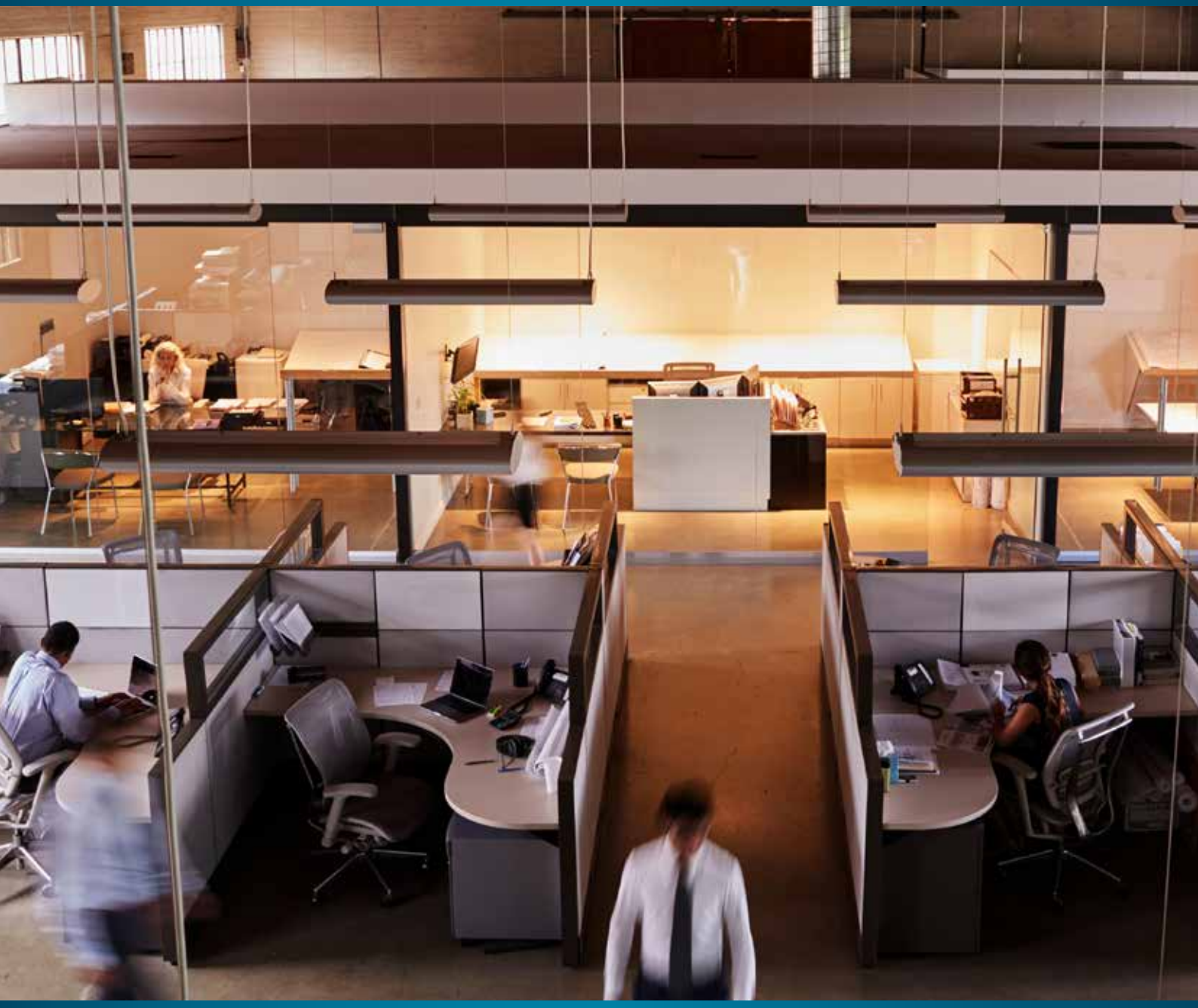
ISSN 2190-944X

BACnet Middle East Journal

Issue 13
November 2024



Precise control, tight closing.

Butterfly valves from Belimo

Our butterfly valves have been specifically developed for heating, ventilation, and air-conditioning applications, meeting all the requirements. They offer a wide range of options for various applications, including 2-way control and open/close applications, as well as 3-way combinations for control and changeover applications. Furthermore, our intelligent JR and PR actuators with parametrisable linear characteristics enable the reliable use as 3-way control valves in mixing and distribution applications.

Additionally, the Belimo Assistant 2 app enables quick and easy commissioning for a wide range of application possiblities and, of course, for BACnet MS/TP.

Find out more
belimo.com

BELIMO Automation AG
info@belimo.ch, www.belimo.eu

BELIMO

Cybersecurity and Regulation: Challenges and Solutions

In an era where interconnected systems define the modern world, cybersecurity has become a paramount concern, especially within the building automation industry. As BACnet continues to expand its influence globally, including the Middle East, safeguarding systems from potential cyber threats must take center stage. While the BACnet standard provides a robust foundation for smart building networks, the ever-evolving threat landscape requires continuous attention and adaptation. Regulatory frameworks are increasingly aligning with this urgency, yet there remain significant challenges.

Challenges of Cybersecurity in Building Automation

One of the most prominent challenges we face is the unique vulnerability of building automation systems (BAS) compared to traditional IT infrastructures. BAS environments were traditionally isolated systems, with little exposure to external threats. However, the integration of these systems into corporate networks, the Internet of Things (IoT), and cloud platforms has made them highly susceptible to cyberattacks. Cybercriminals now see building systems as potential entry points to broader IT environments, creating severe risks for data security and operational continuity.

The complexity of modern building systems adds another layer of difficulty. With thousands of interconnected devices, sensors, and controllers, securing these systems from unauthorized access, manipulation, or sabotage becomes a considerable challenge. Each additional device increases the potential attack surface, making it critical to have an overarching cybersecurity strategy that is not only comprehensive but adaptable to new threats.

The Role of Regulation

Governments and regulatory bodies are increasingly aware of these risks. In the European Union, for example, new regulations like the Network and Information Security (NIS) Directive have been introduced to enforce higher standards of cybersecurity across critical sectors, including energy, transport, and healthcare. Similar regulations are emerging in the Middle East, aiming to establish robust security protocols for infrastructure projects.

However, compliance with regulatory requirements presents its own set of challenges for BACnet users and implementers. The regulatory landscape can be difficult to navigate, particularly when standards vary across regions. Moreover, staying compliant with evolving regulations requires constant updates to systems and protocols, which can strain resources for smaller businesses.

Solutions and the Path Forward

To meet these challenges, a multi-layered approach is essential. First, building automation systems must integrate security from the ground up. The BACnet Secure Connect (BACnet/SC) standard is a key development in this regard, offering encrypted communication to ensure data integrity and protect against unauthorized access. Implementing such standards across all BACnet-compliant devices is critical to creating a secure environment.

Second, collaboration is essential. Stakeholders from different sectors, including government, industry, and technology providers, must work together to develop and implement effective cybersecurity frameworks. Initiatives like BIG-EU foster collaboration across borders, allowing us to share best practices and develop unified security standards for the industry.

Lastly, education and awareness are crucial. Building owners, operators, and IT staff must be well-informed of the latest cybersecurity threats and solutions. Continuous training and updated knowledge of regulatory changes ensure that all stakeholders are prepared to address evolving cyber risks.

Conclusion

As building automation systems continue to evolve and integrate with broader IT infrastructures, the importance of cybersecurity cannot be overstated. While challenges remain, solutions such as BACnet/SC and a collaborative approach to regulation offer a clear path forward. By staying vigilant and proactive, we can ensure that our smart buildings are not only efficient but secure.

Hans Symanczik

Hans Symanczik is a founding member of BIG-EU and has been actively involved in promoting and developing BACnet standards across Europe and beyond.

Hans Symanczik
Founding member of BIG-EU

Editorial

Solutions

Products

BACnet Insight

Technology

BACnet Interest Groups News

Cover picture:
Office building – lighting control example.
© HMS Networks

Issue 13 | November 2024

This issue can be downloaded from www.BACnetjournal.org

VISIT US AT BIG 5 DUBAI!

SMARTER BUILDINGS MADE SIMPLE.

WebCTRL®

At **Automated Logic**, we are the people behind intelligent buildings. We translate ideas and vision into real plans, real systems and, ultimately, some of the most intelligent buildings on Earth. We are designers, consultants, engineers, and builders...and we ensure that the innovation that starts with listening to our customers...is expertly implemented in every building we touch. Let us put our **WebCTRL® building automation system** to work for you.

Automated Logic

Middle East Sales Office
P.O. Box 61368
Dubai, UAE
+971 (0) 56 99 56 100
Jim.Kilcoyne@carrier.com

Energy-Efficient School with Wireless BACnet Technology

Wireless BACnet technology reduced the installation time with 65%. © LumenRadio

Creating a more sustainable school building without construction work and with no disruption to the pupils was made possible thanks to wireless BACnet technology. And together with the 65% reduction in installation time – compared to a wired solution – all added up to the project being a great success.

Manilla School in Stockholm, Sweden is a modern school with advanced technology for both digital and visual learning. The property owner, SISAB, is also at the forefront of new technology but its focus is on running more energy efficient buildings. By modernizing the room controllers throughout Manilla School, SISAB found that it could decrease energy usage, save money and support its sustainability strategy.

The system integrator Kieback & Peter helped SISAB to change from an "unintelligent" room control setup to smart room controllers connected to a SCADA (supervisory control and data acquisition) system, making it possible to regulate the indoor climate and monitor energy usage.

The challenge was that the retrofit needed to be done when the school was still being used, without disrupting lessons. By choosing LumenRadio's wireless BACnet product there was no need to install any new cables and therefore no construction work, which also meant no time-consuming installation planning or daisy-chaining.

126 nodes were wirelessly connected in five separate networks. Thanks to LumenRadio's patented wireless BACnet technology, the communication network has a uniquely high level of reliability and ensures that there is no interference with the other wireless systems at the school.

Petri Kauppinen from Kieback & Peter was impressed by the speed and simplicity of the installation process. "We were very pleased with the quick installation and commissioning," Petri says. "No extra software was needed for the commissioning and due to the quick and easy installation we didn't have to disrupt the daily running of the school."

W-BACnet eliminates time-consuming installation planning, cabling, daisy-chaining and trouble-shooting. © LumenRadio

W-BACnet – BACnet MS/TP through reliable wireless mesh. © LumenRadio

LumenRadio's W-BACnet products make it possible to create a wireless BACnet mesh network that maintains the standard and interoperability of the protocol. The W-BACnet products are compatible with any other product utilizing the BACnet MS/TP standard. ■

Carl von Rosen
Product development manager Building & Industrial Control Systems
LumenRadio
carl.vonrosen@lumenradio.com | www.lumenradio.com

Automation of Street Lighting with BACnet/IP

USEDAROC electrical panel installation. © Distech Controls

ECLYPSE APEX controller. © Distech Controls

Distech Controls is breaking into new markets through its innovative collaboration with USEDA (Union des secteurs de l'énergie du département de l'Aisne) and system integrator Dumortier. USEDA enables mayors to remotely manage their town's public lighting and a major new project involves the installation of 3,800 ECLYPSE controllers in 550 towns.

USEDA is combining its long-standing expertise with new technologies to make everyday life easier for municipalities, by providing them with simple, cost-effective management tools in a complex energy context. The result is USEDAROC, a web-based platform for remote management of public lighting.

The use of street lighting varies according to time and need. Furthermore, it's sometimes necessary for them to be on all night, especially during events. "Taking advantage of this service with today's connected solutions facilitates programmed management from a computer, tablet or my smartphone. I can program my town's street lighting on specific dates, but also at any time and from anywhere in case of exceptional needs," assures Jean-Paul Coffinet – Mayor of Beaurieux (Aisne).

BACnet/IP ECLYPSE™ controller: a well-considered choice

In consultation with integrator Dumortier, USEDA chose the Distech Controls solution to meet its specifications. This choice was motivated by Distech Controls' multi-protocol hardware (BACnet, Modbus, API...), which allows great flexibility. Developed to be future-proof and scalable, the Distech Controls solution is renowned for its openness. As part of the USEDAROC project, ECLYPSE controllers communicate directly with the energy meter, saving time and ensuring reliability.

In addition to control, the USEDAROC platform offers visibility over energy consumption, notably through an energy savings simulator, an EcoWatt alert and an interactive map. In terms of security, users can declare an incident directly from the USEDAROC application, and set up emergency functionalities.

The main module developed for this project supports the remote management of public lighting.

ECLYPSE APEX in the electrical panel. © Distech Controls

Other modules linked to energy consumption are currently being deployed, such as heating, water level monitoring, dumpster monitoring, remote surveillance and billing tracking.

The integrator is equally satisfied: "As a very small company, we're delighted with Distech Controls' support for this project, including its technical side, sales support and logistics. There were no supply delays. This was a large-scale project for a company with 10 employees, which had to be deployed across a fleet of 3,500 controllers," says David Duhant, Dumortier's managing director. ■

Sarah-Jane Demolliere
Marketing Solutions Manager | Distech Controls
marketing-europe@distech-controls.com | www.distech-controls.com

Mitigating the Urban Heat Island Effect with BACnet

The urban heat island effect on big cities. © Shutterstock

As urbanization increases, cities become more susceptible to the urban heat island (UHI) effect, where temperatures in urban areas are significantly higher than in outlying areas. This effect, which is more pronounced in extreme climate regions, contributes to environmental, energy, economic, and human health impacts. One of the factors causing heat islands is the heat generated from human activities, such as the spread deployment of air-conditioning systems. Maximizing HVAC systems efficiency is mandatory to address the problem, and it is through BACnet that the UHI effect can be reduced while keeping high levels of comfort for the building occupants.

The urban conformation itself is the cause of the so-called urban heat island (UHI) effect; on the one hand, cities usually lack the necessary green spaces where trees, vegetation, and water bodies tend to cool the air by the shade of trees, the transpiration of water from the plant leaves and the evaporation of water. On the other hand, the materials used for urban environments, such as pavement or roofing, favor the absorption and re-emission of the sun's heat. Also, urban geometry, with tall buildings and narrow streets, makes cities become canyons where the wind flow is blocked, so another of the available natural cooling systems is lost. Add to that formula the heat generated by human activities and the climate conditions of some regions, with calm, clear, dry, and hot weather, and you'll get all the needed ingredients for having a heat island.

One problem with multiple impacts

The heat islands' impact spreads over several areas, affecting citizens' lives deeper than it may seem. The demand for air conditioning to cool buildings and facilities creates peaks in the energy demand, making the supply energy companies rely on fossil fuel plants to cover that need, so air pollution and greenhouse gas emissions increase. Indeed, not only the quality of air is impaired, but of water too: the high temperatures of the city structures can heat the stormwater, which through the sewers is released into rivers, ponds, and lakes, affecting the temperature of these natural environments and affecting, in turn, its aquatic life.

The consequences of the UHI effect on human health are also evident, particularly for populations who are more sensitive to extreme climate, such as older adults, young children, people in poor health, and people who work outdoors. In the case of young children, the fact that their respiratory systems are still developing and due to their high ratio of breathing, the chances of suffering a lung disease dramatically rise in comparison to children who live in country areas. Because of these consequences, counteracting the UHI effect becomes urgent.

Looking at the factors involved in the UHI effect listed above, we notice that some are very hard or impossible to address, like the climate factor or how cities have been designed until now. All efforts must focus on other factors, such as improving HVAC systems.

Maximizing the efficiency of HVAC systems with BACnet

This improvement necessarily goes through integrating HVAC systems into building management systems (BMS) running under an open communication protocol such as BACnet. By integrating and centralizing the control of the HVAC system into the BMS with BACnet, building managers can monitor how the system uses energy and make the consequent appropriate data-driven decisions.

One example of maximizing the efficiency of HVAC systems in large buildings is the grouping of control areas; since different areas have varying occupancy levels, their cooling requirements also vary. By controlling specific zones independently, energy is not wasted in cooling areas that do not require it. BACnet control systems can automatically adjust the cooling levels in response to occupancy sensors, ensuring that only the necessary zones are cooled.

Also, external humidity and temperature sensors can be connected to the building system and predict the effect of external conditions on the building's comfort without pushing the HVAC system into alarm operation mode. All this reduces the overall strain on the HVAC system, expanding the lifespan of equipment and reducing the maintenance costs to significant levels.

The benefit of efficiently controlling the cooling needs is not limited to improving energy usage. Still, it also ensures better comfort for the building occupants, boosting productivity in offices, encouraging people to spend more time (and money) in commercial spaces, and reducing tenant turnover in residential buildings. And let's not forget that it also increases the monetary value and reputation of the building.

Intesis 700Series Air, the gateway for multi-brand HVAC integration into BACnet. © HMS Networks

700 Series Air gateways: the last bet for HVAC integration by Intesis

One of the challenges for HVAC system integrators is adapting to the diversity of sizes and technologies involved in an integration project. Even when dealing only with BACnet on the BMS side, on the other side, they may find a good amount of different HVAC brands. With these adaptation needs in mind, Intesis, the HMS brand for building automation gateways, launched its new generation of gateways for HVAC systems integration: The 700 Series Air. The pillars of its adaptability are the possibility to configure the same piece of hardware to support several of the major HVAC brands (12 for now and counting) and the availability of different licenses with different capacities, covering any zone's range of size (from four to up to 128 indoor units under control per gateway). Besides, the 700 Series Air gateways are provided with a connection for energy metering devices and with the Intesis Power Estimation Algorithm, which allows building managers to estimate the energy usage of the HVAC system.

Jaume Carballo
Technical Writer | HMS Networks (Intesis Business Unit)
jaca@hms-networks.com | www.hms-networks.com

Micampus: Industrial Area Transformed into a Student Residence District

Micampus MT14: Principal facade of the building. © LG Electronics

Technical rooms and control cabinets play a critical role in the centralized production. © LG Electronics

The well-known industrial area of Madrid, Fuencarral-El Pardo district, has long served as a base for numerous factories and office buildings. Currently, this district is undergoing a significant transformation spearheaded by Windwood Micampus.

The project aims to create a student residence district offering general living services, with each building featuring unique facilities accessible to all Micampus tenants. For instance, some buildings will have amenities such as swimming pools, cinema rooms, workout areas, and specialized catering services. This concept is designed to gather students' needs, transforming the area into a vibrant student residence district.

Living Facilities

Micampus now boasts over 10 buildings in Madrid, each offering a variety of room types tailored to meet students' needs. Each room is equipped with a kitchen, bathroom, bed, and workspace. General facilities include parking lots for cars and bikes, storage rooms, meeting rooms, workrooms, and on-site canteens and restaurants.

VRF Centralized Production System: Comfort and Wellbeing

Rooms are equipped with Domestic Hot Water (DHW) and air conditioning, allowing users to locally control the temperature and fan speed for personalized comfort. All HVAC and DHW installations are centralized and managed by VRF (Variable Refrigerant Flow) systems. Common areas also feature air handling units with VRF-based solutions.

Smart Metering

The VRF systems include a cost distribution feature enabled by a smart energy metering system and a power distribution interface (LG PDI). This system allocates electricity costs, allowing tenants to control expenses for each room and individual air conditioning unit.

BACnet on EBMS Supervisory

The Energy Building Management System (EBMS) facilitates the control and monitoring of each building. Additionally, all buildings are connected to a central EBMS, which oversees maintenance and cost control across the entire property.

Conclusion

The transformation of industrial areas into a student district offers unique common services in each building, providing comfort and wellbeing for residents. Tenants can control their living spaces, and the integrated EBMS using the BACnet protocol, ensures comprehensive property control and monitoring across a private wide-area network (WAN). ■

Multi V 5 Outdoor Units. © LG Electronics

José María Redondo
BMS, Central Controller & Gateways Product Manager
LG Electronics European Business | Member of BACnet Interest Group Europe Spanish Representative of BACnet Interest Group Europe
josemaria.redondo@lge.com | www.lge.com

Game-changing Control Butterfly Valves

The smart control of heating, cooling, and ventilation loads has a big impact on the energy efficiency of buildings. A key aspect here is the heating and chilled water circuit, i.e. the hydronics of a building.

With the introduction of the new control butterfly valves, Belimo's successful product range with the PR actuator has now been further enhanced to include the new family member, the JR. This addition makes it possible to cover a wide range of advanced applications, from DN 100 to DN 300. They are perfectly suited for heating, chiller, and cooling tower applications, and changeover systems, not to mention control applications for large ventilation systems and bypass applications.

The smart JR and PR actuators allow smooth and efficient operation and ensure that the control butterfly valves operate with high precision. Two additional sensors (passive, active or switching contacts) can also be connected. In this way, the analog sensor signals can be easily digitized and communicated via BACS. This extra information enables the creation of optimized systems. Seamless BACS integration is achieved via BACnet MS/TP, Modbus RTU or MP-Bus.

www.belimo.com/ch/en_GB/products/valves/product-documentation/butterfly-valves

Control butterfly valves
New JR actuator (left) and existing PR actuator (right)

The Belimo Assistant 2 app enables not only quick and easy commissioning thanks to its intuitive commissioning workflow, but also flexible parametrization for a wide range of application possibilities.

BELIMO

BELIMO Automation AG
info@belimo.ch | www.belimo.ch

30 Years of BACnet: From Interoperability to Security – and Beyond

It's the 30-year anniversary of the BACnet protocol. By its very nature, an anniversary is a time for looking back, reflecting on how far things have come and, more importantly, looking toward the future and what's next.

As BACnet Vendor ID 37 among today's 1,492 vendors, MSA's FieldServer™ suite of automation gateway products have been around much of these 30 years. So, we thought it a good idea to look at where BACnet gateways have been, as well as where they're going.

After all, BACnet has been a key component in supporting the protocol gateway mission: to help improve the performance, productivity, efficiency, and safety in building automation, including HVAC, as well industrial and military applications, while also helping reduce the demand on resources and energy consumption.

A Look Back at BACnet Protocols

Collaboration and cooperation are an inherent part of any vendor's working relationship with BACnet. The early years provide example after example of how BACnet has partnered with gateway developers to enable seamless integration of building and industrial automation systems.

Even in its infancy, BACnet quickly emerged as the leading automation protocol. But BACnet has never taken a "one-and-done" approach, so here's a look at some of the older BACnet's protocols that have been included in gateway protocols since the 1990s.

BACnet ARCNET

As one of BACnet's original protocols, ARCNET was a local area network (LAN) technology that enabled devices to communicate over shared coaxial cable. The ARCNET protocol was among the first to do what BACnet does best: enable interoperability within building automation and industrial control applications.

BACnet PTP Point-to-Point

PTP was typically used over serial communication lines, such as RS-232, that offered a direct connection between computers and modems. While less common, it was useful in applications in which network-based communications were unavailable.

BACnet Ethernet

Uses Ethernet without the IP layer. Directly tied to the Ethernet layer, limiting its use in wider networks that require routing across IP.

BACnet MS/TP (Master-Slave/Token Passing)

This protocol operates over twisted-pair wiring used as a token-passing mechanism for communication. MS/TP was most used for connecting controllers to sensors and actuators.

BACnet/IP

Designed to allow BACnet devices to communicate over standard Ethernet networks, this protocol, which uses Ethernet and Internet Protocol (IP), is the most common variant used in modern building automation systems.

The Evolution of BACnet for IoT Gateways

The committee that interprets and supports BACnet has done a remarkable job making BACnet easily extendable, so its evolution has not only been inevitable, it's also been invaluable for IIoT gateway developers.

According to Bennie de Wet, former CTO/Managing Director of Sierra Monitor (now MSA Safety), the company's first gateway was based on an Intel 486 processor, featured 8 RS232 serial ports, and 2 RS485 ports, and used a standard ISA expansion slot for the ARCNET card.

"Initially, the BACnet driver supported only basic Read and Write Property services for BACnet Ethernet and BACnet MS/TP," says de Wet. "Implementing BACnet Ethernet was relatively straightforward. BACnet MS/TP, however, presented some challenges, primarily because of strict timing requirements. This tested both the limits of processor memory and processing power. I vividly remember many a late night spent coding the MS/TP state machine from the BACnet specification's state diagrams. Later, we implemented BACnet/IP and the associated BBMD functionality, which, together with the MSTP DLL, remains the most popular variants of our stack."

Since then, the standard has evolved and so, too, have the testing requirements. The establishment of BACnet Testing Labs (BTL) opened the opportunity to test for a broader range of exceptions and compliance scenarios. The maturity of both BACnet and gateways has led to new product launches to support HVAC and other building automation systems.

"There's an immense amount of pride in the BACnet evolution," explains de Wit, "This progression forced further enhancements to our BACnet stack, including implementing additional test cases to meet these standards. The improvements we gained marked a significant milestone in developing our BACnet stack. It makes me super proud to see some of our BACnet products still operating in the field after 10 and 20 years of commissioning. We undertook a major overhaul of our stack during the certification process, adapting it to run on a range of platforms, from the PIC microcontroller to the latest ARM9 processors running Node.js. Each platform transition required a complete rewrite of core parts of our BACnet protocol, reflecting our commitment—and BACnet's—to continuous improvement. Our journey with BACnet reflects our deep-rooted involvement and ongoing dedication to the BACnet community."

Tomorrow's BACnet Protocols

Though FieldServer devices once offered then-current BACnet ARCNET and BACnet PTP, today it still supports BACnet Ethernet.

The key to such longevity, of course, is having the ability to support whatever topologies the market supports. So, both BACnet and BACnet vendors like MSA must continue to adapt and evolve specifications for the "next big thing."

Right now, the next big thing is BACnet Security Connect or BACnet/SC.

BACnet/SC is an addendum to the BACnet protocol, and what makes it unique in the marketplace is its ability to offer a secure, encrypted communication datalink layer. BACnet/SC allows for more secure building automation products and systems in an era marked by cybersecurity threats and attacks.

The addition of BACnet/SC to the protocol is a highly proactive response to security issues and is designed to better protect the integrity of the network by ensuring that every device is authenticated and authorized.

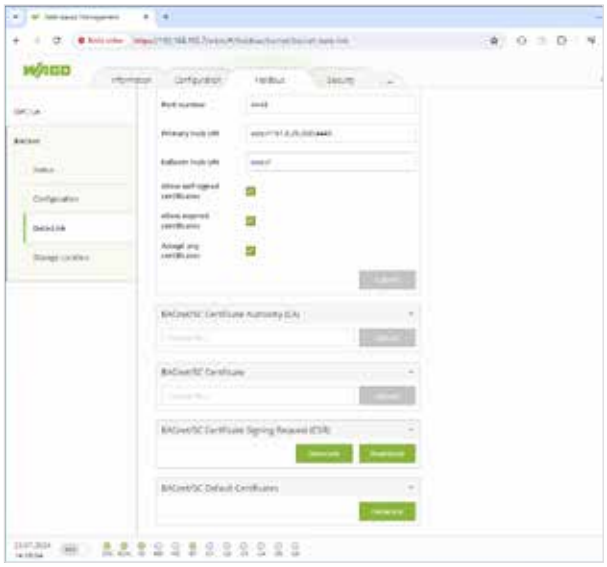
Like BACnet, gateway developers take security very seriously, which is one of the reasons that best-in-class gateways undergo rigorous penetration testing and become BTL Listed. And now, in keeping with technological advancements and BACnet's own innovations, future gateways may feature BACnet/SC, providing secure, encrypted communication channels and enhanced features to better support the integration of emerging IIoT devices and connected systems.

ABOUT THE AUTHOR

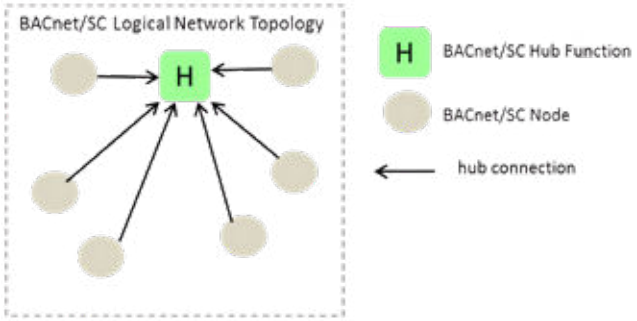
Richard Theron is the Product Manager for FieldServer™ products at MSA Safety, the global leader in the development, manufacture, and supply of safety products that protect people and facility infrastructure. Theron works closely with the HVACR industry in support of MSA HVACR Point Gas Sensors, Aspirated Leak Detectors, and Demand Control Kitchen Ventilation, as well as Cloud-enablement of equipment.

Richard Theron
Product Line Manager | MSA Safety
richard.theron@msasafety.com | msasafety.com/fieldserver

Certificate Handling in BACnet/SC



Certificate user interface example using a WAGO controller.



BACnet/SC Topology.

The aim of this article is to explain the additional tasks involved in handling security in heterogeneous environments with devices and software from different manufacturers.

Hub and spoke

Communication in BACnet/SC is based on the hub and spoke concept, which means that a device or software acting as a hub (server) is at the center. Other BACnet/SC participants connect to it as so-called nodes (clients). In many diagrams, such connections are shown like the spokes of a wheel, with the nodes at the ends and the hub in the center. In contrast to BACnet/IP, communication is then based on permanent WebSocket Secure connections (TCP) with the hub and no longer on loose messages (UDP) between the nodes themselves. The term 'WebSocket Secure' deserves special attention here. What does this mean and how is security achieved?

WSS (WebSocket Secure) is a protocol for secure bidirectional connections and currently uses the TLS 1.3 encryption standard, which is also used for communication via https on the web. The security is achieved with certificates, i.e. digital passports, which are used for two tasks:

- unique identification of the communication partners,
- encryption of the communication so that only the endpoints involved understand it.

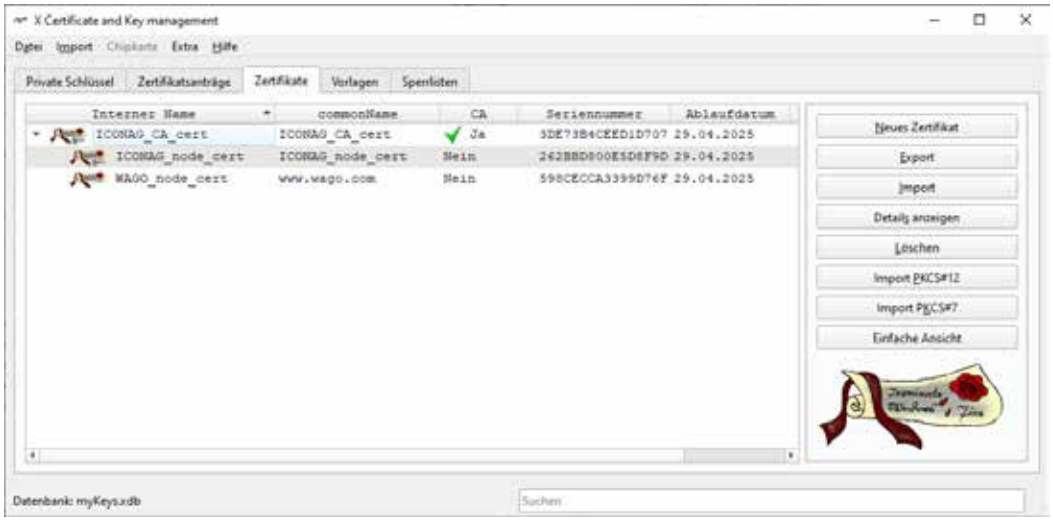
To fulfil this task, there is a trio of related files on each participant in the BACnet/SC network. The root certificate of a so-called Certification Authority (CA), the public operational certificate of the device or software and the corresponding secret private key. As the name suggests, this should never leave the device and be given to a third party.

Handworks

The generation and handling of TLS certificates is not trivial and requires additional effort when implementing BACnet/SC projects. Many larger manufacturers of control technology systems that simultaneously offer hardware and software for management tasks, for example, have recognized the challenge. Here, the software takes over the part of creating certificates and distributing them to the devices used. However, the mechanisms behind this are usually proprietary, or to put it another way: every manufacturer is doing his own thing. Simplicity is therefore sometimes bought by being tied to a single vendor.

The question arises as to how to provide BACnet/SC hubs and nodes from different manufacturers with valid certificates. Fortunately, there is a helpful and freely available open-source software tool that can help you with this task, XCA by Christian Hohnstädt [1]. It is used in many BACnet/SC projects as follows:

1. one-time creation of a self-signed root certificate that identifies the so-called Certification Authority (CA),
2. generation of signature requests on all participating endpoints (hubs and nodes), so-called Certificate Signing Requests (CSR),
3. downloading the CSR and importing it into XCA,
4. signing of the CSR with the root certificate from 1. resulting in the device certificates, called Operational Certificates in BACnet/SC,
5. export the CA certificate from 1. and the device certificates from 4. and upload them in pairs to the respective participants.



User interface of the XCA tool by Christian Hohnstädt.

Thankfully, Christian Hohnstädt himself explains many of the above steps in a video tutorial on his website. He also goes into XCA convenience features, such as the creation of templates to make it easier to issue similar certificates in series. Further instructions on using XCA specifically for BACnet/SC can be found on the web [2].

Unfortunately, issuing certificates only once is not enough. To increase security, for example, it is recommended that their validity be given a sensible expiry date, i.e. no more than one year in the future. The procedure must then be repeated before the year expires.

Conclusion

It is easy to recognize that setting up a functioning BACnet/SC environment involves a considerable amount of extra work and the certificate issues described here are only part of it. It is not without reason that 'security has its price'! However, there are signs that generally binding mechanisms for certificate management could be standardized in future BACnet protocol revisions, which would further simplify the task even in mixed environments. In any case, BACnet Secure Connect has closed a serious gap and ensured the future viability of the protocol. ■

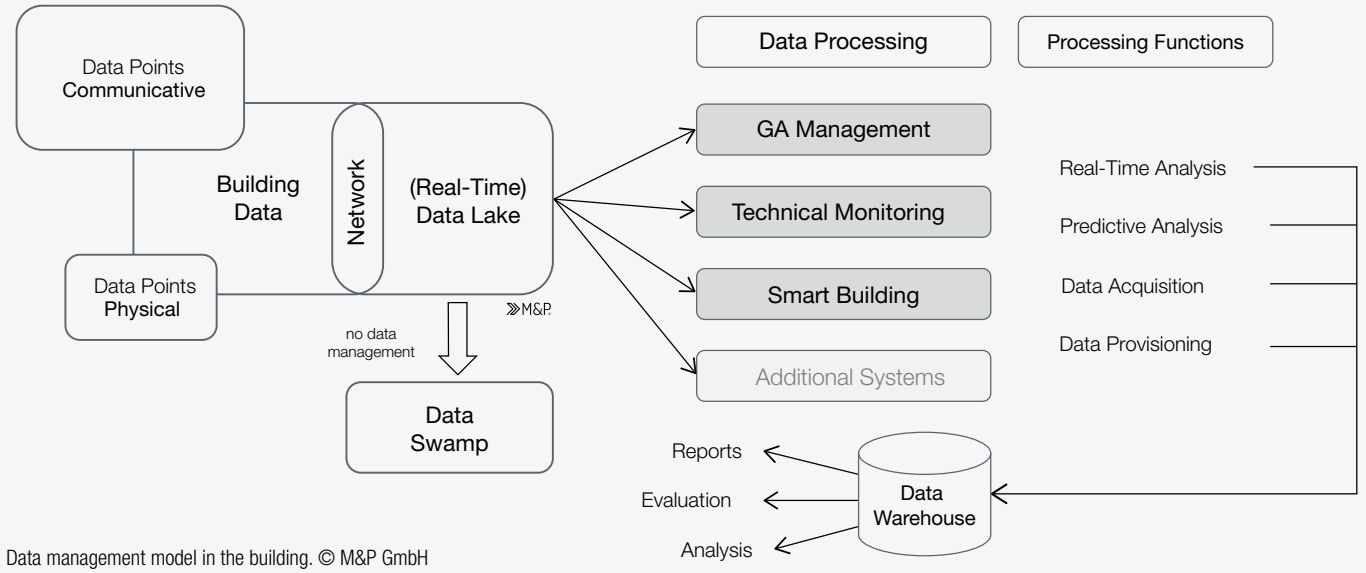
Footnotes
[1] www.hohnstaedt.de/xca/
[2] www.mbs-support.de/bacnet/sc-zertifikate-erstellen

BACtwin Symposium in Mainz

Building owners, planners and operators meet on 24.09.2024 to exchange experiences on the digitalization of technical building management using BACtwin. This standardization published in April 2024 as AMEV Recommendation No. 174 as a digital data model for BACnet-based BA systems promises, among other things, true manufacturer neutrality and machine readability of BACnet projects. The first operators of large real estate portfolios are already prescribing BACtwin, including for federal construction. The event is organized by ICONAG-Leittechnik in cooperation with the AMEV AK BACtwin and other industry partners. Information and registration at https://lp.iconag.com/bactwin2024

Hans-Jürgen Philippi
Software Developer | ICONAG-Leittechnik GmbH
hans.philippi@iconag.com | www.iconag.com

Cybersecurity and Building Digitization – a Broad Range of New Challenges



Data management model in the building. © M&P GmbH

A fully connected building offers many advantages but can become a nightmare for every operator and user if cyber security is not considered. However, a necessary consideration of the entire life cycle can reduce the pain and must therefore begin at the requirements planning stage.

Building digitization can be described with many synonyms, whether it's smart building in functional buildings or smart home in your own four walls. The basic idea is always the same: the complete networking of building technology to generate added value in terms of safety, comfort and efficiency in building operation with the help of information and clever algorithms. The basis for this is a resilient IP-based network infrastructure that can map both current and future requirements.

Building digitalization as a "driver of networks"

The sheer volume of information that will have to be processed in various systems in the future can only be guessed about. Whether multisensors or communicative pumps and control valves, these components already provide a large amount of data that can be recorded and evaluated. Even more data can be expected from the "Internet of Things", which enables many devices with smart, networked functions.

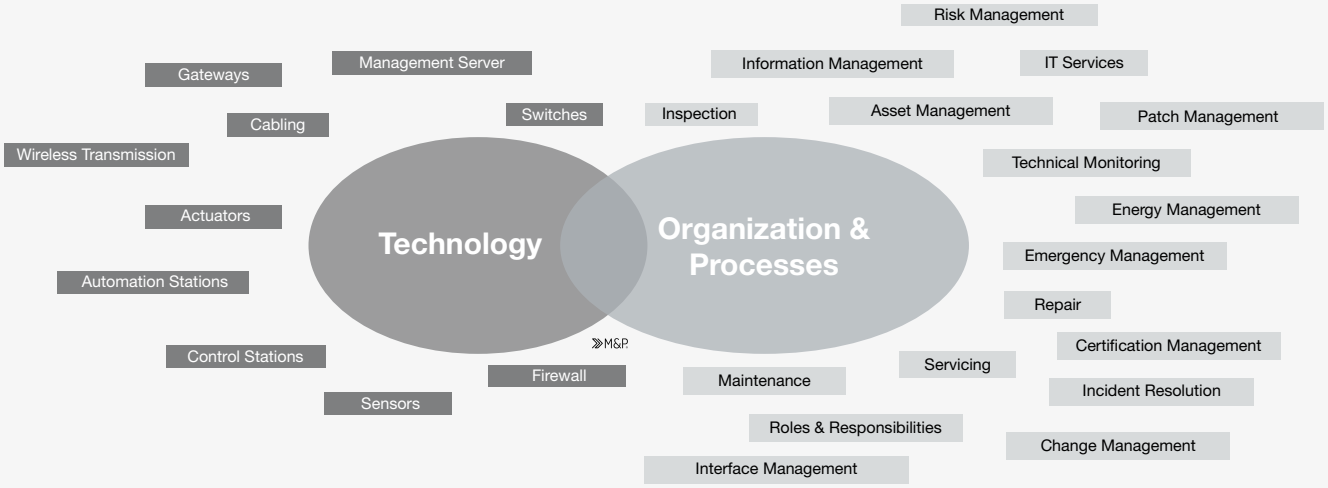
New challenges due to comprehensive interconnection

One challenge is handling the flood of information provided by the building. The fundamental question is, what information do I need to be able to carry out my operating processes comfortably, safely and efficiently? It is also important to ask who should process the recorded building data, when and how. This requires consideration of the intelligent management of building data at an early stage. Another challenge is the connection of the devices and systems themselves. The number of protocols and interfaces in the building is manifold. Starting with proprietary bus systems, through standardized building protocols to universal IoT protocols. Comprehensive knowledge and management of system-internal and external interfaces, as well as information management, are key components of successful building digitization.

As great as the opportunities offered by connectivity are, they also pose major risks. Creating connections between systems creates the potential for attacks on the building's various systems. This can result in sabotage or manipulation of the cooling technology or unauthorized access via the access control system. This requires a high level of attention to cyber security in the building by all parties involved. The core component of cyber security for the operating technology of a building (OT security for short) is the recording of goods/processes worthy of protection, assessment, and reduction of the risk through appropriate protective measures. Risk management encompasses all information recorded in the building and the associated system interfaces.

The planner: intermediary between demand and operation

The task of converting and implementing the requirements of a user into an operational building is the responsibility of the planner. A differentiated view between technology and organization and processes is essential here. Fundamentally, technology has no added value for operations without the associated structures and processes. What use is highly digitized monitoring if the company cannot interpret the information provided? Planning can only provide the technology. Organization and processes must be structured as correctly as possible first. The difficulty in the field of digitization lies in mapping all the new challenges. One component of this is

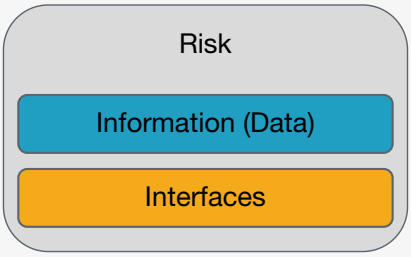


Technology that matches the organization and processes. © M&P GmbH

expanding the expertise of a BA planner in terms of network planning and describing the requirements for a secure BA network to meet the demands of tomorrow. Cybersecurity expertise is also required. Strongly driven by new EU regulations, which will greatly expand the circle of critical infrastructures from October 2024. This increases the likelihood that planners will have to deal intensively with the technical protection measures of BA networks in the future. To make matters worse, decisive factors for planning were usually not considered as part of requirements planning. The mantra of "thinking from the operational perspective" has not yet become established in some cases. Regarding cyber security, the gaps are sometimes even more serious, as a fundamental need for implementation is not seen. Statements such as "Security only costs money and doesn't bring me any added value" are unfortunately the order of the day.

BACnet as part of the solution

Encrypted communication is a core component of a networked building and should be considered in any requirements planning. BACnet/SC provides the "key" to secure information exchange in the building. Furthermore, BACnet offers a standardized approach for interface and information management in the building, as this allows the flood of protocols to be "tamed" with a uniform standard. In this context, users, planners and operators must be familiar with the capabilities and system requirements of BACnet to fully utilize its potential. However, this applies not only to BACnet, but to the entire scope of secure building digitization, which requires an adapted concept and planning approach from all parties involved in order to successfully master the new challenges together.



Management in the field of building digitization. © M&P GmbH

Nicolas Braun
Expert Security Building Automation | M&P Braunschweig GmbH
nicolas.braun@mp-gruppe.de | www.mp-gruppe.de

IT Security in BAS – What Contribution Does BACnet/SC Make?

Both economically and legally, there are high demands on IT security for building management. The legal requirements, risks, and opportunities have changed significantly. This article examines the role of BACnet/SC in this context.

From an economic and legal perspective, there are high demands on IT security in the BAS.

System disruptions can occur from both internal and external sources. Internally induced disruptions to availability, integrity, authenticity, and confidentiality affect the fundamental operational security of the infrastructure. External disruptions typically involve sabotage, espionage, or unauthorized access. The usual points of attack on automation systems are primarily at the automation and management levels of a building, less so at the field level or the higher levels in technical building management. Therefore, there is a particular need for action here.

Regulations for IT security in building automation

Fundamental regulations for IT security in building automation in Germany include the standards and the Basic Protection Compendium of the Federal Office for Information Security ("BSI"). The Basic Protection Modules Infrastructure for Building Management (INF.13) and Building Automation (INF.14) are mandatory for federal authorities and operators of critical infrastructures (information available at www.bsi.de). The VDMA 24774 standard sheet (2023-03) describes the current requirements for IT security in building automation (guideline for building automation), and EU Regulation 2016/679 provides information on the General Data Protection Regulation for the protection of personal data in building automation. Nevertheless, there is no 100% IT security even for building automation. Specific precautions to be taken in the field of building automation must be derived from a risk analysis for the respective use case. The BSI standards and Basic Protection Compendium identify the following threat situations for building automation as particularly significant:

- Inadequate planning of building automation, for example, due to lack of redundancies or high complexity in the collaboration of different trades,
- faulty integration of building services engineering systems into building automation or faulty configuration of building automation,
- use of insecure systems and protocols in building automation, such as the "old" BACnet protocol, as well as KNX or ModBus,
- manipulation of interfaces of standalone building services engineering systems to building automation (for example, via a manipulated fire alarm that opens all doors),

Deficiencies in Technical Building Management (TBM) as sources of risk:

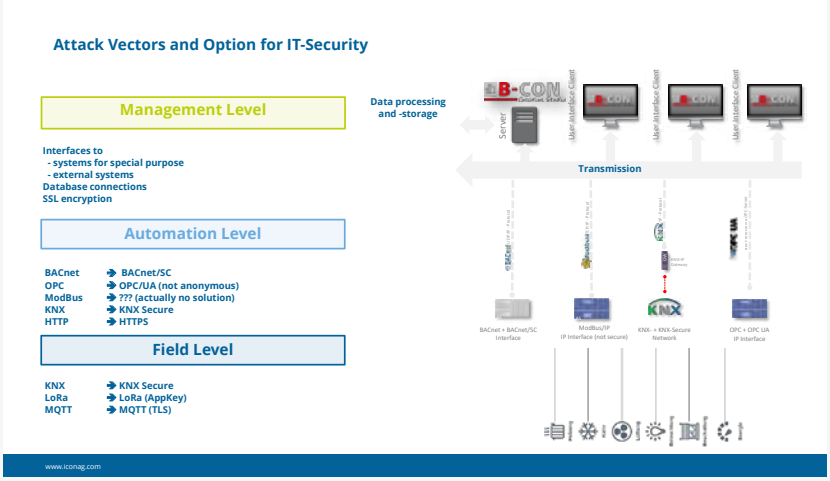
- Lack of basic IT security principles for TBM planning, since, for example, operators are often not yet determined during planning,
- insufficient documentation in TBM leads to uncertainties about the current status quo of IT security,
- deliberate or unconscious compromise of interfaces in TBM, especially when protected areas are
- connected like burglar- or fire-detection,
- inadequate monitoring of building services
- engineering, so that, for example, system-critical malfunctions are not detected,
- inadequate role and authorization management (e.g., multiple persons sharing one user account).
- Additionally, the long life cycles of building technical systems require a special level of foresighted planning of GA systems and a strategic approach. The following specifications should therefore always be considered in the planning of GA systems.

Specifications for the planning of BA systems:

- Encrypted data transmission/communication (especially BACnet/SC, KNX-Secure, etc.),
- deactivation of all unnecessary services and accesses ex-works ("hardened" devices and software) along with documentation of the used ports,
- management software with functions for recording user activities (Audit Trial),
- acceptance of the BA system only with the latest firmware (automation stations) or software version (BMS), at least all security-relevant updates, especially the current patches from Windows, as well as the current versions of the software systems used.

Specifications for the implementation and execution of BAS:

- Establishment of physically or virtually separate IP networks for building automation along with securing particularly vulnerable network segments through firewalls,
- secure access for remote maintenance,



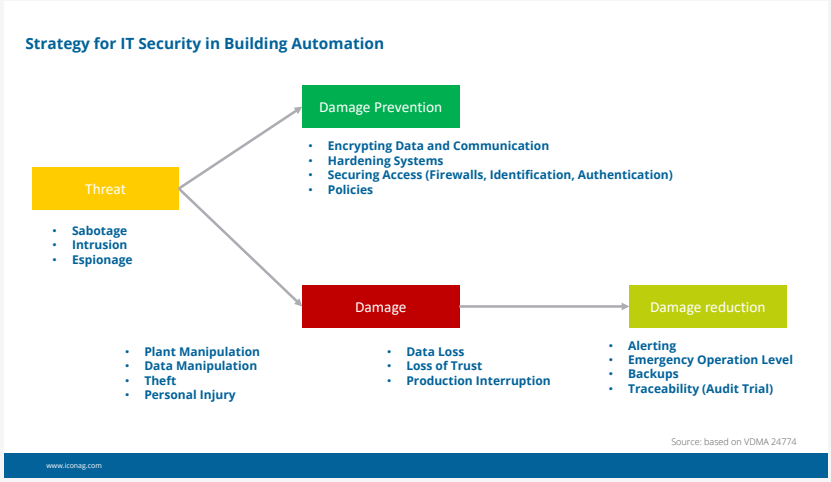
Strategy for IT security in building automation. © ICONAG

Attack points on GA systems and encryption. © ICONAG

- definition of a backup concept for automation stations and management levels along with instructions for recovery,
- physical securing of control cabinets, technical rooms, etc., including deactivation of USB or Ethernet access,
- malware protection and the latest security patches for engineering tools,
- project-specific adjustment of access authorizations and password changes (especially on automation stations, BMS), activation of auto-logoff functions,
- further hardening of the systems by deactivation or deletion of all unused services, physical accesses, user accounts, processes, and programs (especially on automation stations, BMS), activation of auto-logoff functions,
- preparation of work instructions and behavioral instructions for the permanent maintenance of IT security by the installer (SOP = Standard Operating Procedure),
- creation and handover of a BA network documentation with model designations of the components, MAC addresses, installation location, and firmware versions,
- IT security training for operators.

Specifications for the operation of BAS:

- Individual usernames and passwords,
- regular security-relevant updates/upgrades (especially for PCs, servers, and routers), ensuring that updates are downloaded exclusively from unaltered sources with certificates,
- regular backups of system programming, configuration, configuration changes of MBE software, and stored operating data,
- ensuring compliance with work instructions and behavioral instructions, including regular updating of the IT security concept as part of BA system maintenance,
- regular IT security training.



Summary

Even in building automation, there is no 100% guarantee of availability, integrity, authenticity, and confidentiality of data. However, by specifying and adhering to simple technical and organizational measures, a good level of security can be achieved. The consistent use of BACnet/SC is just one, albeit important, component for greater future security. In summary, the following 5 tips:

1. Determine the protection requirements for each building based on a risk analysis. This must be done jointly by specialist planners, clients, and operators.
2. Recognize that BA systems are particularly vulnerable in terms of IT security, with the greatest risks currently arising from the connection of building automation to the internet, e.g., due to cloud computing.
3. Based on a security concept, establish concrete IT security requirements for planning, implementation, and operation based on VDMA 24774. Also, in the context of increasing cloud computing, encrypted protocols such as BACnet/SC should be required for newly installed BA systems and for the renovation of existing BA systems.
4. Establish work instructions and behavioral instructions (policies) for damage prevention and mitigation. Agree on software maintenance and system maintenance to regularly close known security vulnerabilities.
5. In the course of regular maintenance, check not only compliance with policies but also the currency of the security concept. ■

Christian Wild
CEO | ICONAG Leittechnik GmbH Idar-Oberstein
christian.wild@iconag.com | www.iconag.com

Using Lighting to Your Advantage

Lighting control strategies in buildings are a crucial aspect in today's world, as they can make our lives better in several ways.

Directly, lighting control strategies are the primary way to create a human-centric lighting environment, that is, an environment that mimics natural light, improving our well-being and enhancing our concentration organically, something increasingly important nowadays as we spend more and more time inside buildings. On the other hand, they are also essential in achieving efficient energy use, helping to reduce energy consumption, and minimizing environmental impact on a more global scale.

Rules and Regulations

The importance of both factors has led to the creation of many energy or building codes and standards that include requirements for lighting controls in commercial and residential buildings. These codes may often specify the use of occupancy sensors, daylight harvesting, and automatic shutoff controls to optimize energy usage.

DALI and BACnet

Knowing this, using the right tools to comply with these requirements becomes a matter of utmost importance. This can be quite challenging, as these tools usually involve using different technologies that have historically evolved independently, each covering specific fields. For example, BACnet is one of the most widely used protocols in building automation, and the DALI protocol holds a similar position for lighting control.

In a DALI system, we can have sensors (for light or occupancy) and devices to enable user input, such as push buttons or sliders. These are collectively known as input devices because they provide information for automated control and

Circadian rhythm simulation in hotels. © HMS Networks

Office building – lighting control example. © HMS Networks

allow occupants to adjust the lighting settings manually. They allow occupants to select different scenes in a meeting room for presentations, meetings, or a relaxed atmosphere, the light sensors can be used to dim the lights down automatically when sunlight is bright; this happens proportionately, so the brighter the sunlight, the dimmer the lights get.

DALI also offers color control gear, which can emulate outdoor lighting conditions to connect us with the natural light mentioned above. Creating color fixtures for different applications such as hotel lobbies, restaurants, spas, and relaxing spaces is also possible. These control methods bring significant advantages on their own, but their potential is much bigger. Integrating them, as part of a DALI system, with a BACnet Building Management System (BMS) can take things to another level. The problem is that being different protocols, BACnet and DALI can't understand each other directly. How can this problem be solved?

Stronger together

This is where Intesis gateways come in, working as the link between a BACnet BMS and a DALI system, establishing bi-directional communication between both and allowing for data exchange and feedback. With both systems connected, the BACnet BMS can control the DALI system directly, and it's also possible to have it interact with other systems within the building in real-time. For example, you can:

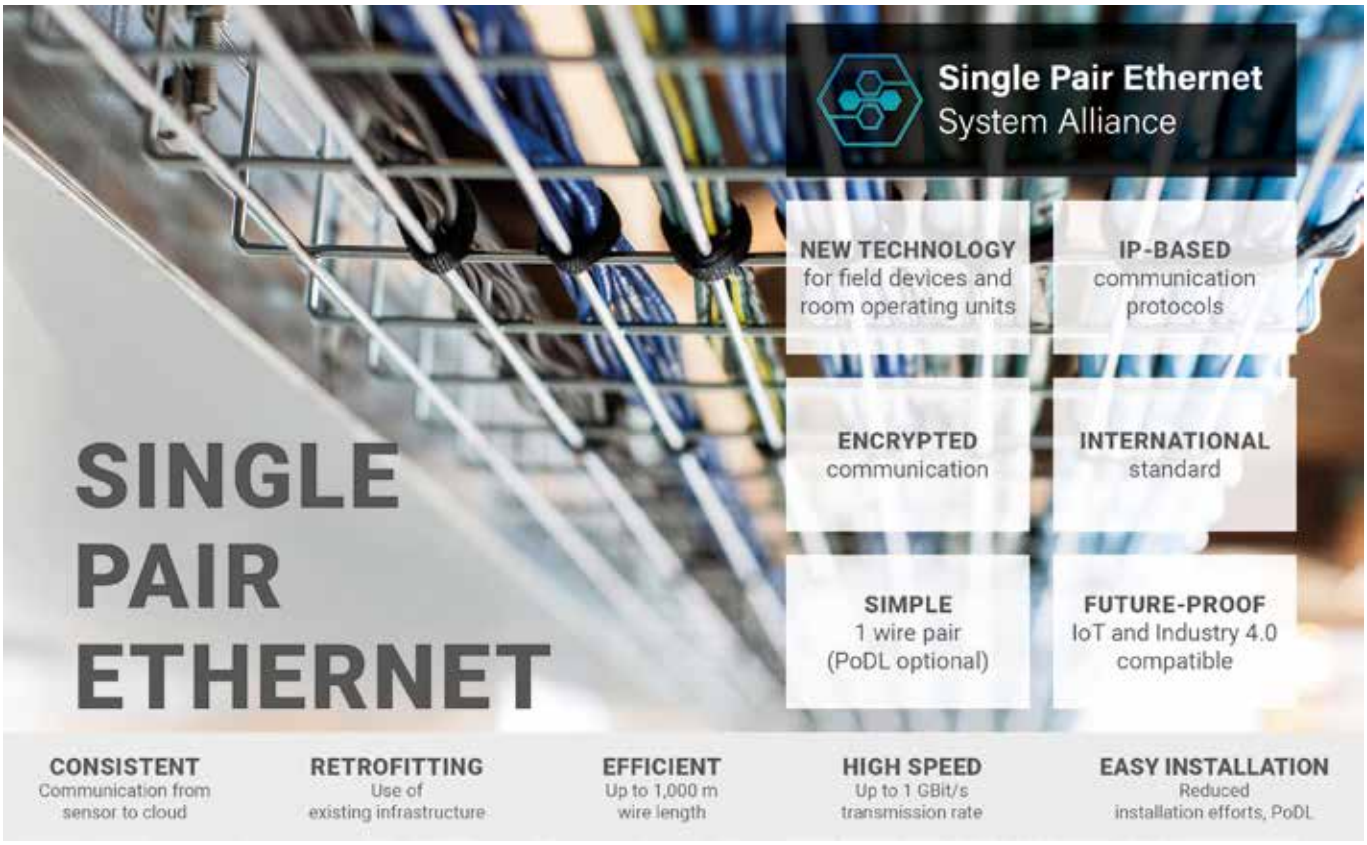
- increase a couple of degrees on the HVAC at certain times of the day if the space is empty, for energy efficiency,
- coordinate the lobby lights to turn on when people are about to arrive if your lift system is part of the BACnet BMS, for energy efficiency and comfort.

The possibilities are endless once all the information and control are in a single place. ■

Yenny Suancha
Product Engineer | Intesis
yesu@hms-networks.com | www.intesis.com

Xavier Jorquera
Technical Writer | Intesis
xajo@hms-networks.com | www.intesis.com

Single Pair Ethernet – Problem Solver in Building Automation



Features and field of application of Single Pair Ethernet (SPE). © Thermokon

The requirements in networked building automation in terms of communication speed and functionality are constantly increasing. Components in a building become more and more communicative. At the same time, new building security requirements such as the EU 2022/2557 CER (Critical Entity Resilience) are being added.

Looking ahead, some existing bus systems and communication standards based on the RS485 protocol reach their limits in terms of communication speed. An immediate response is expected, particularly in the event of switching lights and blinds. Modern room operating units now have high-resolution graphic displays for convenient control of room parameters. In addition to low latency, the data transmitted also require a high communication speed and integration into networks based on the IP protocol. Modern security requirements are largely based on the Internet protocol and can therefore no longer be easily implemented using (existing) RS485 standards.

Single Pair Ethernet (SPE) is one of the latest technologies with the potential to fundamentally change building automation. SPE enables IP data transmission and simultaneous power supply through a single pair of wires, which not only simplifies cabling, but also reduces costs while considerably simplifying installation in a wiring-safe manner. Thermokon regards SPE as one of the key technologies for the future of wired building automation.

Use of SPE Technology for Operating Devices: The Beginning of a New Era

Thermokon will initially introduce the SPE technology in room operating units, as the need for high speed, low latency and high security is particularly important here. These devices require fast and reliable communication with the BMS to ensure the operation of complex systems and to meet the increasing demands of modern building automation.

1. Speed and Latency: Room operating units that need to communicate with other systems in real-time benefit significantly from the high data bandwidth of up to 10 Mbit/s and the low latency of the SPE technology. This improves response times and the efficiency of the entire BMS.

2. Security Requirements: Modern building automation systems must meet high security standards, especially if they transmit sensitive data. The integration of IP-based security standards in SPE-based room operating units ensures secure data transmission and protects them against potential threats.

Using SPE with BACnet

BACnet/IP and BACnet/SC are based on the IP protocol. In these cases, the use of SPE is an ideal alternative to classical IP network cabling. There is no need for time-consuming cabling or the assembly of RJ45 connectors. The plug-in two-wire connection is easy and inexpensive to install. Alternatively, with SPE, the power supply and data cable can be laid separately as usual. Numerous well-known manufacturers are already presenting the first SPE-capable components for building automation as an alternative to RS485.

Application examples of SPE room operating units

- Building management: SPE-based room operating units are ideal for the central control and monitoring of heating, ventilation and air-conditioning (HVAC). They offer precise control and help to increase energy efficiency.
- Lighting and shading control: Thermokon's room control units allow flexible and energy-efficient control of lighting & shading systems, helping to improve energy efficiency and comfort.

Retrofit: Modern Solutions for Existing Systems

Another important area of application for SPE-based room operating units is retrofitting existing infrastructures. Existing automation networks can be adapted to this technology almost cost-neutral as part of a building refurbishment. Research has shown that existing cable infrastructures are already suited for SPE in many cases. The great added value lies in the increase of performance. SPE facilitates integration into existing infrastructures, as less cabling is required, and installation costs are lower. This makes SPE components an attractive solution for modernizing older buildings.

EPBD-Compliant Solutions

The European Energy Performance of Buildings Directive (EPBD) stipulates high demands on the energy efficiency and sustainability of buildings. SPE-based room operating units make a significant contribution to meeting these requirements. By precisely controlling and monitoring HVAC systems as well as lighting and shading systems, Thermokon supports its customers in achieving the required energy targets and operations in compliance with the EPBD. This enables customers / building owners to meet legal requirements, reduce operating costs and ultimately reduce carbon emissions.

Conclusion

Thermokon is convinced that SPE will play a decisive role in the future development of building automation systems. By integrating this technology into their operating units and seamless integration into BACnet networks, they can offer their customers innovative solutions that not only improve the energy efficiency and reliability of a BMS, but also reduce costs and simplify installation. The products show their strength particularly in the retrofit sector and with regards to increasing security requirements. ■

thermokon®
HOME OF SENSOR TECHNOLOGY

Dominique Alt
Head of Product Management | Thermokon Sensortechnik GmbH
dominique.alt@thermokon.de | www.thermokon.de

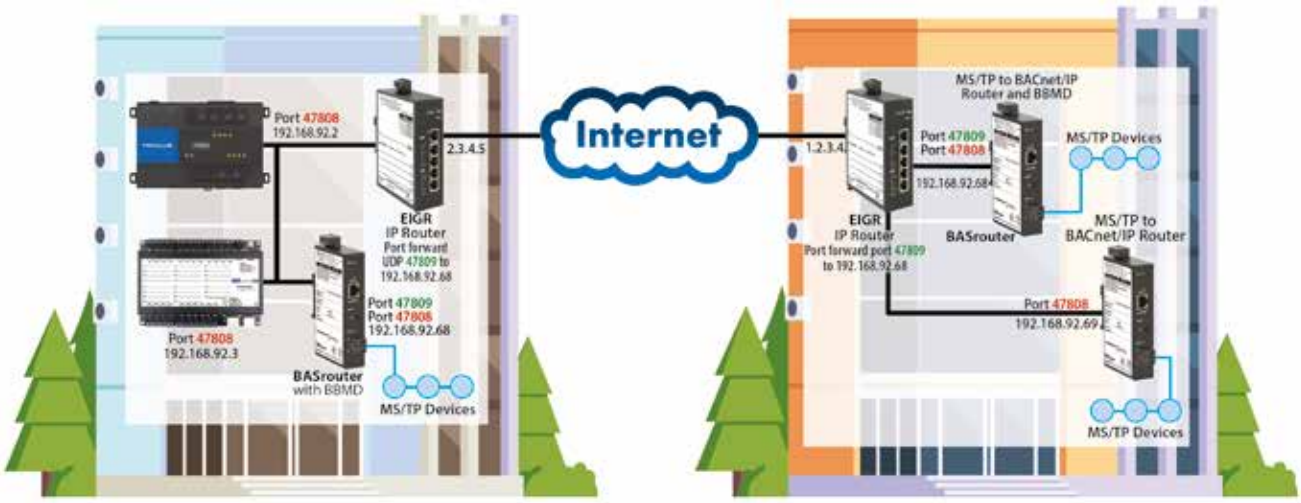
Secure Remote Access to BACnet Systems

The Internet makes it possible for systems integrators to easily manage buildings from the comfort of their home or office. Initial commissioning, remote diagnostics and troubleshooting of the building provide additional savings over the building's lifetime.

Remote access can be achieved using various methods – some are more secure than others. Fortunately, the Building Automation industry is dominated by the BACnet protocol, and its IP version, BACnet/IP, lends itself well to all the enhancements and techniques deployed in the Information Technology (IT) world. Common techniques for remote access involve the use of Port Forwarding through a firewall, setting up BBMDs, and the use of VPNs. But the security provided and their ease of setup for BACnet systems varies. IP routing with Firewalls and VPNs adds to the security of BMS systems. The IP Protocol and TLS form the basis for the new BACnet Secure Connect allowing secure communication.

Remote Access with BACnet/IP

BACnet/IP uses broadcast messages to initially discover other devices. BACnet communication across subnets needs additional configuration since IP Routers do not route broadcast messages. BACnet resolves this issue by utilizing a BACnet/IP Broadcast Management Device (BBMD). The BBMD sends received BACnet broadcast messages as directed messages through the IP router to its partner BBMD devices. The receiving BBMD device retransmits it as a broadcast message to its local network. You can configure each BBMD with the IP addresses of all other BBMDs or have all BBMDs send their broadcast messages to one central BBMD, however, all client devices must utilize the central BBMD. These entries go into the BBMD's Broadcast Distribution Table (BDT). It is possible to have more than one BBMD device on a single subnet and care must be taken while configuring BDT entries. A duplicate entry in BBMD devices will result in broadcast loops.



Typical Typical setup connecting 2 Buildings using Port Forwarding and BBMDs. © Contemporary Controls

Many BACnet/IP devices or applications also support a feature called Foreign Device Registration (FDR). FDR allows the BACnet/IP device or application to send its messages to a BBMD which then forwards broadcast messages to all other BBMDs and all other FDR devices. If a subnet has only FDR supported devices, then it does not need a local BBMD. These devices can register with a BBMD on another subnet. BBMD and FDR allow BACnet devices and application PCs to communicate across subnets, i.e., the Internet. This setup is used to connect buildings or to gather data at a central location from multiple buildings.

Adding Security to BACnet/IP Communications

There are tools that can detect BACnet communication over the Internet by checking for the standard BACnet UDP Port 47808. It is good practice to change this port to a non-standard port if communicating over the Internet. The IP routers/firewalls also provide additional features that should be utilized. A list of IP addresses that can communicate through the firewall can be specified on the Internet facing firewall. Some BACnet routers also provide this Allowlist feature. BACnet/IP communication occurs over UDP and is unencrypted. Using VPNs can provide additional security by encrypting the traffic over the Internet and restricting communication to only authorized VPN endpoints. There is no need to use non-standard BACnet UDP Ports with VPNs. Setting up firewall rules or VPNs requires help from the IT department while the BMS professional can configure the non-standard BACnet UDP port on their own.

Security with BACnet/SC Datalink

The open nature of BACnet/IP and broadcast traffic created some pushback from IT departments. BACnet Secure Connect (BACnet/SC) was released to address these concerns by incorporating the widely used IT security practices. BACnet/SC used connection-oriented TCP instead of UDP and TLS 1.3 for security with encrypted communications. Each device must be authorized to be on the network and assigned a certificate and key. The broadcast discovery protocol and BBMD have been eliminated. BACnet/SC uses a hub and node model. Devices/nodes primarily communicate via the BACnet/SC hub with standard provisions for

BACnet/IP vs BACnet/SC Communications	
BACnet/IP	UDP Broadcast traffic No encryption Any device can join
Firewall Rules	VPN
BACnet/SC	TCP No broadcast traffic Encrypted communications Device authorization required

Benefits of BACnet/SC vs BACnet/IP. Non-standard Ports, Firewall Access Control Lists and VPNs provide additional security. © Contemporary Controls

node-to-node communication. The SC hub can be on the Internet, with nodes at different locations only originating an outbound connection that doesn't require firewall changes. If the hub is located behind the firewall, a port forwarding entry for access from the Internet is needed. But for a remote node or application to successfully connect to the hub, it must have already been provided the credentials (certificate and key) and approved to be part of this network. Temporary access can be granted by creating a certificate for a shorter time duration. The use of BACnet/SC provides security inherently. BACnet/IP and BACnet MS/TP devices can be integrated with BACnet/SC using BACnet routers that support all three datalinks, thus allowing current and future BACnet Systems to be securely interconnected. ■

CONTEMPORARY CONTROLS

Harpartap Parmar
Director of Product Management | Contemporary Controls
hparmar@ccontrols.com | www.ccontrols.com

More BACnet Publications Worth Reading

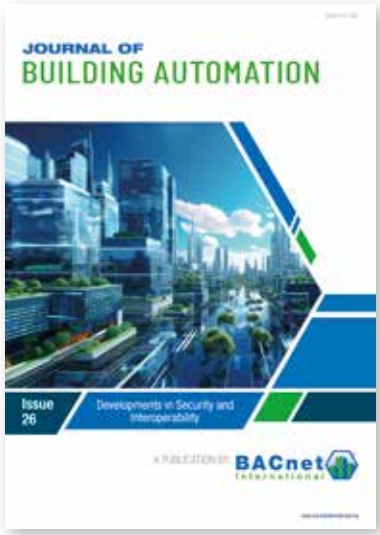
BACnet Europe
Journal 41 – 09/24

bacnetjournal.org/bacnet-journale/bacnet-europe-journal

BACnet France
Journal 17 – 11/24

bacnetjournal.org/bacnet-journale/bacnet-france-journal

Journal of Building Automation



bacnetinternational.org/journals

Calendar of BACnet Events

2025	Event	Location
February 8th – 12th, 2025	ASHRAE Winter Conference	Orlando, FL
February 10th – 12th, 2025	AHR Expo	Orlando, FL
March 17th - 20th, 2025	ISH 2025: BACnet Joint Booth, Academy and BIG-EU Award	Frankfurt, Germany
May 12th – 13th, 2025	BIG-EU Spring Meetings	Lisbon, Portugal
May 14th – 16th, 2025	BIG-EU Plugfest	Lisbon, Portugal

Editorial Notes

BACnet Middle East Journal
ISSN 2190-944X

The BACnet Middle East Journal is the Middle East magazine for building automation based on BACnet technology. Experts, practitioners and professionals show the way in applying and developing the BACnet standard – from building automation trends to devices and application projects; from qualification and training to testing and certification; from who's who in the BACnet community to useful information on events and publications.

Distribution
This Journal can be ordered free of charge by partners, members, media representatives and friends of the BACnet Interest Group. Order the BACnet Middle East Journal by email from: bacnetjournal@tema.de

Online distribution
The BACnet Middle East Journal is initially posted as a Portable Document Format (PDF) File to www.bacnetjournal.org

Editor
TEMA Technologie Marketing AG
Burtscheider Markt 24
52066 Aachen, Germany

Editorial Office
TEMA Technologie Marketing AG
Hans Symanczik (Editor in Chief)
Phone: +49 241 88970-110
email: symanczik@tema.de
Hermann Josef Pilgram
email: pilgram@tema.de

Media Services
TEMA Technologie Marketing AG
Dirk Sistemich
Phone: +49-241-88970-801
email: sistemich@tema.de

Picture credits
TEMA AG or company specified at the end of the text, unless otherwise stated

A VERSATILE INTEROPERABILITY SOLUTION

MSA FieldServer's BACnet Router offers a complete BACnet internetworking solution for BACnet/IP, BACnet Ethernet, and BACnet MS/TP networks, while also providing a secure connection to the cloud.

MSA Grid Cloud Support
Register your BACnet Router to the MSA Grid FieldServer Cloud interface for remote access to local applications, configuration, and device management.

BTL Certification
Most compliant and highest quality BACnet stack enables interoperability and reduces troubleshooting time.

Easy Configuration with Discovery
One page set and forget configuration along with unique network discover capability minimizes installation time.

BACnet Explorer
Minimize commissioning time by automatically discovering all BACnet devices connected to a BACnet network.

Dual RS-485 Port Option
Results in lowest cost per connected device or highest performance (response time) per connected device.

To learn more, **visit msasafety.com/fieldserver**

MSA
The Safety Company