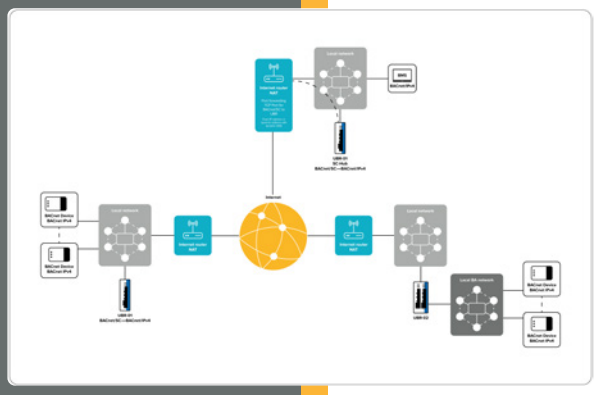
Beschreibung der Grafik rechte Seite

Auf der rechten Seite wird für die Datenübertragung zwischen lokaler Anlage und Internet ein Router eingesetzt, beispielsweise ein IP-fähiger DSL-Router. Dieser muss nicht Port-Forwarding-fähig sein. Das lokale Netzwerk umfasst nicht nur ein eigenes Netzwerk mit BACnet/IPv4-fähigen Devices für die Gebäudeautomation, sondern auch andere Endgeräte, wie etwa PCs in der Verwaltung. Die Kommunikation ist nicht abgetrennt, was bedeutet: Die anderen Geräte im Netzwerk können den IPv4-Traffic in BACnet sehen und gegebenenfalls darauf Einfluss nehmen.

Um diesen Standort fit für BACnet/SC zu machen, kann ein UBR-02 eingesetzt werden, der zwei Netzwerkkarten enthält. Eine der Netzwerkkarten routet die Daten in das lokale Netzwerk für die Gebäudeautomation, deren Endgeräte damit abgetrennt von den anderen Geräten im restlichen lokalen Netzwerk und somit abgesichert sind. Die zweite Netzwerkkarte verbindet über den lokalen Internet-Router das Standort-Netzwerk mit dem BACnet/SC-Hub in der Leitstelle. Auf diese Weise ist auch in der Kommunikation zwischen Standort und Zentrale für verschlüsselte Datenübertragung gesorgt.

Fazit

Wenn in einem Standort nur ein einziger Internet-Anschluss vorhanden ist, der von dem GA-Netz mitgenutzt wird, kann der UBR-02 größtmögliche Sicherheit herstellen.



Beschreibung der Grafik linke Seite

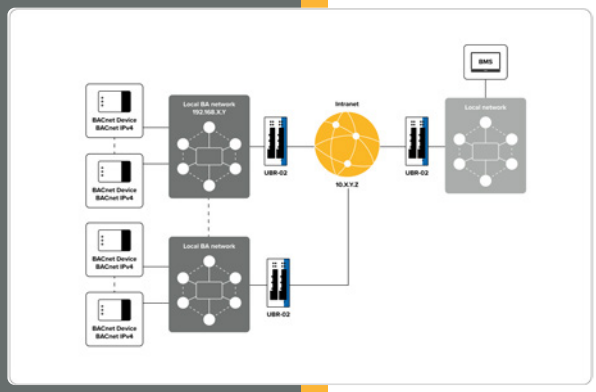
Das Szenario auf der linken Seite stellt ein ähnliches lokales Netz an einem Unternehmensstandort dar. Es umfasst aber außer BACnet/IPv4-fähigen Devices für die Gebäudeautomation keine weiteren Endgeräte. Für die Datenübertragung zwischen lokalem Netzwerk und Internet wird ebenfalls ein IP-fähiger DSL-Router eingesetzt, der nicht Port-Forwarding-fähig sein muss, da hier weder feste noch dynamisch vergebene IP-Adressen benötigt werden.

Im Unterschied zu dem Szenario auf der rechten Seite wird hier mit einem UBR-01 (mit nur einer Netzwerkkarte) das vorhandene BACnet in BACnet/SC übersetzt und somit verschlüsselt. Außerdem kommuniziert der UBR-01 – mit der gleichen Netzwerkkarte – über den DSL-Router verschlüsselt mit der GLT.

Fazit

Diese einfachere Variante kann ist sinnvoll sein, wenn das lokale Netzwerk keine anderen Geräte enthält und der Internetanschluss ausschließlich für die Gebäudeautomation verwendet wird.

BACnet/SC in einem Campus-Netzwerk (Variante 1)



Die Ausgangssituation

Eine Zentrale auf einem Campus-Netzwerk mit sehr vielen Teilnehmern, die via Intranet vernetzt sind. Derzeit wird der Datenaustausch in der Gebäudeautomation über BACnet/IPv4 abgewickelt. Anwendungsbeispiel kann etwa ein Klinikums- oder ein Universitätsgelände sein.

In der Zentrale befindet sich die Gebäudeleittechnik (GLT), die auf die gebäudetechnischen Anlagen in einzelnen Häusern und Gebäudegruppen via Intranet zugreift. Das lokale Netzwerk umfasst nicht nur ein eigenes Netzwerk mit BACnet/IPv4-fähigen Devices für die Gebäudeautomation, sondern auch andere Endgeräte, wie etwa PCs in der Verwaltung.

Die Herausforderung

Diese Anlagen sind quasi Inseln aus lokalen Netzwerken, die ihre Daten mit BACnet/IPv4 austauschen. Die Datenpakete werden unverschlüsselt verschickt und können von allen Teilnehmern im Netzwerk eingesehen – und gegebenenfalls auch verändert – werden.

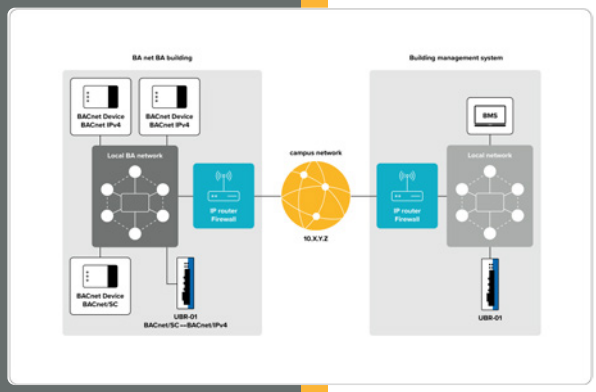
Was tun?

Um die gebäudetechnischen Anlagen physikalisch abzusichern, kann ein UBR-02 eingesetzt werden. Seine beiden Netzwerkkarten ermöglichen die Trennung zwischen Campus- und GA-Netzwerk: Eine Netzwerkkarte wird eingesetzt, um zwischen beiden Netzwerken ausschließlich BACnet-Daten zu routen. Mit der zweiten Netzwerkkarte wird die Campus-Kommunikation mit BACnet/SC abgewickelt. Durch die Verschlüsselung ist der Datenverkehr für die Teilnehmer außerhalb der Gebäudeautomation nicht mehr sichtbar.

Fazit

In einem lokalen Campus-Netzwerk kann der UBR-02 größtmögliche Sicherheit herstellen.

BACnet/SC in einem Campus-Netzwerk (Variante 2)



Die Ausgangssituation

Eine Zentrale auf einem Campus-Netzwerk mit sehr vielen Teilnehmern, die via Intranet vernetzt sind. Derzeit wird der Datenaustausch in der Gebäudeautomation über BACnet/IPv4 abgewickelt. Anwendungsbeispiel kann etwa ein Klinikums- oder ein Universitätsgelände sein.

In der Zentrale befindet sich die Gebäudeleittechnik (GLT), die auf die gebäudetechnischen Anlagen in einzelnen Häusern und Gebäudegruppen via Intranet zugreift. Auf der rechten Seite ist ein lokales IP-Subnetz für den allgemeinen Datenverkehr dargestellt, auf der linken Seite das lokale GA-Netz. Beide Subnetze sind via IP-Router an das Netzwerk angebunden.

Die Herausforderung

Die gebäudetechnischen Anlagen sind quasi Inseln aus lokalen Netzwerken, die ihre Daten mit BACnet/IPv4 austauschen. Der initiale Verbindungsaufbau in BACnet wird mit Unterstützung von sogenannten BACnet Broadcast Management Devices (BBMD) ausgeführt, was eine aufwändige Konfiguration erfordert. Die Datenpakete werden nicht nur unverschlüsselt verschickt, sondern können auch von allen Teilnehmern des anderen Subnetzes eingesehen – und gegebenenfalls auch verändert – werden.

Was tun?

Um die gebäudetechnischen Anlagen physikalisch abzusichern, kann in beiden Subnetzen jeweils ein UBR-01 eingesetzt werden. Seine Netzwerkkarte wird jeweils verwendet, um in jedem Subnetz ausschließlich BACnet/SC-Daten zu routen. Auf diese Weise wird der Datenverkehr im Intranet verschlüsselt. Überdies kommunizieren die einzelnen Geräte nicht mehr eigenständig über das Intranet, sondern stets über den UBR-01.

Fazit

In einem lokalen Campus-Netzwerk mit Subnetzen kann der UBR-01 nicht nur größtmögliche Sicherheit herstellen, sondern auch die Konfiguration der Endgeräte erheblich vereinfachen.

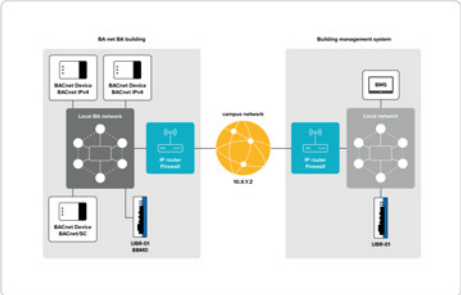
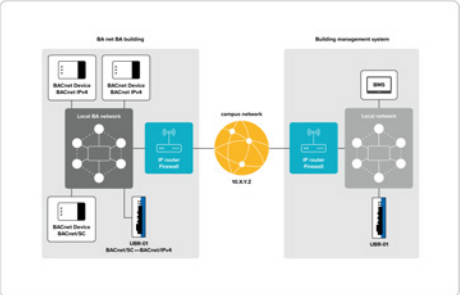
Unser Tipp: Die MBS GmbH kann Unternehmen bei der Transition von BACnet/IPv4 auf BACnet/SC unterstützen:

- angefangen bei der Bestandaufnahme einer Liegenschaft und
- der Netzwerkanalyse über
- die Erarbeitung von Vorschlägen für Lösung und Umsetzung
- bis zur Lieferung und
- dem Einbau von BACnet/SC-fähigen Geräten
- als Komplettleistung oder als Einzelleistung (wie beispielsweise auch Schulungen).

Fragen Sie uns – wir helfen Ihnen gern.

Vorher - Nachher Darstellung

BACnet/IPv4 - BBMD — BACnet/SC

BACnet im Campus-Netzwerk	BACnet/IPv4 - BBMD	BACnet/SC
		
Firewalloptionen	Die Firewalls müssen UDP (User Datagram Protocol) von jedem BACnet-Gerät im Netzwerk zu jedem anderen BACnet-Gerät erlauben.	Firewalls können BACnet-Verkehr mit TCP (Transmission Control Protocol) auf die BACnet/SC-Router in den einzelnen Subnetzen einschränken.
IP-Konfiguration der einzelnen BACnet-Devices	Jedes BACnet-Device muss z.B. durch eine Default Route auf den lokalen IP-Router/Firewall so konfiguriert sein, dass es alle anderen BACnet-Geräte erreichen kann.	Die BACnet-Devices müssen nur direkt mit den anderen Geräten inklusive des SC-Routs im lokalen GA-Netz kommunizieren. Eigenes IP-Routing über das ganze Campus-Netzwerk ist nicht erforderlich.
Security im Campus- Netzwerk	Der BACnet-Verkehr im Campus-Netzwerk erfolgt unverschlüsselt und ungesichert über BACnet/IPv4.	Der BACnet-Verkehr im Campus-Netzwerk erfolgt verschlüsselt und gesichert über BACnet/SC.
BBMD-Konfiguration	erforderlich	nicht erforderlich

MBS GmbH | Römerstraße 15 | 47809 Krefeld | Tel. +49 21 51 72 94-0 | info@mbs-solutions.de

Impressum: **Geschäftsführer:** Gerhard Memmen-Krüger, Nils-Gunnar Fritz
Handelsregister: Krefeld HRB 33 7, USt.-IdNr.: DE 120 148 529, Registergericht: Krefeld
Inhaltlich Verantwortlicher gemäß § 6 MDStV: Gerhard Memmen-Krüger, Nils-Gunnar Fritz