ISSN 2191-7825

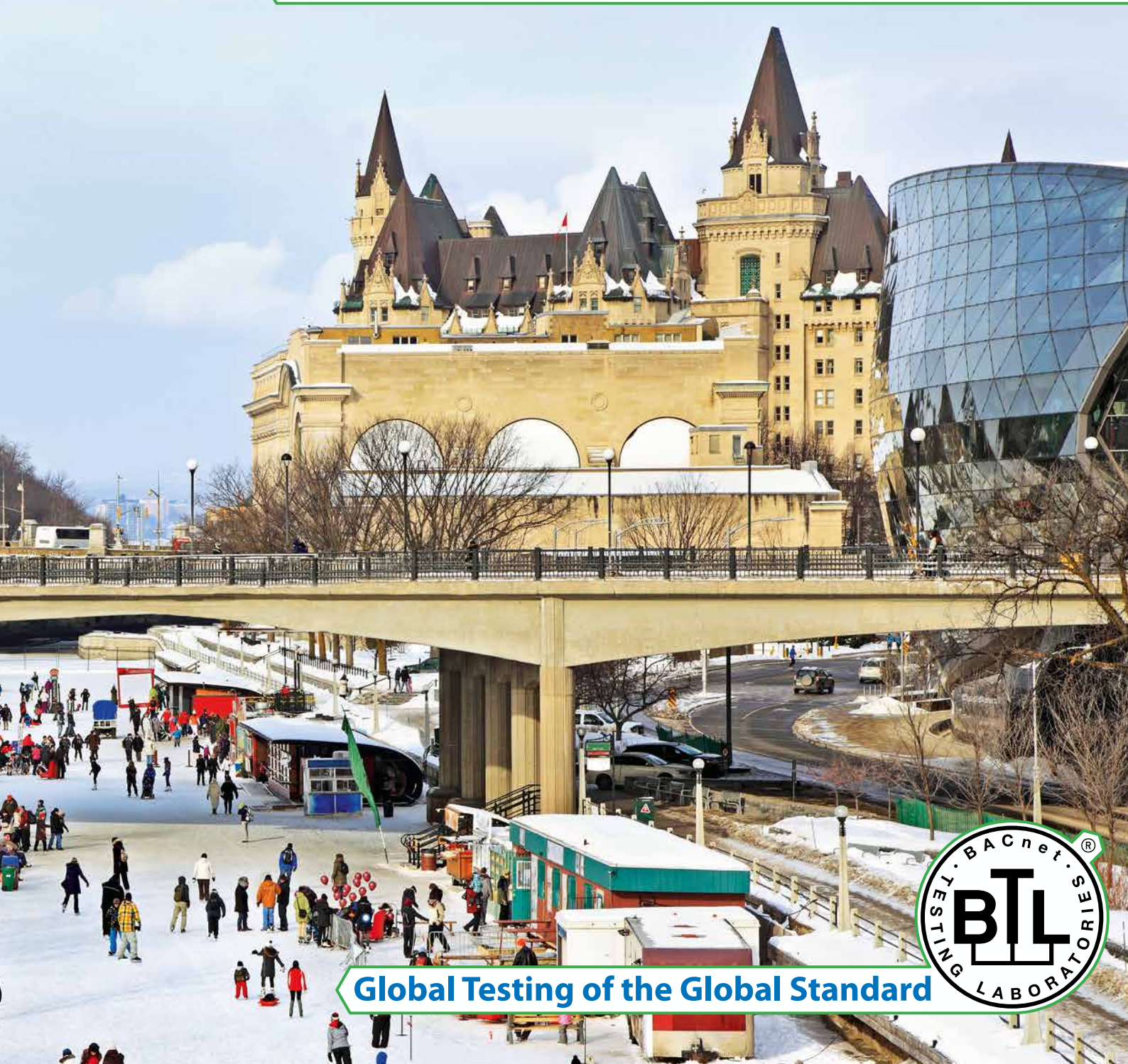
www.bacnetinternational.org

BACnet International JOURNAL

Issue 18

This Issue

BACnet Security: The Big Picture



Global Testing of the Global Standard

the ART of Building Sustainability

1 CERTIFIED OPEN STANDARDS

Ensure a strong level of interoperability by using open protocols which have third-party listing laboratories to verify adherence to your protocol's form and function.

2 SECURE DATA

Employ a single sign on (SSO) architecture with compliance to scalable credentialing architectures and secure tunneling methodologies such as BACnet virtual private networks (B/VPN).

3 INTEGRATED FAULT DETECTION & DIAGNOSTICS

Specify integrated FDD (IFDD) that delivers real-time fault detection, step-by-step root-cause diagnostics while using all your existing cabling structures, including twisted-pair networks.

4 OWNERSHIP OF ANALYTICS

Insist on timely analytics for all stakeholders with complete control of formatting and scheduling while retaining full ownership of your data and the reports generated.

5 SINGLE-APP EXPERIENCE

Create better-connected spaces with real-time access to occupancy, lighting, ventilation, and thermal comfort levels, using a holistic single app on the occupant's mobile device.

6 MIMIMAL WASTE

Select lifecycle-centric manufacturers who minimize the negative impacts of waste with long-term warranty and repair services while adhering to WEEE, RoHS and LEED directives.

7 BACKWARD COMPATIBLE

Enjoy the long-term benefits of suppliers who engineer a path forward to new technologies while remaining backwards compatible without third-party gateways or hardware replacement.

8 OPERATOR TRAINING

Stay on top of regular advances in technology with supplier-certified, multi-lingual online educational videos, technical documentation, software updates, and advanced face-to-face classroom courses.

9 FACTORY-CERTIFIED SERVICE

Choose from a global network of factory-certified service partners who are passionate about long term, consistent, local support for you and your buildings.

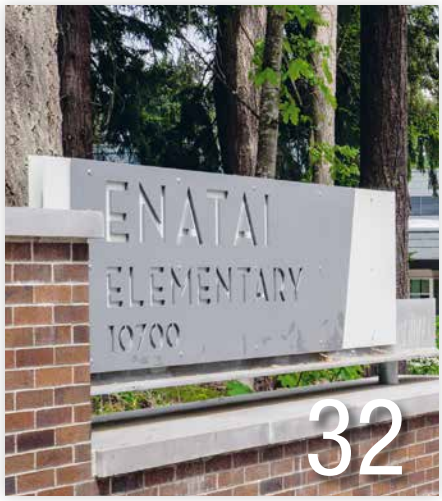
Sustainability requires a high level of integration between HVAC, lighting, and security systems. The art of building sustainability skillfully combines this integration with other technological and supporting elements that must endure over the long term. When these additional elements are maintained over the life of your building, true building sustainability emerges. To learn more about the ART of Building Sustainability please visit **www.reliablecontrols.com.au/TABS**

Better by design™

Reliable® controls

© ABB

© City of Ottawa



© ATS Automation

Cover picture:
City of Ottawa – Rideau Canal Skateway

© City of Ottawa

Content

Issue 18 I Nov. 2020

All issues can be downloaded from https://www.bacnetinternational.org/journal

Letter from the President

Dear Reader,

As I write this note, I do not know exactly what the world will be like at the time it gets published and finds its way to you. The uncertainties created by the global coronavirus pandemic make even short-term predictions difficult. However, there are a few things I know will not change as we continue to work through and eventually move beyond this difficult time:

- We will still be feeling the loss of Mike Newman and his visionary leadership in the BACnet community.
- We will still be in a world where energy efficiency needs to increase, and carbon emissions need to decrease.
- We will still be faced with the need to improve cyber-security in building automation systems.

Knowing these are certainties that transcend the current situation, we have tried to focus this issue on content that will be relevant whenever and wherever you find yourself reading it.

The BACnet world is a different place without Mike Newman, widely recognized as the founding father of the BACnet protocol. You can hear about the beginning of BACnet and its evolution through the years in Mike's own words by searching YouTube for a video titled, "BACnet Retrospective from People Who Were There." It is a video featuring Mike and Steve Bushby in a casual session at the 2018 BACnet Testing Symposium.

Worldwide progress in improving energy efficiency and carbon footprint in commercial buildings is deeply connected to effective control systems. In this issue we address several practical implementation topics through articles relating to cloud connectivity, VFDs, digital twins, BACnet Broadcast Management Devices (BBMDs) and protocol integration.

Network security has been an important topic ever since networks were invented. For many years building controls and automation networks were less impacted by security issues than IT networks. That has been changing for a while now and more recently cybersecurity has become a significant topic of conversation and a focus for BACnet development. In this issue we address BACnet Secure Connect (BACnet/SC), one of the most important developments in this area. We have an excellent overview article by David Fisher and an article describing the BACnet Interoperability Acceleration Program that includes 26 companies and over 100 technical participants. The resulting BACnet/SC Reference Implementation and System Test Bench are invaluable tools for all product developers. See the news article on the program for more information.

Whether you are a building owner/operator, product developer, system integrator, consulting engineer or any other member of the BACnet community, I hope you find useful information and insights in this issue of the BACnet International Journal.

© McMillan

Andy McMillan
President and Managing Director | BACnet International
andym@bacnetinternational.org | www.bacnetinternational.org

ABOUT THE AUTHOR

Andy McMillan is President and Managing Director of BACnet International, where he works with users and suppliers to expand and enhance the BACnet community. Previously he served as President of a building automation and energy management business unit of Philips Lighting.

BACnet/SC: The Big Picture

Introduction

Every day we hear about concerns over cybersecurity and the disruptive effects it could have on building infrastructure and operations. Often cited concerns are network and information security and infrastructure integrity. The growth of interest in cloud-based applications has building owners, managers, BAS and IT professionals under pressure to create BAS infrastructures that provide very high levels of security.

These concerns are well understood by BACnet's SSPC-135, who have been hard at work for the past five years on a new technology called BACnet Secure Connect (BACnet/SC) which is now part of the BACnet standard. BACnet/SC provides the means to create secure communications connections between BAS devices both across the cloud, and within facilities. BACnet/SC uses the latest techniques for security and integrates easily with IT infrastructure. At the same time, BACnet/SC preserves 100% of the capabilities and is backward-compatible with all existing BACnet deployments and devices.

Why Do We Need This?

The world got along without the Internet for a very long time. But no one can deny the millions of benefits that worldwide interconnectedness has provided and continues to grow at a relentless pace. But along with progress there are also new challenges. Once our buildings and their communications infrastructure are exposed to the Internet, they become a target for exploitation and potential attack by others.

Even without Internet connectivity there are many scenarios under which these same infrastructures can be exploited and disrupted from within by those with malicious intent. Ironically, after decades of successful effort to bring international standards into BAS communications, that same standardization can be used against us.

None of this is news to the technology side of buildings. BAS and IT experts have known about these possibilities for a long time and have developed standards for securing against these kinds of threats. However, it is only recently that these standards have come together in new ways that are much better suited to addressing all of the concerns of owners, managers, BAS and IT professionals.

Can't I Already Buy Solutions to These Problems?

Sure, there are many companies offering what I'll call proprietary solutions to cybersecurity, some of which are applicable to BAS as well as IT requirements. But if we've learned anything from the past 30 years of BAS technology developments, it's that standards are better and more robust long-term investments. Nearly every proprietary BAS that existed 30 years ago has been displaced or replaced by BACnet-based systems for this very reason.

What Exactly Does BACnet/SC Do?

BACnet/SC allows two BAS devices to establish a highly secure and encrypted connection between each other, over which conventional BACnet messages can be sent and received. These connections can't be "hacked" and can't be decrypted without proper certifications, and the certifications themselves can't be forged or faked. This assures that only legitimate devices can get connected together, and that the content of their communications is completely private. The mechanisms that assure this security are based on established international standards and best practices and are fully aligned with IT standards.

What that means is that BACnet/SC uses the same mechanisms that banks, military and other entities use to secure their communications.

BACnet/SC allows two devices to make such connections with each other directly. Having said that, it is likely going to be much more common to see essentially two kinds of BACnet/SC devices:

- A BACnet/SC "hub" that acts as a centralized conversation manager
- A BACnet/SC "node" that makes a connection to the hub, and sends all messages through the hub, which in turn redistributes the message(s) to recipient nodes

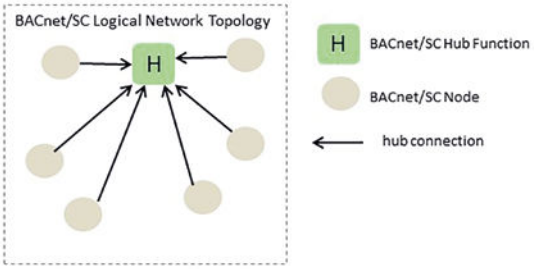


Figure 1 ©ASHRAE www.ashrae.org

In any system where there are centralized components, such as the BACnet/SC hub, it is desirable to have the possibility of redundancy. BACnet/SC allows you to have primary and failover hubs. If nodes can't reach the primary hub, or lose connection and can't reestablish it, they can turn to a failover hub instead. When the primary hub comes back, the nodes can then switch back to the primary.

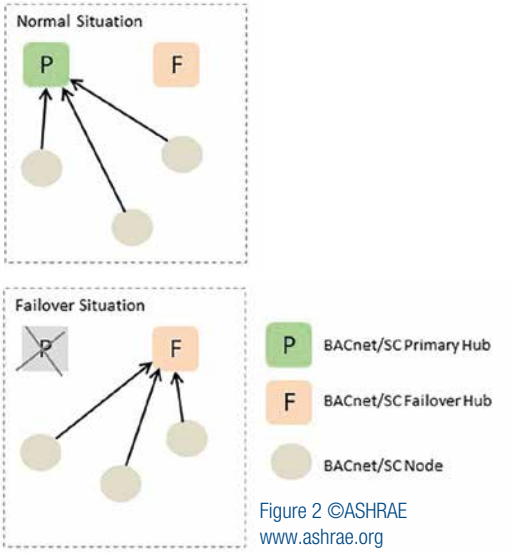


Figure 2 ©ASHRAE www.ashrae.org

Because nodes are allowed to create and accept direct connections, the real picture may look more like Figure 3. The point is that BACnet/SC has flexibility in terms of the kind of architecture that can be used in secure portions of a BACnet network.

When Would BACnet/SC Be Beneficial?

There are many ways that BACnet/SC can be deployed that provide distinct benefits. Like all security, the question is: what is the threat that you want to secure against?

If the concern is securing all BACnet devices against internal threats, then you can convert all existing BACnet devices to use BACnet/SC. In this scenario even hackers with physical access to the network, i.e. inside of a firewall, would be unable to disrupt the BACnet network.

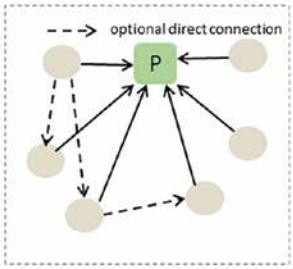


Figure 3 ©ASHRAE www.ashrae.org

The problem here is that at the moment BACnet/SC can't "secure" MS/TP devices. So this scenario only works if every device is a BACnet/SC device (and therefore using Ethernet and an IP infrastructure).

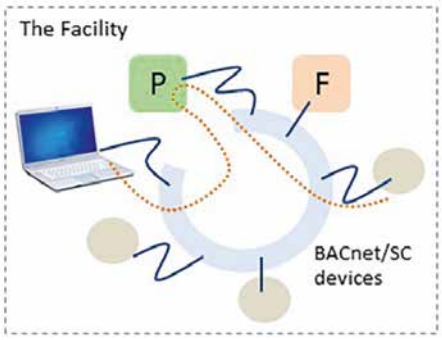


Figure 4 ©ASHRAE www.ashrae.org

This might be a viable option for some, but more realistically won't there be a period of time when there will need to be a mixture of (new) BACnet/SC devices as well as older "regular" BACnet devices? Yes and that's where BACnet routers come into the picture.

In this diagram, the main network is secure because all of its devices are using BACnet/SC. But there are also some "legacy" BACnet/IP and MS/TP devices that can't be replaced with equivalent BACnet/SC devices.

The solution is to use a BACnet router that can route between SC-IP or one that can route between SC-MS/TP. In either case the "local" network portions (shown with red *) are "insecure" in the sense that they could be hacked by someone with physical access to these local segments. Of course, more traditional methods, such as VPN, could still be used to provide security on the BACnet/IP segment.

Not everyone needs or wants this kind of everywhere security. Much more common is the desire to have Internet accessibility to the building BAS that is secure on the public facing (Internet) side of the building. There are several different ways to do this.

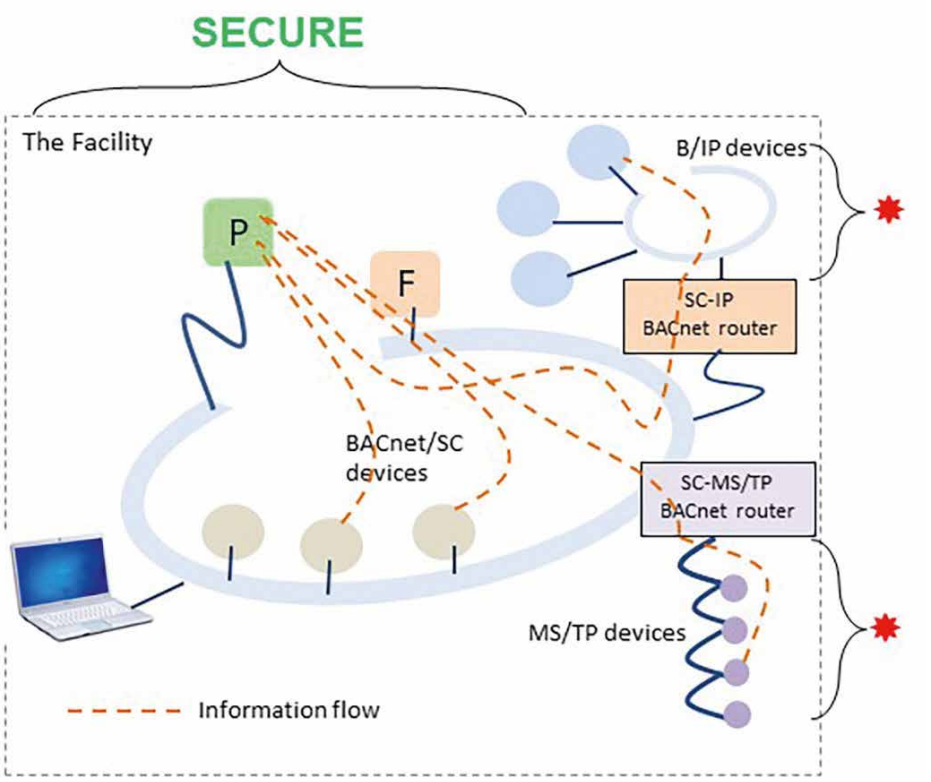


Figure 5 ©ASHRAE www.ashrae.org

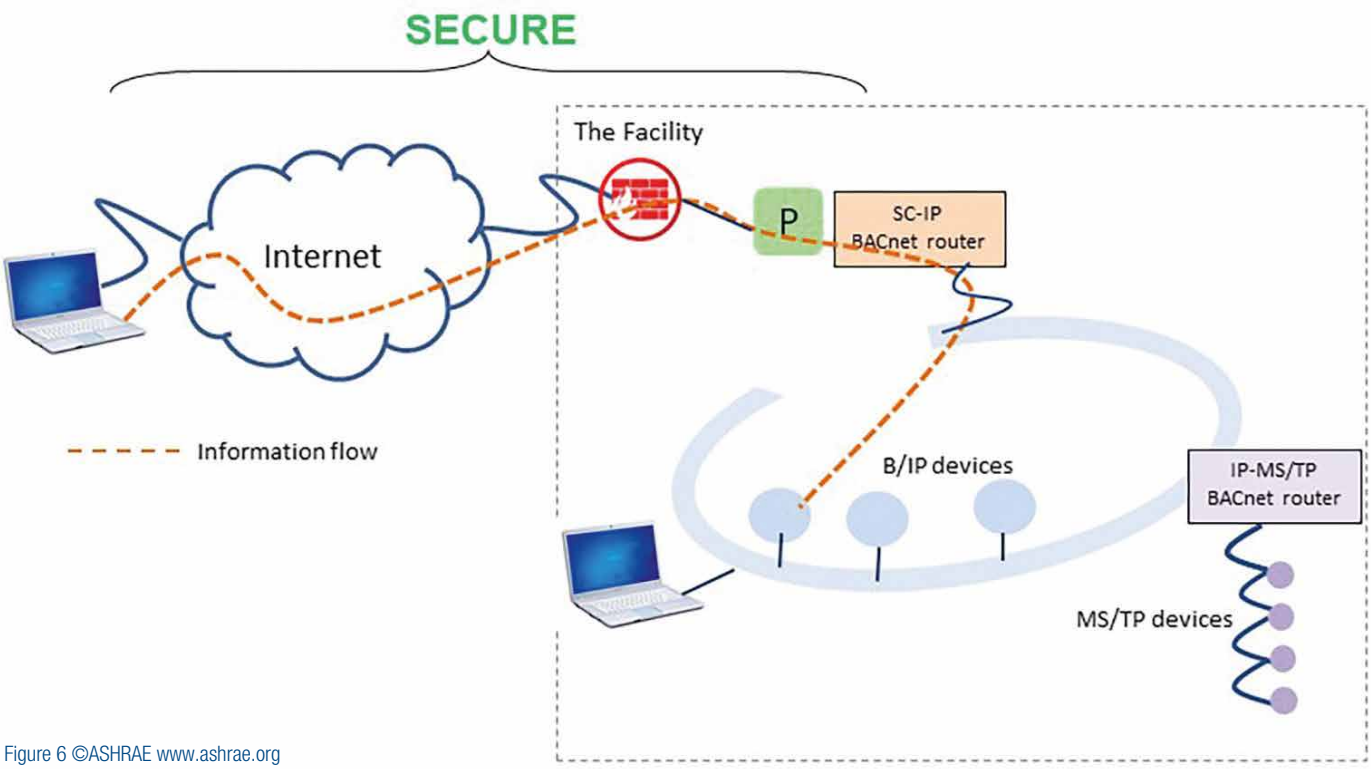


Figure 6 ©ASHRAE www.ashrae.org

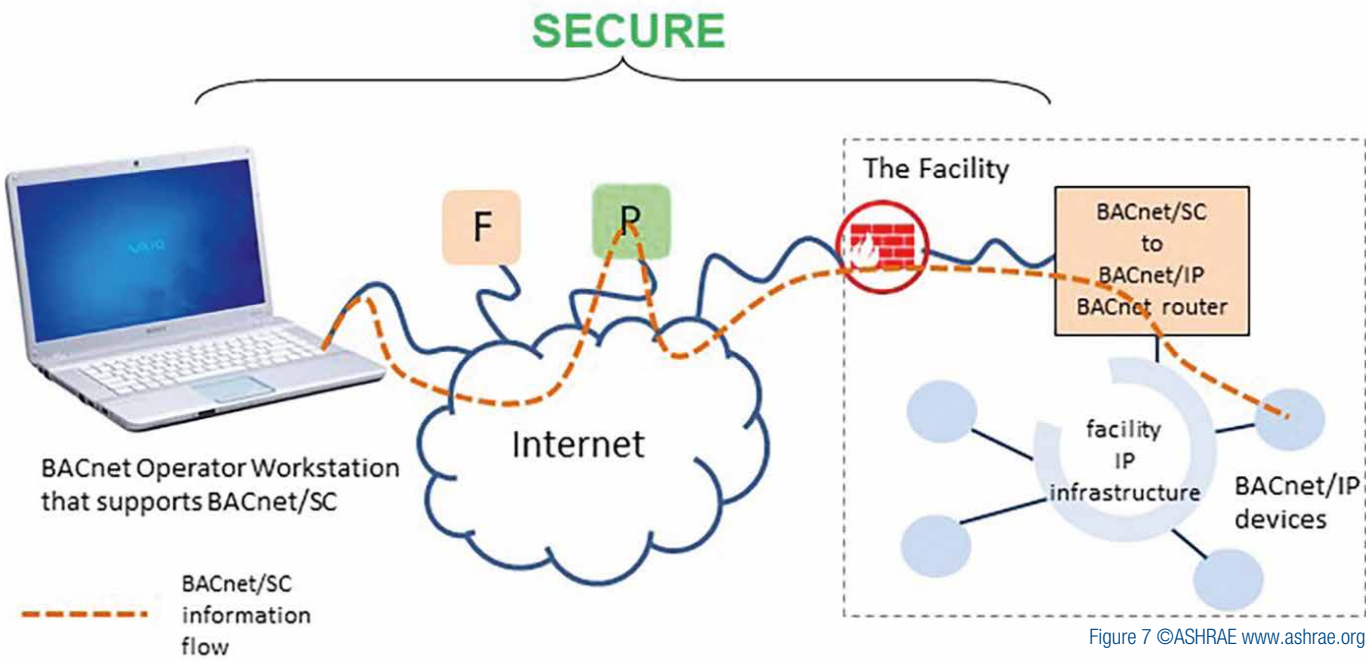


Figure 7 ©ASHRAE www.ashrae.org

One way is to use either a BACnet/SC hub and an SC-IP router, or a device that can do both functions, on the inside of the building firewall. This provides secure access across the Internet, and then business as usual inside the building.

Another solution is to put the BACnet/SC hub "in the cloud", and an SC-IP router inside the building firewall. This makes the external (Internet) part of the network secure, while the internal part of the building network is the same as it is today.

What Does 100% Backward-Compatible Mean?

In this context what we mean is that existing BACnet/IP and MS/TP devices can remain in-place and can interact with BACnet/SC devices through SC-X routers. This allows you to migrate existing systems to higher levels of security in an incremental fashion. For device manufacturers it means that they don't have to reinvent all of their BACnet devices since 90% of what they do for BACnet will be exactly the same. We can expect that most manufacturers of BACnet routers will also adopt BACnet/SC into their existing products. This will likely be only a software change not necessarily requiring costly replacement.

New Challenges

While BACnet/SC does provide a much more secure network infrastructure, there is of course a cost and new challenges. One of the challenges is the creation and deployment of so-called "secure certificates". These are somewhat like master keys and are used in the generation and authentication of BACnet/SC connections. As part of the ongoing effort to achieve a more "holistic" kind of cybersecurity, BACnet is also working on standardized methods of certificate creation and deployment that will ease the administrative burden of using BACnet/SC.

It's also important to keep the human element in mind when implementing any cybersecurity solution. BACnet/SC takes us a big step closer, but humans are still going to play a very central role in achieving higher levels of cybersecurity.

Conclusion

BACnet/SC makes it much easier to create secure and standardized BAS infrastructure that is backward-compatible with existing BACnet deployments, friendly to IT best practices and enabling cloud-based applications.

© Fisher

David Fisher
President | PolarSoft Inc
dfisher@polarsoft.com | https://polarsoft.com

ABOUT THE AUTHOR

David Fisher is president of PolarSoft Inc. a Pittsburgh-based software company that specializes in BACnet software development and consulting. He is an ASHRAE Life Member and consultant to SSPC-135.

Fisher was a charter voting member of ASHRAE's SPC 135P and has been very active in the development of the BACnet Standard since its inception. He has over 45 years experience in real-time software, human-interface design and distributed direct digital control systems. He attended Carnegie-Mellon University where he studied Computer Science and Artificial Intelligence.

Proper BACnet Integration to a VFD

Which Points to Monitor and Why

Variable frequency drives (VFDs), which are widely used in HVAC systems, control the speed of motors used on pump and fan applications. Their ability to provide energy (cost) savings and improved flow control (comfort) value have been well documented and accepted in the HVAC industry. Although VFDs are commonly integrated with building automation systems (BAS), they are often not integrated in such a way as to extract their full value for the building owner, chief engineer, and maintenance personnel. In this article we will review how to use BACnet to take full advantage of the valuable information within the VFD.

Most HVAC VFDs have BACnet MS/TP as a standard protocol, and many also have BACnet/IP available as an option. The information within the VFD is the same for both BACnet MS/TP and BACnet/IP. VFDs can be controlled and/or monitored over BACnet. The most common installation has the VFD controlled (start/stop and speed reference) via hardwire and then monitored over BACnet. Controlling the VFD over BACnet can provide additional installation related cost savings, but the hardwire control versus BACnet control will be a conversation for another day. This article focuses on the features and points that can be monitored over BACnet.

The following information identifies some key VFD BACnet objects that should be monitored by the BAS to provide full value. The operator workstation (OWS) should include this information either on the graphics, a dashboard, a trend log, or a combination of these methods.

Run/Stop Status

This fundamental piece of information indicates whether the VFD is running or stopped. This data point is used by chief engineers and maintenance personnel to confirm the state of the unit when they get that initial call about an area being too warm or too cold.

VFD Fault Status

This status indicates whether the VFD has experienced a fault. A fault occurs when the VFD identifies a situation, such as a damaged motor, and prevents the VFD from running.

Fault Type

Assuming a fault occurred, the object identifies the type of fault. This information is key to support remote troubleshooting. Technicians and maintenance personnel appreciate how this object gives them a heads-up on what tools to bring, or items to focus on, before they even get in front of the drive.

System Safety/Permissive Status (Digital Inputs)

Safeties from the system should be wired back to the VFD, as this allows the safety to work in both Auto and Hand modes of VFD operation. Safeties for an air handler include devices such as a high static pressure switch, freeze stat, fire stat, or smoke sensor. The discharge air damper end switch feedback is a good example of a run permissive interlock. Each safety should be wired to a unique digital input (DI) on the VFD. This allows each DI to be monitored over BACnet, so if the system does have a safety go open, the OWS clearly indicates which safety opened. This information allows the maintenance personnel to know what caused the VFD to stop operating before they are in front of the air handler, again reducing the amount of time spent troubleshooting. Having the controls contractor bring each safety to a unique DI (as opposed to putting them all in series to a single DI) is a minor coordination challenge with implementing this feature, thus it should be clearly specified.

Output Frequency (or Output Speed)

The output frequency/speed advises how fast the VFD is running the motor. VFDs control the motor speed by controlling the frequency and voltage to the motor. Output frequency information can be used for troubleshooting. Trending this point allows a better understanding on how the equipment operates over the course of the day.

Output Current

The output current (amps) data is used for remote troubleshooting. Having the motor's full load amp rating documented on the graphics is helpful as a comparison point.

Instantaneous Power

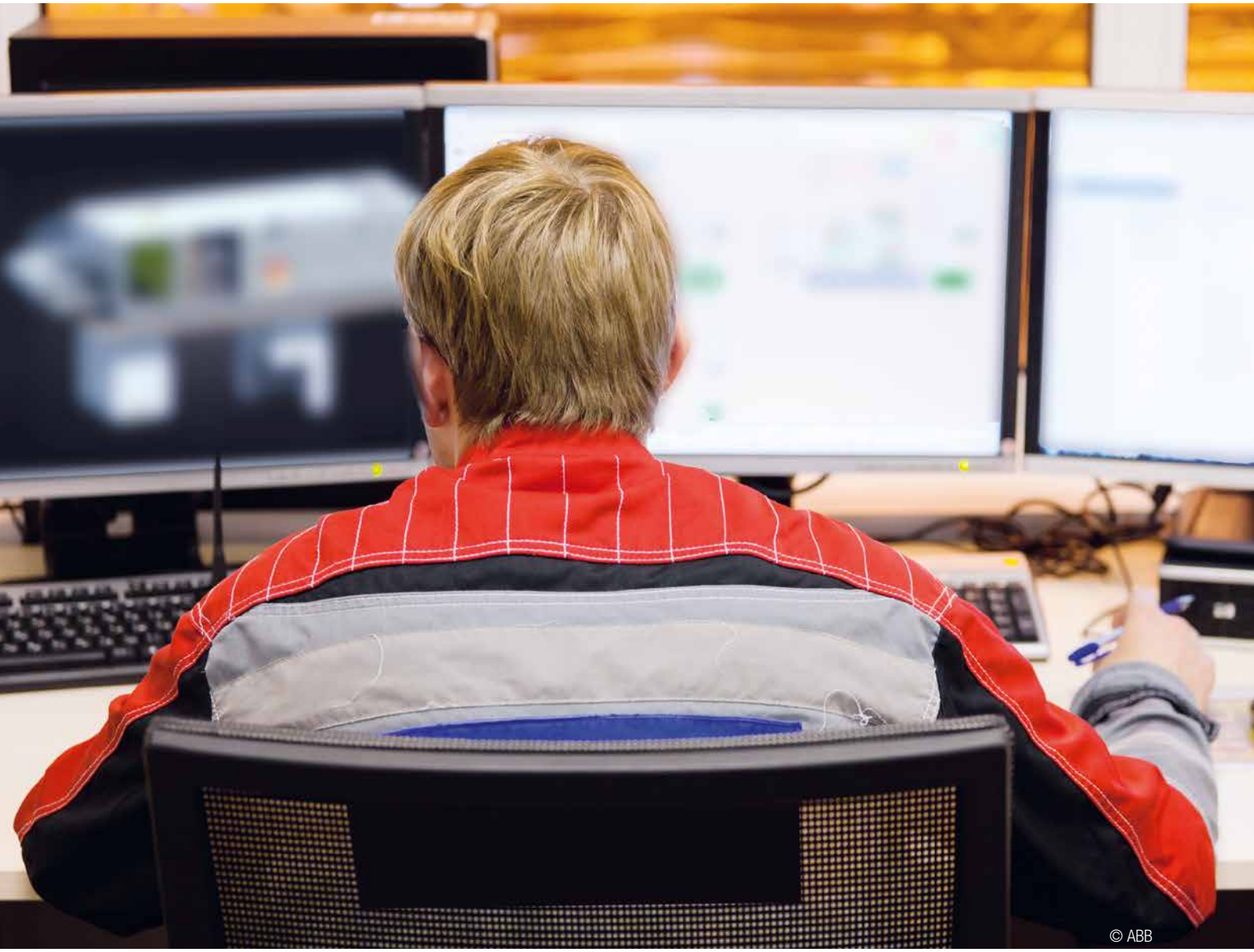
Building owners and chief engineers are looking to better understand where their power (kW) is being consumed. To gather this understanding, some solutions involve installing power meters (submeters) throughout the building. Adding all those meters on VFD controlled equipment are unnecessary costs in most situations, as the VFD can provide power (kW) information at no additional cost. Pulling the power information from VFDs can be used toward earning LEED® credits, such as the Measurement & Verification credit, for providing an understanding and accountability of the power consumption of the building. The OWS should display instantaneous kW for the loads in the system and have trends set up to graph kW through the day.

Cumulative Power

The cumulative output power (kWh) is the power consumed over time. Most VFDs have power metering that includes kWh counters, in addition to the instantaneous kW data. The savvy BAS integrations query the VFD once a month and record this kWh data. Month over month, and year over year comparisons can now be tracked and historical databases are created in the BAS. This data is used to set baselines and identify trends that may indicate an issue, such as a dirty filter, that was missed during the last maintenance schedule.

Hand vs Auto Status

Auto mode indicates the VFD is following the commands from the BAS. A VFD should typically be operating in auto mode. Hand mode allows the drive to be controlled manually via its control panel. Sometimes a maintenance person may need to temporarily put a VFD into hand mode and override the BAS commands. Far too often, the VFD is forgotten about, and left in hand mode while operating the fan or pump at or near full speed. Leaving a VFD in hand mode results in wasted energy, and thus higher utility bills. The OWS should include an indication of hand or auto status and generate an alarm if the VFD is placed into hand mode.



Loss of Load (if Applicable to the Application)

Loss of load (also known as proof of flow) indication identifies a situation where the motor has no load. This scenario is usually the result of a broken belt or broken coupling. In the days before VFDs, the BAS monitored current sensors to identify a broken belt situation. Unfortunately, that practice continues today with external current sensors installed between the VFD and motor. VFDs internally sense current and torque, so there is no need to install the external current sensor. In fact, with induction motors, identifying a broken belt scenario by monitoring torque is much more reliable than monitoring current. Due to the magnetizing current of an induction motor, there is a rather small difference in current draw between no load and light load, making torque the better indicator to monitor.

VFD Temperature

The VFD temperature indicates the temperature of its output power devices. These devices are designed to operate at a high temperature, and depending on the brand of VFD, the temperature indication could be in C, F, or percent of trip level. The key is to set up trends in the BAS that allow a comparison of temperature over time. The trending of temperature can be used to indicate that a VFD needs to have its heatsink cleaned or has a failing cooling fan.

Input Voltage (or DC Bus Voltage)

While some VFDs will indicate input voltage, all VFDs will indicate DC bus voltage. The DC bus voltage is based on the input line voltage; and under load, the DC bus voltage is approximately equal to the input voltage multiplied by 1.35. Under light loads, the DC bus voltage is closer to the input voltage multiplied by 1.414. Understanding the voltage supplied to the drive is a troubleshooting tool. This first level of troubleshooting information reduces how often maintenance personnel need to take live voltage measurements, and thus gear up with appropriate personal protection equipment (PPE).

Analog inputs

Analog inputs (AI) should be monitored for a variety of reasons. The monitoring of the AI verifies the signal is reaching the VFD for applications where the VFD follows a speed command signal from the BAS. For other applications where the VFD is acting as a controller, and utilizing its internal PID control, monitoring the AI allows the OWS to display the sensor feedback. For example, the sump temp sensor on a cooling tower can be wired to the VFD, and the BAS

would monitor the VFD's AI and allow the OWS to display the actual water temperature.

Analog outputs

Some applications use the VFD's analog outputs (AO) to control an external process. One example is using the VFD's AO to control the chilled water valve position. In those applications, the AO should be monitored, and AO trends created in the OWS.

Relay outputs

Like the above example, some applications use the VFD's relay outputs (RO) to control an external process. A common example uses the VFD's RO to control an isolation damper on an air handler. In those applications, the RO should be monitored, and RO trends created in the OWS.

Checksum

While not available on all HVAC VFDs, the checksum value is a very useful item to monitor for consistency and security purposes. Security concerns, and features to make HVAC systems more secure, continue to grow in the industry. With this feature, the VFD assigns a checksum value based on how the VFD is programmed. If a parameter setting is changed within the VFD, a new checksum value is created. The BAS should monitor the checksum value, and if it changes, the BAS should indicate an alarm on the OWS. The alarm alerts the chief engineer that a change was made to that drive's programming, and now they can investigate whether it should have been changed or not.

Many consulting engineers and temperature control contractors (TCC) agree that there is value in the above information being readily available for the building owner, chief engineer, and maintenance personnel. Most building owners, chief engineers, and maintenance personnel agree that they'd like to see this information. So if that's the case, why aren't all systems including this information today?

There is no single answer to the above question. We live in a world where the lowest bidder often gets the project, and the lowest TCC bidder may not have included some of those nice-to-have-features (NTHF) unless they were clearly specified. The TCC technician may not have the time to implement those features, or the training to know those features were even possible. Consulting engineers may not have clearly specified the NTHF, as they were focused on other core functionality needs; in addition, NTHFs (like the checksum feature) are not available from all VFD vendors. The building owner/operator may not know those features exist, and therefore do not ask the consulting engineer to specify them.

Moving forward, how do we implement the NTHF in the BAS and OWS? It starts with organizations like BACnet International spreading the knowledge that allows building owners to talk to their consulting engineer about what they'd like to see. Consulting engineers naturally want to specify a quality solution and understanding what the VFD can provide helps them know what to specify. TCCs at the factory level can update their standard graphic templates to include NTHFs, and the local TCC technician can further adjust the templates based on the application or customer needs. Information must be displayed in a way that is easy to access and understand. Chief engineers who engage in continuous commissioning with their TCC can have NTHFs added to their OWS over time.

COVID-19 has impacted how buildings are used and operated. Certain situations only allow essential personnel into the building. BACnet, combined with properly integrated devices, supports the opportunity for remote troubleshooting. In some cases, the TCC no longer needs to send a technician to troubleshoot a problem locally. Instead, the TCC troubleshoots the problem remotely and advises the local chief engineer or maintenance personnel what needs to be done to correct the problem. In this example, the third party TCC never needed to go into the building, which was the ultimate form of social distancing.

We live in a world of big data. VFDs in HVAC systems are filled with valuable data and BACnet can securely access that data. Having the right data readily available saves time and money. Displaying (and trending) the data points outlined in this article is another step forward in using big data to help a building owner and chief engineer safely and effectively manage their building.

© Skell

Tim Skell
Sales Application Engineering Manager | ABB
tim.r.skell@us.abb.com | www.abb.com
Connect: www.linkedin.com/in/tim-skell

ABOUT THE AUTHOR

Tim Skell, Sales Application Engineering Manager at ABB, has been working with variable frequency drives (VFDs) in the HVAC industry for over 15 years. He is also active in the BACnet community and has received a past BACnet Member of the Year award..

Two Protocols Are Better Than NONE

If you are looking for one communications protocol that does everything, for everyone in the BAS industry, all the time, it does not exist!

The front runner is certainly BACnet, as documented by the number of installed systems. The BACnet market share is over 60% globally and more than 80% in North American, and it continues to grow rapidly. BACnet is free to use. The success of BACnet is fueled by the fact that it is an open protocol managed by ASHRAE SSPC 135 (BACnet Committee) and supported by an army of volunteers, BAS companies, and academia. The BACnet committee continues to evolve the standard to meet the ever-changing needs of the industry. The SSPC 135 committee meets quarterly to revise and expand the protocol. BACnet is an ISO standard and is independently testable and certifiable.

BACnet International is an industry association that promotes its use, provides education, testing and certification services. BACnet International oversees operation of the BACnet Testing Laboratories (BTL) and maintains a global listing of tested products.

Consistent meta-data for sites, devices, and points that convey the function of the objects simply did not exist in the BACnet world. Almost everything in this area was left up to the developer or installer.

Project Haystack evolved as analytics, energy management, and other value-added applications gained momentum in the marketplace. Haystack tagging provides a way of uniquely and consistently identifying objects in a building automation system at all levels of the architecture. The Haystack RESTful protocol was added as a way of extracting tagged data from an automation system for analysis by value added applications.

With Smart Building, Smart City, and digitalization initiatives gaining momentum it is hard for the BAS industry to keep up. Cybersecurity is front and center as the most important topic. BACnet/SC will address these needs.

Multiple networking transport standards are available to carry the BACnet payload. The BACnet payload is a series of objects, properties, and services that implement the mission of BACnet. The standard does not tell manufacturers how to implement their algorithms or sequences of operation behind the BACnet objects and services. So, it leaves plenty of room for innovation and competition. The BACnet services and transports can evolve independently of each other. So, as stove piped applications in buildings converge to Smart Buildings and Smart Cities, new objects and services will be added to BACnet.

Similarly, the Haystack community has been very active. The tagging syntax, dictionary, and supporting relationship definitions have evolved as the needs of the value-added applications community have evolved and become more sophisticated. Haystack 4 represents a significant step forward in tagging technology. The most critical open issue in this community is that many value-added applications require a labor intensive and error prone process of manually applying Haystack tags to data before it can be processed.

The latest BACnet standard ANSI/ASHRAE Standard 135-2016 introduced a new optional property to each BACnet object. The TAGS property is an array of tag names and values that describe the characteristics, restrictions, relationships, and semantics of the containing object. BACnet Standard 135-2016 also introduced Annex Y – Abstract Data Model. This Annex defines the methodology for constructing and naming TAGS within BACnet but does not include a tags dictionary. It also provides guidance on how to identify TAGS defined by organizations outside of ASHRAE.

Since the standard stopped short of providing a tagging dictionary, the adoption level appears to be quite low. However, the functionality is there and should be utilized. In an ideal world there would be one BAS protocol and one tagging dictionary. The BACnet, Haystack, and Brick Schema communities are working together under the auspices of ASHRAE Standard 223P to define a protocol independent TAGGING dictionary. This effort should accelerate the adoption of tagging capabilities into BACnet protocol stacks and client implementations. But this will take time. With most organizations having limited resources, it will probably take longer than anyone would like. However, it is obvious that the commitment to make this happen is there.

Recently, here at S4 we have started looking at BACnet a bit differently than we have in the past. We have been doing it a disservice by treating it only as a communications protocol. It is much more than that. It is an "environment" that enables the implementation of ASHRAE building standards in a way that is Open and Interoperable. BACnet objects and services facilitate local control of building infrastructure for real time control operations. BACnet transport options provide multiple ways to move the BACnet objects between systems.

Two Protocols are better than NONE!

ABOUT THE AUTHOR

Steve Jones founded The S4 Group, Inc. in 2002. His professional experience includes delivering networking and integration services for carriers, networking vendors, and system integration companies in both the government and commercial sectors, and he is currently Chair of the BACnet International Marketing Committee.

Mr. Jones previously held multiple positions with Johnson Controls focusing on developing enterprise solutions and integrating the Metasys® Building Automation System into customers' IT environments, network infrastructure, and management platforms. He belonged to both ASHRAE and BACnet International and reviewed BACnet standard Annex J (BACnet/IP) as it was being adopted. He holds a Master's degree in Computer Science from Stevens Institute of Technology, a Bachelor's degree in Computer Science from Rutgers University, and an Associate degree in Computer Science from Penn State.

© Jones

Steve Jones
Managing Partner | The S4 Group, Inc.
sejones@thes4group.com | www.thes4group.com
Connect: www.linkedin.com/in/stevejoness4group

All About BACnet Broadcast Management Devices (BBMDs)

Modern local area networks are fast, robust, and secure which makes them ideal to support a BACnet internetwork, an international standard for building automation controls and networking. A BACnet internetwork is composed of BACnet networks each of which includes only devices of the same BACnet network protocol. As need, BACnet routers convert the various protocols to join all the networks into one BACnet internetwork.

In many installations, the BACnet IP protocol is used to integrate the various BACnet networks because it interfaces easily with the LAN. However, BACnet depends on the broadcast messages "Who Is" and "I Am" for discovering and sharing data among devices and workstations. Because broadcasting can pose a threat to network security, most IT managers block broadcasting between IP subnetworks at the IP router. To overcome blocked broadcasts, one BACnet solution places a BACnet Broadcast Management Device (BBMD) on every subnetwork that must carry BACnet traffic. A BBMD may be part of a dedicated BACnet router, such as a BAC-5051E, embedded in a BACnet device, or a software service running on a computer.

BBMDs monitor network traffic for BACnet broadcast messages. When they receive a broadcast message, they repackage it and then forward it to the other BBMDs as a normal network message. The receiving BBMDs then unpackage the message and rebroadcast it on the local subnetworks as the original BACnet broadcast message. Subnetworks know the location of other BBMDs because of an internal table that is part of every BBMD. The table, known as the Broadcast Distribution Table or BDT, contains the address of every other BBMD on the internetwork. The BDT is added by a technician as part of the installation and configuration of the BBMD.

When configuring BBMDs and network routing, the following rules will help reduce network problems.

- Use a BBMD for permanent devices and workstations. Use Foreign Devices, detailed in Scenario 4: Foreign Device Registration, only for temporary connections.
- Connect only one BBMD with the same port number to a subnetwork.
- The BDT in every BBMD must include all BBMDs on the BACnet internetwork. If a BBMD is added to an internetwork, all BDTs must be updated.
- The BBMD must have a static IP address. The IT department must supply this address.

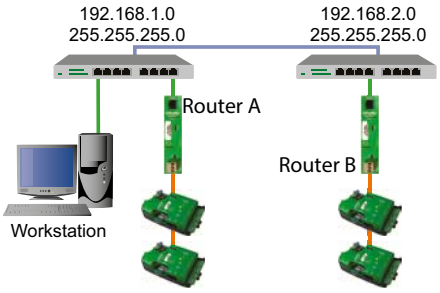
System plans are essential for installing, commissioning, and troubleshooting a BACnet internetwork. When planning an internetwork, the BACnet system engineer and the IT department contribute the following information to the system plans.

- BACnet network and port numbers are part of a BACnet router configuration and are assigned by the system engineer.
- Device instance numbers are part of a BACnet device and are also assigned by the system engineer.
- IP addresses, gateways, and subnetworks are part of IP router configuration and are assigned and managed by the IT department.

While there are many possibilities for using BBMDs, the following three scenarios focus on common BACnet solutions.

Scenario 1: Simple networks

The network in Figure 1 consists of two subnetworks, each with a BACnet router that includes a BBMD. In addition, a workstation is connected to subnetwork 192.168.1.0 as a BACnet IP device. By using the BBMDs that are embedded in the BACnet routers, the BACnet devices on both IT subnetworks are joined with a single BACnet network, in this scenario Network 1 using UDP Port 47808.



© KMC Controls

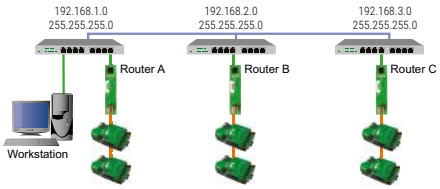
Figure 1: Internetwork with two subnetworks

Without the BBMDs, a BACnet broadcast message sent from the workstation is blocked by the IP router at 192.168.1.0 and cannot reach the devices connected to Router B. However, the BBMD in Router A forwards the broadcast message to the BBMD in Router B. The message is then rebroadcast to the devices on subnetwork 192.168.2.0. When devices on 192.168.2.0 respond with their own broadcast messages, the process is reversed.

Workstation IP: As assigned by DNS or static Device Instance: 10 IP: Enabled Network: 1 UDP Port: 47808	BACnet Router A IP: 192.168.1.10 Device Instance: 1 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 (self) 192.168.2.10	BACnet Router B IP: 192.168.2.10 Device Instance: 2 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 192.168.2.10 (self)

Scenario 2: Adding subnetworks

Scenario 2 is similar to Scenario 1 but includes a third IT subnetwork. Adding a subnetwork to the internetwork requires adding a third BBMD. Note that each BDT now includes three addresses, one for each BBMD.



© KMC Controls
Figure 2: Internetwork with three subnetworks

Workstation IP: As assigned by DNS or static Device Instance: 10 IP: Enabled Network: 1 UDP Port: 47808	BACnet Router A IP: 192.168.1.10 Device Instance: 1 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 (self) 192.168.2.10 192.168.3.10	BACnet Router B IP: 192.168.2.10 Device Instance: 2 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 192.168.2.10 (self) 192.168.3.10	BACnet Router C IP: 192.168.3.10 Device Instance: 3 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 192.168.2.10 192.168.3.10 (self)

Scenario 3: Connecting across the Internet

Using the Internet to form a Wide Area Network usually involves crossing a Network Address Translation and Port Address Translation (NAT/PAT) router. To cross a NAT/PAT router, add a second BBMD to one subnetwork on each side of the NAT/PAT router. Configure one BBMD with an IP address for the LAN and configure the other BBMD with a public IP address to connect through the Internet. In Figure 3, the second BBMD in Routers B and C form the public part of the BACnet internetwork on Network 2 and UDP Port 47809.

Connecting across a NAT/PAT router follows the same rules as internal BBMDs plus the following items.

- Static, public IP addresses are required for the BBMDs. These addresses, in addition to the local static IP addresses, are provided by the IT department.
- The network port for the BBMD connecting to the Internet, in this scenario UDP Port 47809, must be opened in the IT firewall.
- Do not mix public and private IP addresses in the same BBMD.
- Do not use the public network for devices with internal IP addresses.

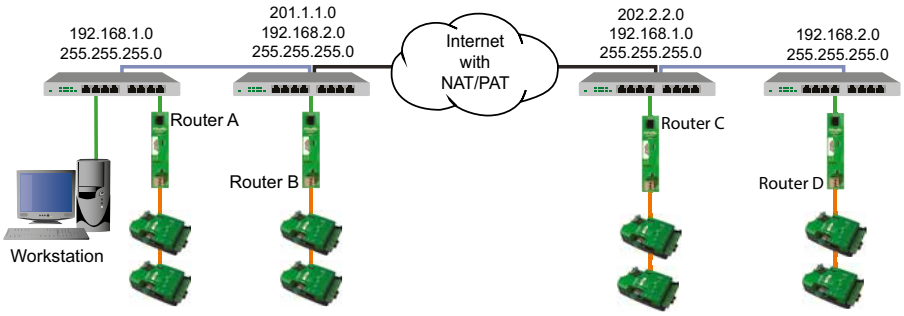


Figure 3: Connecting across the Internet

© KMC Controls

BACnet Router A IP: 192.168.1.10 Device Instance: 1 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 (self) 192.168.2.10	BACnet Router B Local IP: 192.168.2.10 Device Instance: 2 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 192.168.2.10 (self) BBMD 2: Enabled Network: 2 UDP Port: 47809 Public IP: 201.1.1.1 BDT 201.1.1.1(self) 202.2.2.2	BACnet Router C Local IP: 192.168.1.10 Device Instance: 3 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 (self) 192.168.2.10 BBMD 2: Enabled Network: 2 UDP Port: 47809 Public IP: 202.2.2.2 BDT 201.1.1.1 202.2.2.2 (self)	BACnet Router D IP: 192.168.2.10 Device Instance: 4 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 192.168.2.10 (self)

Scenario 4: Foreign Device registration to a BBMD

Use Foreign Device registration to temporarily connect devices, such as a technician's BACnet service tool, to a BBMD without adding the device address to the existing BDTs. The Foreign Device needs only the address of one BBMD, the BACnet network number, and the port number assigned to the BBMD. By configuring the Foreign Devices using the following guidelines, it can then join the BACnet internetwork from anywhere on the LAN.

- The BBMD must be enabled to accept Foreign Device registration.
- The Foreign Device can be configured with the internal IP address of any BBMD that is on the same LAN as the Foreign Device.
- The Time To Live setting automatically disconnects the Foreign Device after inactivity. The length of time is a local policy.
- The Foreign Device can use the IP address assigned by a Domain Name Server (DNS) as it is connected to a subnetwork.

Figure 4 is a typical connection for a BACnet workstation running on a laptop as a Foreign Device. The subnetwork 192.168.3.0 is not part of the BACnet internetwork and does not have a BBMD or router. However, the temporary workstation has registered as a Foreign Device and will join the internetwork as if it were connected to one of the subnetworks. Also, the laptop can be connected to either of the two subnetworks without changing settings and still join the BACnet system. The disadvantage to using Foreign Device instead of a BBMD is that if the connection is lost, there is no means to automatically reconnect the Foreign Device.

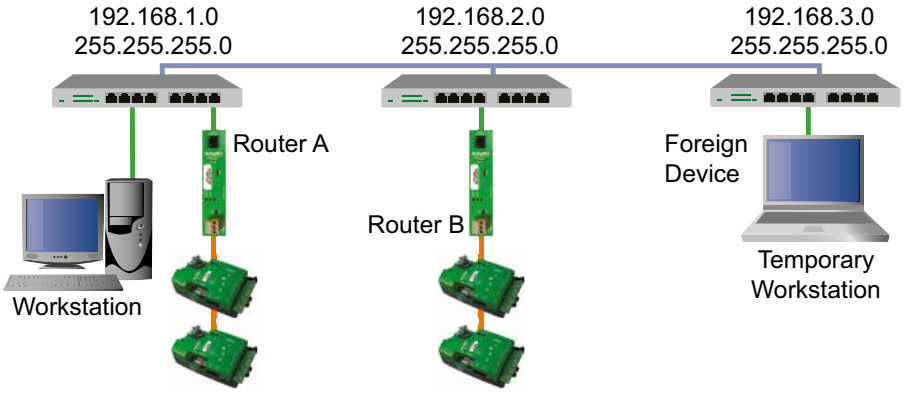


Figure 4: Foreign Device registration

BACnet Router A IP: 192.168.1.10 DI: 1 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 (self) 192.168.2.10 Accept Foreign Device Service: Enabled	BACnet Router B IP: 192.168.2.10 DI: 2 BBMD: Enabled Network: 1 UDP Port: 47808 BDT 192.168.1.10 192.168.2.10 (self)	Temporary Workstation Foreign Device IP: As assigned by DNS DI: 20 Foreign Device: Enabled BBMD: 192.168.1.10 Network: 1 UDP Port: 47808 Time To Live: 1800 seconds

Other solutions

Using BBMDs is not the only solution for crossing IT subnetwork boundaries. Packet-Assembler-Disassembler routing (PAD) is an established method but, because it chains one PAD router to another, it is vulnerable to single-point network failures. Virtual Private Networks (VPNs) are an alternative for connecting across the Internet or a NAT/PAT router. A VPN securely joins the two sides of a BACnet internetwork as if they were part of the same LAN. VPNs are provided as hardware, software, or a combination solution and require coordination with the local IT department.

A new, recently approved method is BACnet Secure Connect, or BACnet/SC, that will replace BBMDs with secure hubs. In addition, BACnet/SC devices, when used with the secure hubs, will provide BACnet internetwork security beyond the network security provided by the IT department.

Conclusion

Using an existing LAN as the infrastructure for a BACnet internetwork has the advantage that network upkeep and security does not have to be maintained by the BACnet provider. It does, however, add some complexity that cannot be ignored. By working with the IT department and understanding both IT and BACnet networking requirements, a successful and dependable internetwork can be operated, commissioned, and maintained.

ABOUT THE AUTHOR

David T. Menges is a senior technical writer at KMC Controls, Inc. For the past 17 years he has developed content for their BACnet routers, BACnet networking, and software help systems for TotalControl and KMC Connect.

David T. Menges
Senior Technical Writer | KMC Controls
dmenges@kmccontrols.com | www.kmccontrols.com

Safely Navigating the Age of Cloud Connectivity

Do you manufacture connected equipment?

If you said yes, according to Gartner's market forecast, you'll be contributing to the 20.4 billion connected devices in the Internet of Things (IoT) market. You, as a manufacturer, have made the leap to a more connected future.

And if you said no, then there's a pretty high chance you will be very soon — consumers are expecting the same connected experience from their professional environments as their personal environments.

It's no secret in 2020 that connected equipment, or IoT-enabled devices in commercial buildings, unlock potential within businesses on both sides of the selling equation. Suppliers benefit from increased device insight, access to operational data, the ability to identify product optimizations, and the potential to generate new revenue streams. Users typically enjoy the ease of maintaining a connected ecosystem, operational cost reductions due to efficiency gains, and remote equipment monitoring. On the surface, it's a true win-win scenario.

But it's also no secret in 2020 that the internet isn't getting any safer.

Business potential is not the only thing IoT-enabled devices unlock; they also frequently "unlock" confidential user data, cloud-stored documents, and building access.

Don't think it could happen to you?

Let's rewind to 2013 and take a closer look at the Target Corporation data breach. According to sources close to the investigation, the breach started with the HVAC service provider Target contracted nationwide. Hackers were able to steal Target network credentials and move laterally across the Target network until they infiltrated the point-of-sale (POS) system. More than 110 million consumers lost their personal data, and Target has paid upwards of $300 million in total damages.

Jumping forward to more recent news cycles, the city of Baltimore's "city systems" were held ransom May 2019; student and staff data from two Long Island school districts were stolen by hackers during the 2019 summer break; and Tillamook County in Oregon is currently in the midst of their own systems attack.

In today's sophisticated cyber landscape, it is no longer good enough for customers to erect a virtual fence around their on-premise network – or simply use IoT as a substitute for a Building Automation System (BAS). Not only are end-users accessing equipment data from several different networks and devices, but the number of internet access points within buildings is increasing. A new approach to security must be considered – one that encourages precautions implemented at every access point.

So, how can you safely navigate the age of the cloud-connected?

It truly depends on your business needs. Even though there is no one-size-fits-all answer to this question, there are a few strategies you can evaluate as you continue to explore ways to make your equipment secure.

Security at the network level: Regularly evaluate your firewall and network security

It goes without saying, but please make sure your IT department is regularly evaluating your own firewall and network security conditions. The Target data breach began when one of the HVAC service provider's associates opened a malicious email attachment. In this case, $300 million in damages could have been avoided by implementing additional IT precautions and network security.

The bottom line: all preventive measures you take to ensure the equipment you manufacture is secure provides immense customer value, but if your own network is vulnerable, you're leaving your customers vulnerable as well.

Security at the BAS level: Consider adopting BACnet Secure Connect (BACnet/SC)

Although BACnet/SC is in its infancy, the timing of its release couldn't be more impeccable. Growing user awareness and concern for privacy and security will likely lead to quick and swift adoption of BACnet/SC among device manufacturers and BAS Managers.

In addition to the multilayered BAS security recommendations made by ASHRAE member Levi Tully, in the previous issue of the BACnet International Journal, adopting BACnet/SC further supports and protects your equipment and your customers' BAS. Its built-in security features eliminate the need for extra VPNs; it provides an IT-friendly way for devices to protect themselves; and it utilizes Transport Layer Security (TLS) and Private Key Infrastructure (PKI), allowing you to make very secure connections to the internet.

Furthermore, your ability to match BACnet/SC demand from the field will communicate to your customer base that you take their security seriously. This in turn will provide you with a unique competitive edge – at least until the rest of your industry catches up with you.

For more information on BACnet/SC, please go to www.BACnetInternational.org.

Security at the device level: Partner with a cloud-connectivity gateway provider that has "baked" security into their hardware.

If you're at the stage in your product roadmap when adding cloud-connectivity makes sense, consider outsourcing to a third-party cloud-connectivity gateway provider. This common strategy allows manufacturers to accelerate their go-to-market timeline in a cost-effective way while keeping their engineering department focused on other R&D priorities.

When choosing a cloud-connectivity partner, make sure that…

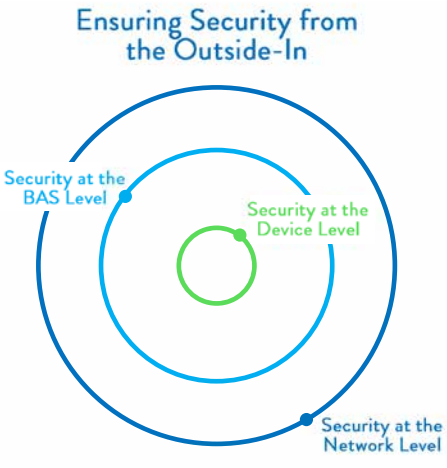
1. Their engineering team has performed thorough penetration testing and would be happy to provide you with the certificate and/or report to prove it.
2. The hardware is compliant with CA Senate Bill No. 327 and its national counterparts which require all IoT device manufacturers to equip devices with reasonable security features.
3. The product security features are capable of growing with you – meaning they can be ramped up as your customer requirements fluctuate over time.

It would be a bonus if the gateway could provide BACnet/SC support through a simple software update when the time comes as well.

It's not ludicrous to think that hackers could gain access to on-premise networks through your IoT-enabled equipment. Whether your equipment has a native IoT connectivity solution or you partner with a third-party connectivity provider, you and your customers are at risk.

You know how the saying goes; **Rome wasn't built in a day**. And, unfortunately neither will your new "Outside-In" IoT security plan. Taking the time to consider all of your options and available security partners and methods will be crucial in creating a sustainable solution for your IoT security needs.

Don't be the next cybersecurity story in the news – make sure you and your customers are protected.



Cyber-security in the cloud-connected age must be approached from a multi-layered, concentric perspective ensuring security from the outside in.

© Theron

Richard Theron
Product Manager FieldServer | MSA Safety
Richard.Theron@msasafety.com | www.msasafety.com
Lindsey Allen, Co-author

MSA The Safety Company

ABOUT THE AUTHOR

Richard Theron is the Product Line Manager for FieldServer and Cloud at MSA Safety, where he works intimately with companies in the building automation, industrial automation, energy management and life safety markets to understand and build connectivity products and cloud solutions.

BACnet – the Backbone for Smart Buildings

The buzz word "**IoT**" has been around the IT & Engineering world the past 7 to 10+ years. And it is gaining strong momentum day by day with the presence of major players' (Microsoft Azure, Google Cloud, IBM Watson, Amazon AWS, Alibaba Cloud etc.) huge investments and continuous technology & product releases.

IoT already penetrated many sectors like the Online Retail Industry (where the smartphone you are using is an IoT device), Financial, Medical & Investment (where data analysis is conducted on the data from different & discrete sources in order to predict & suggest investment and trading), Energy Utility Trading (where IoT is providing dynamic pricing for selling & buying), Covid19 Pandemic (IoT based sensors are used to track the human body temperature, adherence to covid19 protocols etc.) and many other sectors as well.

So, what's the role that IoT is going to play in the building space? The building is a physical entity where we human beings spend most of our time. On an average day we all spend approximately 18 to 20 hours inside buildings, which include residential, commercial, office buildings, restaurants, hotels etc.[1]

In most of these buildings, in order to provide comfort for the occupants, the indoor space is maintained with required temperature, humidity, air quality, air flow, acoustics and lighting level. These conditions are met with the help of much mechanical & electrical equipment running behind the scenes, which mostly fall into HVAC (Heating, Ventilation & Air Conditioning) System. And all of these consume a considerable amount of energy for their operation. That's why several studies done by prominent organizations have found that buildings consume more than 40% of total energy produced[2].

Apart from this there are multiple safety, security and smart services in place in and around the building for safeguarding the occupant & building assets and to cater the sustainability goals of the organization:

- Fire Alarm & Fire Suppression
- Physical Security
- Access Control
- Lighting Control
- Public Address
- Digital Signage
- Parking Management
- Indoor Space Management
- Smart Metering
- Indoor & Outdoor Navigation
- Elevators & Escalators
- Indoor & Outdoor Landscaping
- Water treatment plants
- Solar/PV Panels
- EV charging stations

The above-mentioned systems consume less energy compared to the HVAC system, but at the same time the up-time and proper operation of these systems are highly critical.

Building Automation Industry Evolvement & Latest Trends

Let's try to understand the background of a Building Management System and how it evolved from a standalone system to an enterprise or semi-cloud-based offering by going back to 2008 when I started my career in the HVAC and BMS industry.

I still remember when we used to provide two ink-jet printers with paper rolls for a six-month period for printing alarms and events with a desktop to the BMS operator. Technology has evolved greatly since then, as has the BMS and HVAC industry. Now, the Facility Manager can see the near real-time facility equipment heath and performance data in a mobile app or via any standard browser without any physical location constraints.

The BMS PC or Server used to be isolated, meaning not connected to any network other than the supervisory controller. The USB port of the BMS PC was kept disabled in order to protect the BMS system from any malware attack.

The field controllers, like AHU controllers and VAV controllers, were not equipped with any web interface, and if you needed to reprogram/troubleshoot the controller, which was situated inside a false ceiling, you had to climb up a ladder and spend a few hours locating the controller.

These are just a few of the things that occurred in the BMS industry. Things have definitely changed over time. Now the client is requesting a lot of functionalities which were previously never thought to be incorporated into a building automation system, such as:

- Persona based dynamic responsive dashboards
- Enterprise visibility of multiple buildings' performance
- Command center for centralized operation of multiple building services
- KPIs visualization & tracking
- Mobile notifications
- Facility Management services
- Work order creation and tracking
- Financials analysis
- AFDD & advanced data analytics
- Building Integration Management services
- Digital twin of the building
- Remote commissioning & configuration
- Energy management with advanced metering, Demand management etc.
- Automated reports for LEED, wellness certification, ENERGY STAR, etc.
- Voice based assistance (Alexa, Siri, Google assistant etc.) & Wearable devices

The requests are never ending, and it's challenging the building automation industry to focus on improvements in features and technology.

But at the same time this requirement does not force the building automation industry to adapt/transform to a complete IoT/Cloud based solution.

The current building automation industry is very strong and reliable and the main reason for this is that it **runs locally.** This means the whole automation system, which is comprised of sensors, actuators, meters etc., is connected to the equipment at one end and the DDC/IO modules are at the other end - equipment specific controllers where the equipment operation logic sequence/program runs and the central controllers, like chiller plant controllers, network controllers, the BMS server, and data storing historian DBs, all are physically located in the same building on different floors.

This type of methodology or architecture is well refined and optimized and is perfectly suitable for running the building smoothly without any down time or data latency, and without any delay in command and control triggers with all safety measures in place.

So, completely replacing this existing building automation architecture to match with an IoT

solution is not the right path to be followed during this era of IoT/Cloud/Industry 4.0 revolution.

Rather, the building automation industry should take a path which is constructive and coherent, where whatever cloud services can be accommodated without demolishing the current architecture, also create the features asked for by the client, for example incorporating BIM drawings of equipment and floors in the BMS UI instead of using standard graphics library images, persona based dashboarding, enterprise visibility, advanced fault diagnostics and more. Another example is accommodating power BI tools to create dashboards & reports, etc.

Choosing a Suitable Cloud Platform & its Future Flexibility

Another major concern in adopting the IoT/Cloud solution in building automation is Upper Layer Vendor Lock. When we talk about a cloud solution where millions of data from the building can be accommodated and analyzed, that data still falls into a particular vendor system that is providing the cloud infrastructure or cloud services.

Maybe this can be defended by saying that the standard IoT protocols like MQTT, AMQP that are used for data management and JSON, Python, R, etc. languages are used to create programs with the data feeds for further analytics. But this still does not solve the vendor lock problem completely. If the client, after a few months or years, wants to change the cloud vendor or wants to incorporate a few services from another cloud, there is a significant development/configuration effort associated. This means you must install and configure the new IoT gateway/API services, then all other associated activities need to be performed. Just imagine how costly it would be and the huge engineering work associated with it. Even if you deal with the same cloud infrastructure, but the data end points are from different vendors, then there is also the possibility that inherent JSON data formats will be different and this will also necessitate the data normalization effort.

Another concern is validating the field sensor data authenticity and eliminating the chances of data manipulation. This functionality check is still not addressed by IoT solutions when handling the conventional BMS controllers and field sensors, and these checks are only available with very limited IoT ready devices/sensors.

This kind of scenario existed in the building automation industry where vendor locking was a big issue with the presence of legacy protocols, multiple protocols and tools. This created many problems and restricted the client to the same OEM/vendor providing the building automation services.

The Role BACnet Organizations Played in Data Standardization

BACnet industry associations, like BACnet International, played an important and valuable role by educating and nursing the different OEMs to follow the BACnet protocol and get BTL certification for their BACnet controllers and devices. This led the Building Automation industry to have many BACnet protocol-based controllers and devices. Now you cannot find a single building automation company without a BACnet based solution or BACnet gateway, which makes the space for creating a unified building automation solution.

This has not happened in one day or in a short duration. This is a result of efforts made by the BACnet community for years, and it has created the flexibility in choosing controllers, BMS software, VAV actuators, FCU controllers, sensors, etc. from different OEMs with all of them working together as a complete solution with the power of the BACnet protocol and BACnet standards.

So, this vendor flexibility is already established in the Building Automation industry, but vendor locking is still persistent in cloud solutions.

The contribution of the BACnet community to the building automation industry, together with the ASHRAE SSPC 135 committee, is not limited to the above factors but extends to many paths.

Their contributions to the Building Automation industry include;

- Upgrading the BACnet protocol into an IoT ready protocol
- Standardizing the point objects
- Ensuring PIC statements for BACnet controllers
- Easy discovery of device & points
- BBMD for complex network connectivity
- Providing MSTP network data communication optimization
- BACnet testing lab facilities
- Providing domain & network level training to new BMS professionals
- Periodic enhancement & recommendations for BACnet protocol security
- Encouraging IP based BACnet controllers with Web servers

All these continuous improvements and technology enhancements are reflected in multiple verticals of the Building Automation industry:

- Network communication
- Network security
- Product development
- Semantic data modeling
- Edge computing functionality
- Enterprise connectivity readiness
- Improved accessibility
- Enhanced UI & UX
- Less tool dependency

With these positive waves in place, when we check the current operating condition of these systems, we still find that even though BACnet is the major protocol followed, there are OEMs that provide building automation solutions with the help of field sensors, controllers, and management software with multiple protocols, other than BACnet. This restricts the ability to share data within the system or to a unified management platform.

The different manufacturers (where each of them is a pioneer in one or multiple systems mentioned above) follow multiple protocols for data communication, like BACnet, Modbus, LonWorks, N2, ARCNET, M-bus, H-Link, CCN, CPP, KNX, ONVIF, Wiegand and many more. Each of these protocols inhibits communication with the others and that's one of the bottlenecks for having a Unified Building Management Platform. This can be resolved through the help of BACnet gateways.

One of the less discussed topics, which needs to be addressed when implementing a unified management platform, is the presence of legacy systems. The controllers, field devices which have been in place in many buildings for 20 or 30 years and are still working fine, are really a challenge for system integrators. The customer will not agree to completely replace those systems since they are working fine, so how will you convince them to change them out since they are not open protocol systems and they don't have advanced computing functionalities?

This issue can be resolved with the support of the manufacturers of those legacy solutions. Luckily most of the major players are thinking along those same lines and have started providing enhancement /replacement kits for those legacy systems. It's now up to the building owners to accept and implement the new technology.

Cloud-based Analytical Solutions from Domain Players

Recently in the Building Data Management Market we see that major Building Controls and

Building Equipment Manufacturers have focused on Building Data Analytics and have released products which include IoT Edge Device and Cloud Hosted Applications, On-Premise Applications, Add-on Services to existing BMS, etc. Examples include:

- Johnson Controls OpenBlue
- Honeywell Connected Services
- Schneider Electric EcoStruxure
- Siemens Mindsphere
- UTC EcoEnergy CORTIX
- ICONICS Gensis64/IoTWorX
- Samsung SDS Brightics
- GE Predix
- SkyFoundry SkySpark
- BuildingIQ
- CopperTree Analytics

They are also taking care of the normal operation of the building automation functionalities during the absence or failure of cloud services. This is a good sign for the smooth implementation of Cloud/IoT technologies in the building automation industry.

Advantages of Domain OEMs Developed Cloud Solutions

The Building Automation OEMs' cloud hosted products also take care of the commercial aspects involved with a cloud-based solution for the building automation domain. The typical cloud-based solution works on a subscription model - to be precise, a data subscription based on endpoints created in the cloud instance and the data polling frequency. If we go deeper there are more factors, like the cloud services consumed and many more, but let's restrict that in this discussion and take a practical example.

Creating endpoints for zone temperature in the cloud platform: Let's assume that there are 50 zone temperatures per floor for a building with 10 floors. So, the total endpoints will be 500. But is it really necessary to push all these zone temperature data points into the cloud, or just compute the average zone temperature per floor or per zone and push those data feeds only to the cloud, thereby limiting the cloud endpoints to 10 or 20 instead of 500? Because the individual zone temperatures are mainly consumed for VAV operation and the average zone temperature can be consumed for the AHU operation, it is not clear that from the cloud aspect there is an exact need for individual zone temperature availability. So, unless or until a specific use case exists, we can optimize the endpoints that are communicated to the cloud and minimize the cost involved.

Access control system card reader swipe data in order to calculate the amount of time spent by a person/employee inside a building for a day: In this case the existing controller/server can also compute this locally rather than pushing each event from the card reader to the cloud platform. So, this helps to optimize the data load and thereby limit the cost involved.

There are many other practical examples which necessitate the connectivity with a cloud platform.

Standardizing the missing data coming in from energy meter data feeds, where the cloud services can fix the missing data by running the logic blocks with the historical data and populate the dummy data in the missing slots.

Enterprise level comparison of key building parameters fed from different buildings located geographically at different time zones and climate zones. Here the cloud components can standardize the data feeds according to the building location and create logical insights accordingly.

End to End Cloud-based Solutions Use Cases

A leased building space for a fast food chain restaurant or banking company's branch location: The better solution would be to install wireless sensors that are self-powered, like EnOcean based sensors, and push the data to the cloud for all other activities like analytics, visualization, reporting, notifications, etc. This would make life easy, because there would be little work involved to relocate the solution into another space/place when the client ends the contract with that leased property.

These scenarios are self-explanatory and reiterate that conventional building automation and cloud based digital services provide value according to the situational demand.

The cloud service layer is a perfect **add-on** which can provide better features to the existing Building Automation System in many aspects and will be an essential part or nervous system of the building automation industry in the coming years.

Semantic Data Modeling and Value Addition by Embedding Tags

In the meantime, there is another major effort already underway standardizing the building data which will improve the quality of data and increase outcomes from the analysis done on that data. ASHRAE is playing a major role in framing and implementing a standard for building data with tags and relationships.

- Semantic Tags for Building Data
- Project Haystack
- Brick Schema
- BACnet/SC

The BACnet committee recently introduced an important enhancement in their protocol security which is BACnet/SC or BACnet Secure Connect. This is going to be a major milestone in uplifting the Building Automation industry into an Enterprise/IoT/Cloud based Industry. The BACnet community has already asked the OEMs that manufacture BACnet controllers, devices and sensors to incorporate this feature into their devices. They are also arranging training sessions to educate the respective stakeholders.

Now, the BAS industry is waiting for the major cloud solution providers to begin to accept the BACnet data directly into their cloud infrastructure. For example, the Microsoft Azure IoT hub does not accept BACnet data directly. Instead they ask the vendor to provide the data in MQTT, AMQP or HTTPS.

Other cloud providers are also following the same framework, which is restricting the entry of BACnet data into the cloud platform. This, in turn, creates a lot of rework and other related tasks, like finding the right gateway (hardware + software), finding the right professional to configure the gateway, and making sure the data reaches the cloud platform properly.

This also creates many duplications of work like creating the data tags, asset hierarchy, space relation, and data point parent/child/cross relations with other data points. Most of these things work perfectly in a traditional building automation system with a BMS server and controllers set up. But when they need to be brought into a cloud/enterprise platform most of these tasks need to be reworked. Another issue is the cloud industry asks providers to use JSON format to standardize the data points which is relatively less familiar among building automation industry professionals.

This way of connectivity will work for direct IoT sensors which are relatively new in the industry and provide substantial security risks of their own. Such devices, like LoRa based sensors and BLE based sensors, do not utilize middleware like aggregator/field controllers, and the gateway is sending the data directly to cloud. The OEMs of these sensors also support cloud API connectivity/cloud ready gateways. This presents the user

with additional cloud connections to secure and monitor.

Existing Building Automation System manufacturers, along with the building automation industry, are following a complex framework which is steady as well.

The BACnet community is rapidly defining compliance for BTL tested controllers & servers which will transform them to BACnet/SC based data sharing. At the same time, cloud approved devices which can directly share the data into cloud infrastructure for enterprise level services (like AI, ML based analytics, visualization, consumption and storage, etc.) may also fit into the architecture.

Road Ahead Looks Flexible, Scalable & Hybrid

These all indicate that the future is very clear for IoT in Smart Buildings. It is clear that IoT technology will be incorporated in buildings but, unlike consumer IoT, the solutions will have to be interoperable and flexible, and at the same time building oriented. That is why people refer to the use of IoT in buildings as Building IoT, or BIot. With a matured architecture, both the building system and IoT are going to work hand-in-hand to help to create a Sustainable Eco System

1. https://www.deseret.com/2018/5/17/20645140/indoor-generation-here-s-how-much-time-we-spend-indoors

2. https://openei.org/doe-opendata/dataset/6aaf0248-bc4e-4a33-9735-2babe4aef2a5/resource/3edf59d2-32be-458b-bd4c-796b3e14bc65/download/2011bedb.pdf

© Krishnamurthy

Anish Krishnamurthy
Senior Consultant (IoT for Buildings) | Infosys Limited
anishpk123@gmail.com |
www.infosys.com/services/engineering-services.html
Connect: www.linkedin.com/in/anish-pk-57583234/

Infosys® Navigate your next

ABOUT THE AUTHOR

Anish Krishnamurthy is a Building Automation & Energy Management professional with 12 years of experience in project management, techno commercial consulting, system design, site commissioning, energy audits, ELV system integration, PLC-SCADA & automated energy distribution. He worked with various multinational companies and clients from the Building Automation, Energy and ICT domains in multiple countries, including India, UAE, KSA, USA & Chile.

Digital Twin of Building Automation with BACnet

Garage area of the Birago Barracks in Melk, Lower Austria. © Österreichisches Bundesheer

"User-oriented building technology" is the title of a series of lectures that was announced with the flyer for the Building Services (TGA) congress on April 2 and 3, 2020 in Berlin. Of course, the technology has to be based on the user and the customer is king! Really?

On the one hand, the user of building technology systems is not always the same as the person who procures them, and on the other hand, not all customers see through the complexity of modern technology, which manufacturers and the market advertise effectively. Purchased devices can often do much more than one actually needs. And, honestly, do you know all the functions and programs of your washing machine and do you actually need and use them? Wouldn't one with less refinement and easier operation have met your needs? It would probably have been cheaper to buy and operate.

The interests of the manufacturers of systems and components as well as the trade that sells them, the planners and the system integrators who plan and implement them on behalf of the customer, and those who should ultimately use and operate the technology offered to them, lead - wanted or unwanted - to a compromise that is usually not an advantage for the operator.

If you take into account that the standardized requirements for the BACnet interface are in revision 22 (EN ISO 16484-5) and the "protocol-neutral" rules for BACS planning, hardware and implementation since 1995/2004 (VDI 3814 / EN ISO 16484-1, -3) exist unchanged in revision 1, it becomes clear that the overall solution cannot meet the current requirements. The connection from the BACS Functions to the information, i.e., to the BACnet properties, is missing.

In this area of conflict of divergent interests, it is therefore important that the customer formulates his requirements for building technology and its automation precisely and demands that they be fulfilled - given the feasibility. Not all planners, manufacturers and integrators provide that.Some follow philosophies, market strategies and proprietary product lines that run counter to the goals of the customer.

Automation components für heating circuit groups.

The most important requirements relate to the information we need from the automation system to control the mechanical systems. In the BACnet jargon, information that we need to reduce energy expenditure or to adapt the convenience of use to the needs is in the "Properties" that are contained in the BACnet objects.

Interoperable solutions with BACnet for landlords with a large real estate portfolio

Companies with a larger real estate portfolio must demand interoperable multi-vendor solutions in order to be able to use economies of scale and to reduce the dependency on integrators and BACnet device manufacturers.

Integrators or manufacturers who know that the client is dependent on them will use this position sooner or later. Only by means of simple and standardized solutions can the human resource dilemma at the real estate locations be countered on the basis of clear corporate guidelines based on the global BACS standards.

BACnet is the data communication protocol that best supports the interoperability of building automation components. This has prevailed internationally, but is interpreted and applied differently in practice, which often counteracts the hoped-for interoperability. All the more so if there are no concrete specifications on the part of the client or the planner. Then the systems are "optimized" by executing companies for the benefit of implementation or due to time pressure or to their own, often proprietary, company philosophy and not in terms of operation.

There are also numerous communication gaps in the implementation of building technology projects and their automation:

- organizational (client, planner, integrator, operator, user),
- technical (heating, air conditioning, ventilation, electrical engineering, building automation, information technology, security) and
- time (idea, specifications, planning, work planning, implementation, acceptance, operation).

And there exists currently no continuous, IT-conform process.

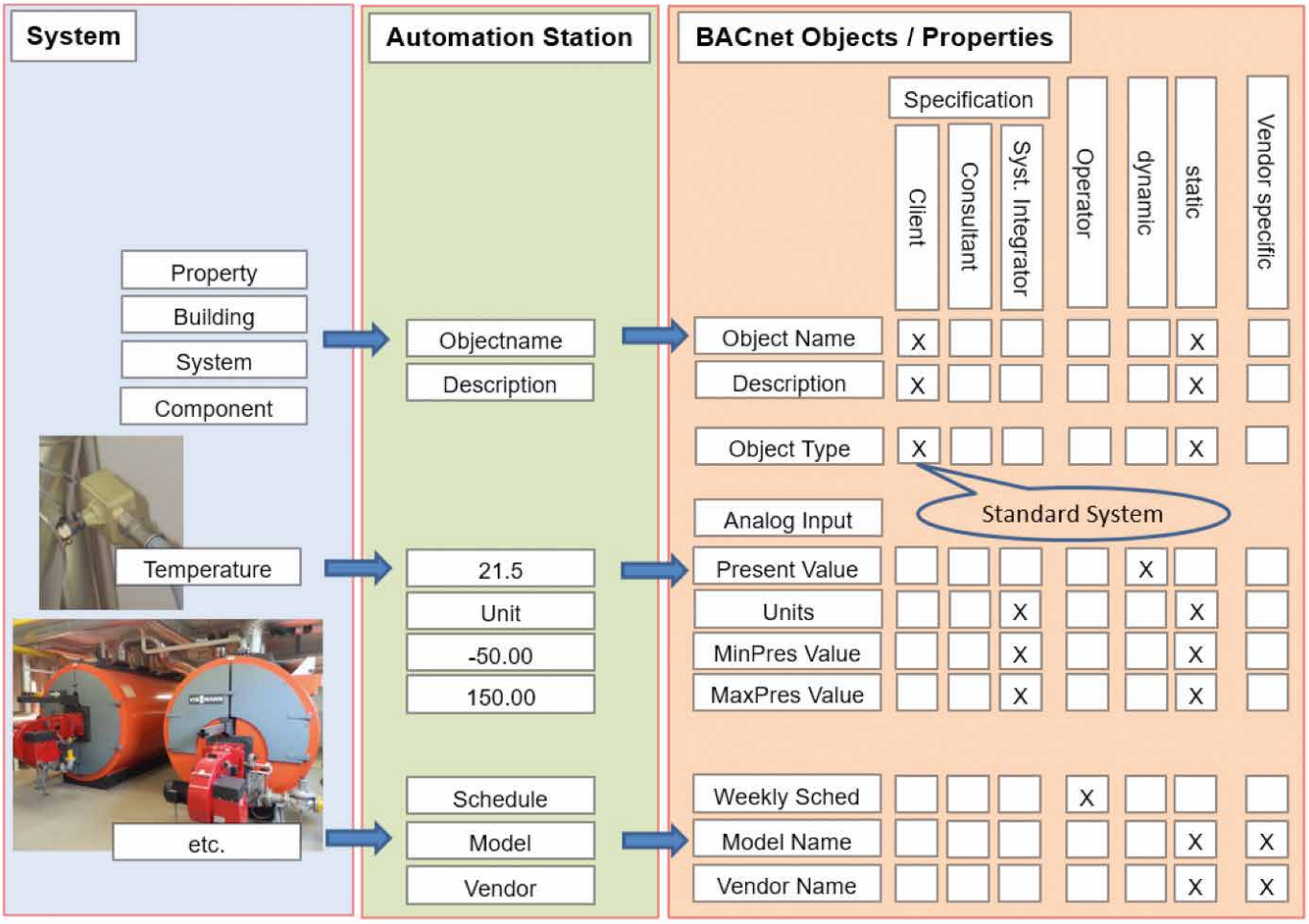
Simple, uniform standard systems and specifications

Uniform mechanical systems (e.g., heating circuit, domestic water heating) and components (e.g., aggregates as pumps or fans) offer planners and integrators the advantage of being able to use ready-made implementation templates, reduce the risk of reworking on the construction site, support automated quality management and lead to synergies and savings in acceptance and visualization, but especially in the operation of the systems.

For larger real estate portfolios, the client's goal must therefore be to implement simple, uniform and easy-to-operate solutions, i.e., standardized mechanical systems and components with unique IDs, descriptions and largely predefined functions. For this purpose, the BACnet objects and in particular their properties must be specified with all important information and proprietary BACnet objects and properties must be prohibited to ensure interoperability, knowing that this may limit the variety of solutions and providers. This reliably covers the requirements of a large number of real estates. Due to their special position, individual buildings will, however, require an individual solution.

The client's requirements, for example the content of the specification, usually include Definitions:

- of the network and its security regulations,
- the nature of the automation stations and the management and operating equipment,
- the addressing system of the data points or BACnet objects, the systems and components,



Derivation of the competence matrix

Book on the Digital Twin © CCI

- for message and information management,
- for planning and implementation documents,
- for visualization and type of image display and
- for general operator requirements, etc.

This content of specifications with the exception of the specifications for properties can be assumed to be generally known.

Less common - and in this sense new - are, however, the topics and guidelines outlined below, which are urgently recommended to owners with larger real estate portfolios.

Competence Matrix

In the competence matrix, all relevant BACnet properties (all information contained in the BACnet objects, such as the name, state condition, unit, limit values, parameters, etc.) of the BACnet objects currently approved in the client's specifications are listed in a spreadsheet with a short description of the respective property and its possible specification of the client. This is used to determine who has to fill in which settings or values (client, user, planner, manufacturer, integrator or the system itself).

Practice has proven the need for such clarification of responsibility for individual properties and their value content. In the absence of such a stipulation in the BACS standards, the owner and user are "surprised" by the various configuration settings depending on the manufacturer and integrator, which call into question the future interoperability of the components in the network.

Digital Twin of building automation with BACnet

In the case of the digital twin, the existing BACS Function List in accordance with EN ISO 16484-3 is expanded to the left by the client's defined standard systems and standard components and supplemented to the right with the BACnet properties and configuration settings of the implementation ("complete EDE table" – for engineering data exchange).

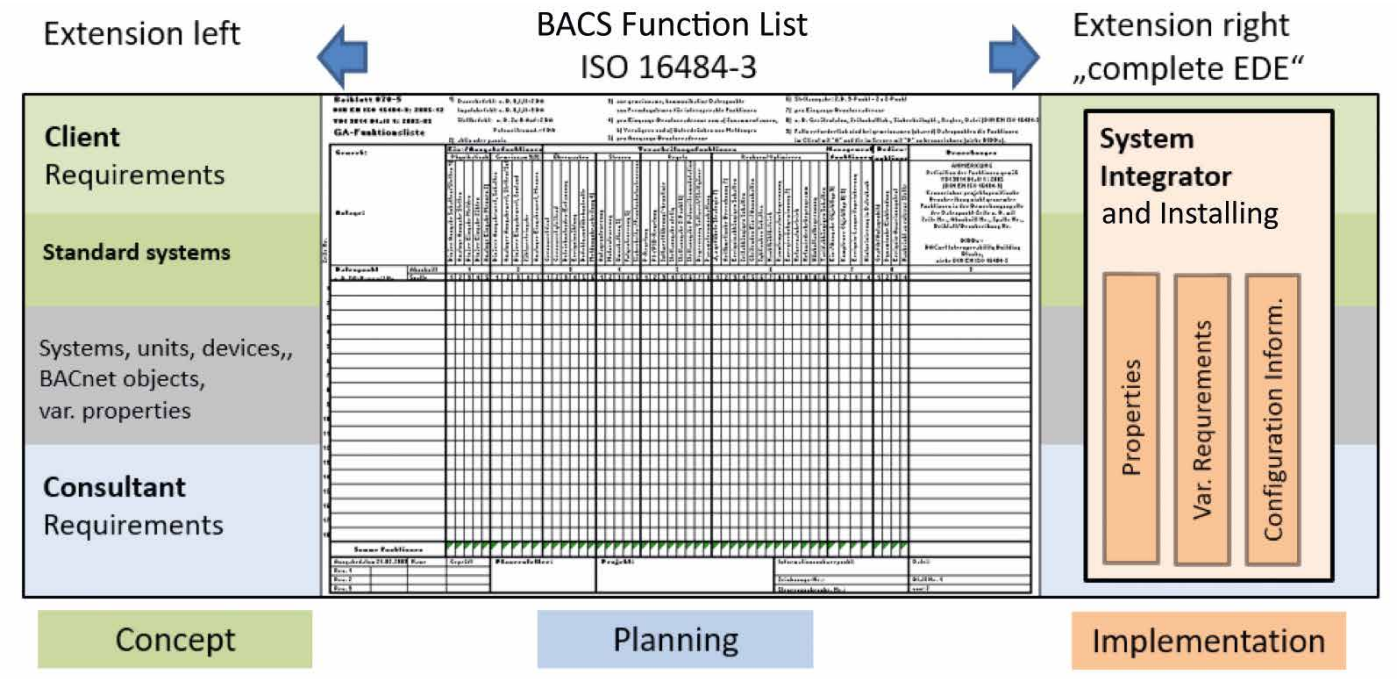
While the EDE table contains only a few BACnet properties as recommended by the BACnet Interest Group Europe (BIG-EU) and the Working Group for Mechanical and Electrical Engineering of State and Local Authorities (AMEV) in Germany, the "Complete EDE table" has to contain all BACnet objects, the properties together with the values and the configuration information used on the automation station.

In this way, an integrated process is supported in a simple manner and on the basis of a commonly used spreadsheet system, from the client's specifications through planning to engineering and operation of building automation and control systems.

In autumn 2019, the cci Dialog GmbH published the book "Digital twin of building automation with BACnet - Instructions for low-effort system integration" (ISBN 978-3-922420-66-8) written by Dipl.-Ing. Hans KRANZ and Hofrat Dr. Rupert FRITZENWALLNER.

BACnet implementation guide

In order to ensure the implementation of building technology projects and their automation in accordance with the client's specifications, an implementation guide including appointment allocation has been created in which the outputs of the respective project phase are specified and presented in the correct chronological order. Since usually several participants are involved in projects and the integrator for building automation at the end of the chain often only comes into



Digital Twin (BACS = GA) © Austrian Army

play as a subcontractor, the chronological representation of the outputs is essential in order to prevent lost effort.

If the documents required by the BACS standard, such as

- automation schematics,
- BACS-function fists,
- function descriptions,
- network concept, etc.

are not based on the actually implemented mechanical systems and are not documented in a current hydraulic diagram, there is a risk of "stranded costs" due to the mostly large number of participants.

Due to the complexity of the projects, a structured processing with uniform terminology is absolutely necessary.

BACnet test tools

Reworking is time and cost intensive, among other things through repeated re-checking and judging correct implementation as well as through a possibly multiple "uploading" of the data of an automation station to the management and operator unit. The quality control, i.e. the checking of the implementation in accordance with the specification, has to be carried out by the contractor and not the client, but in the end it will be indispensable for the client to check whether the contractual agreements have been implemented.

This check cannot be carried out economically manually, so a simple tool was created in which the client's requirements can be maintained and the automated check is supported with the help of the digital twin of building automation.

By the IT-supported check clear errors, such as incorrect addressing, ObjectNames, descriptions, notifications, NotifyTypes, and points to be clarified, will be transmitted to the integrator for correction.

It is clear that several thousand Excel lines cannot be checked manually, so tools must be made available to the technician on site that are easy to use and nevertheless enable checking the work of the integrator.

There are tools available on the market for reading out via the network the BACnet objects and content of the properties that are available and used on automation stations, also the settings made by the integrator - provided they have not been created "hidden".

Some tools also offer the option of comparing the client's or planner's specification with the actual implementation of the integrator and showing differences.

A large Austrian client therefore has developed a tool based on "BACeye" through Bernhard RAMROTH to be able to implement the task efficiently and effectively. This is an ideal tool for quality assurance.

Conclusion and outlook

Landlords with a larger real estate portfolio are well advised to require interoperable solutions with BACnet for GA projects and to specify their ideas in a specification and concrete guidelines for uniform and simple standard systems. Under no circumstances should these change the existing EN/ISO standards, but at most supplement them. Since this requires a high level of knowledge in the field of building technology and its automation, support from planners with sufficient BACS and BACnet know-how would be necessary, who should also be commissioned to monitor the implementation as part of the acceptance of projects

In addition to the client specifications on the topic of BACnet and BACS, a BACnet implementation guide and a BACnet test tool for the economical implementation of simple and uniform systems are essential, according to the author's experience.

The raw material of digitization is structured information, i.e. the BACnet properties.

Digitization offers the opportunity to overcome gaps in understanding between the building owner, planner and integrator and to map the process from planning to implementation and commissioning, to avoid redundancies and to implement the goals of building automation.

The structured information in the form of predefined BACnet properties is the basis for supporting the organizational goals by means of a management and operator unit (MOU), which in the future will have to have more energy management functions and artificial intelligence.

Only when the parameters for the quality of use can be adapted to a changed need with the available staff during the use phase of the building and, in addition to other goals, the energy expenditure can be reduced, does building automation create added value and benefit.

It should be clear to all experts that the building automation must support the goals of the owner, operator and user in the life cycle of the real estate and that the focus is not the device manufacturer's or the integrator's implementation process.

If the operation of a facility can be optimized through building automation, investors and users will be ready to bear the investment costs of a properly installed building automation system. It is undisputed that standards and interoperability are a mandatory prerequisite for tapping the added value of digitization.

ABOUT THE AUTHOR

Dipl.-Ing. Hans R. Kranz has been passionate about the building services industry for 59 years, has received numerous medals of honor from VDI, DIN, REHVA and the Automation Trends Hall of Fame. In 1983 he was the initiator for the development of the first BA com-munication protocol and in 1990 for the introduction of the standardized BA functions, as well as the project manager of the BACS world standard. He is the author of the first BACnet book in German, which is now available in the version BACnet building automation 1.19.

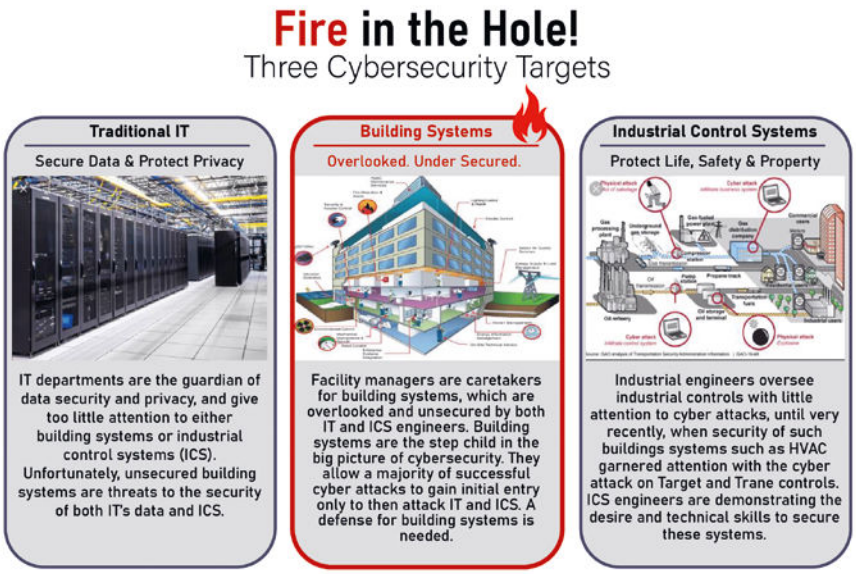
© Kranz

Hans R. Kranz
Dipl.-Ing. | HAK Ingenieurberatung
hans@kranz.com | HAKforst@kranz.com

© Fritzenwallner

Dr. Rupert Fritzenwallner
Head of Constr. Dep. | Bundesheer
r.fritzenwallner@hbv.gv.at | www.bmlv.at

Securing Building Systems in a BACnet/SC Environment: One Set of Devices at a Time



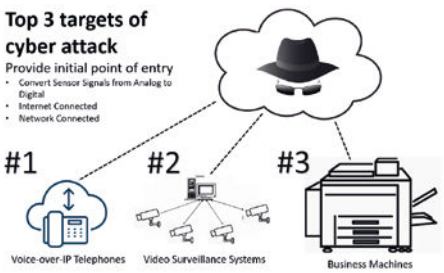
© Fortium Partners

Graphic #1. Cyber attacks strike Building IoT first. Following this initial point of entry, the attacker can either move to the IT system to disrupt, hold ransom, or steal data, or, move to building automation or industrial control systems to disrupt or threaten life, safety and physical destruction.

Just a few years ago, nobody expected the Harvard Business Review (HBR) to report research claiming that "building systems" are the targets of computer hackers around the world. Yet, in June of 2019, HBR reported that 60% of successful attacks on public corporations in 2017 gained their initial entry via building systems.

Then Microsoft followed with an independent report of its own in "IoT Signals" that the top 3 points of entry for attacks by nation states (think Korea, Russia, China) were achieved via:

- VoIP telephone systems
- Network video surveillance recorders (cameras were not in the top 3)
- Business machines (e.g. copiers, scanners, and other connected machines).



Graphic #2.

© Fortium Partners

It is worth noting that Microsoft referred to these points of attack without categorizing them as "building systems".

On top of all of this, we know that cyber attacks on sensors are well suited to injecting malicious code into the IT data stream by targeting analog-to-digital converters in front of and before the digital signal even reaches the IT infrastructure.

So, this tells us loud and clear:

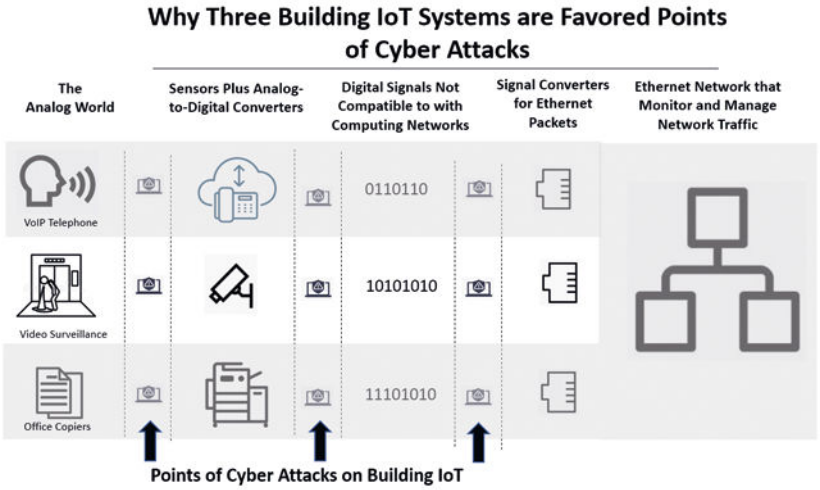
Nothing is secure unless the building systems are secure.

Having said that, what building systems? Speaking from my own perspective, I focus on:

- VoIP Telephones
- Video Surveillance
- Door Access Control System
- A/V Conference and Collaboration Systems
- Elevators, especially those with Destination Dispatch
- Lighting
- HVAC especially non-engineered systems
- Way Finding

In the right setting, I sometimes refer to these as the Junior Varsity of building systems. They are overlooked and seldom have good coaching, or in this case technical leadership.

The reality of the situation is that there is not a lot clarity in differentiating between building automation (BAS), building information (BIS), industrial controls (ICS), Building IoT (B-IoT), Industrial IoT (IIoT) and all of the other IoT, such as medical devices, smart speakers, etc. It is not that we do not understand what somebody means when they refer to one or the other. The problem for analytical types is that there



© Fortium Partners

are no clear demarcations for each type of IoT system. It is similar to politics and policies. What is the point at which Republicans who are socially moderate and financially conservative become moderate Democrats? There is no clarity at the margins, for politics or IoT systems.

For creating more clarity, let's identify some unique attributes of the particular set of building systems listed above. For example, these building systems are likely to:

- Be a control system for common building functions limited to communications, heating, lighting, physical access, security as well as safety
- Have a legacy that extends prior to the Internet (many have a legacy extending prior to local area networks
- Be connected to both the Internet and the corporate network
- Be identified as a low-voltage system by building architects
- Be installed during new construction by subcontractors to the electrical contractor
- Be installed and serviced in existing buildings by contractors or system integration companies under the direction of facility management
- Be capable of integrating with other B-IoT, but seldom is except for access control and video surveillance
- Be unequipped to interoperate with the IT department's network management tools and platforms

This is the group of systems that might be productively described as Building-IoT, or B-IoT. Since it is quite common that Facility Managers have primary responsibility for these systems, and much less so for many of the others, let's rely on B-IoT for the discussion and perhaps others.

Many of the B-IoT systems would benefit from integration with BACnet as would the operation and management of buildings. At this point in the history of BACnet and B-IoT, it may make as much sense for B-IoT to interoperate with BACnet as it does for it to interoperate with the IT department. Both sides could be argued persuasively. In either case, the BACnet community, and the BACnet/SC working group should be concerned about the lack of attention being paid to B-IoT and cybersecurity. The Harvard and Microsoft research referred at the outset of this article clearly describe a threat to any BACnet environment.

Thanks to the BACnet IT working group, significant progress is being made at the network security level for BACnet-connected systems, which to date have largely focused on HVAC, and perhaps lighting. The progress with BACnet/SC is foundational and the work group should be applauded. But network security is but one layer of defense, and as every security professional knows, effective security requires multiple layers of defense. There is no silver bullet available when considering security.

Without device-level security for B-IoT, BACnet/SC's network security is left wanting, as the sole layer of defense. Device-level security provides a second security layer which, in most cases, constitutes a commercially viable strategy for cybersecurity and B-IoT.

I propose that BACnet/SC promotional materials, related training, podcast programming, etc. address B-IoT and the integrity of security with the following:

1. Multiple Layers. Establish the goal of at least two layers of cybersecurity for B-IoT. People represent another layer and anti-phishing applications are coming to market and will supplement awareness training applications

2. Secure the Devices. Implement a program for having the suppliers of B-IoT assume responsibility for providing "device-level security." They are the people who actually know the ins and outs of those devices. Device-level security is an essential layer in the defense of B-IoT against cyber attack, including attacks on devices in the BACnet/SC ecosystem. The controls deployed at the device level should conform to the considerations identified in the NIST 8228 Internal Report and can use the Secure Controls Framework for further clarification when necessary.

3. Secure Across Devices. This is where BACnet/SC shines. It can provide network security of the connected systems and devices that interoperate with BACnet.

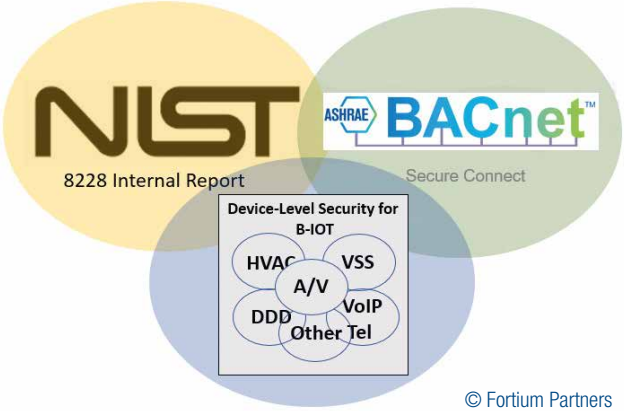
In the event that some of the B-IoT operate independently of BACnet, the IT working group can recommend that those systems be secured, at the device level, to prevent contamination of the network that is shared or connected to BACnet-connected systems and devices. There are a growing number of excellent technologies for securing such independent B-IoT, such as:

- Software-defined networks that can create a firewall and a single managed port to control access
- Software-defined perimeter that can cloak the identity portion of each device's IP address. This makes the device invisible to unauthorized traffic
- Signal isolation devices that assure the input and output of IoT sensors
- Signal fingerprinting of devices that enable detection of anomalous signals

These technologies did not exist in critical mass prior to 2019, so now is the time to include, at least, two security layers for defending all B-IoT, including those outside of BACnet.

4. Ongoing Security Improvement. B-IoT are often comprised of hundreds, even thousands, of devices distributed widely, all in various stages of maintenance, repair and configurations, not to mention numerous suppliers, their back-up suppliers, end users and administrators. Two special considerations regarding B-IoT and cybersecurity are:

- Deploy a software platform that enables the management of 10 to 50 or more suppliers of B-IoT. This management platform is used to retain the device-level configuration data, applicable security controls, administrative users, schedules

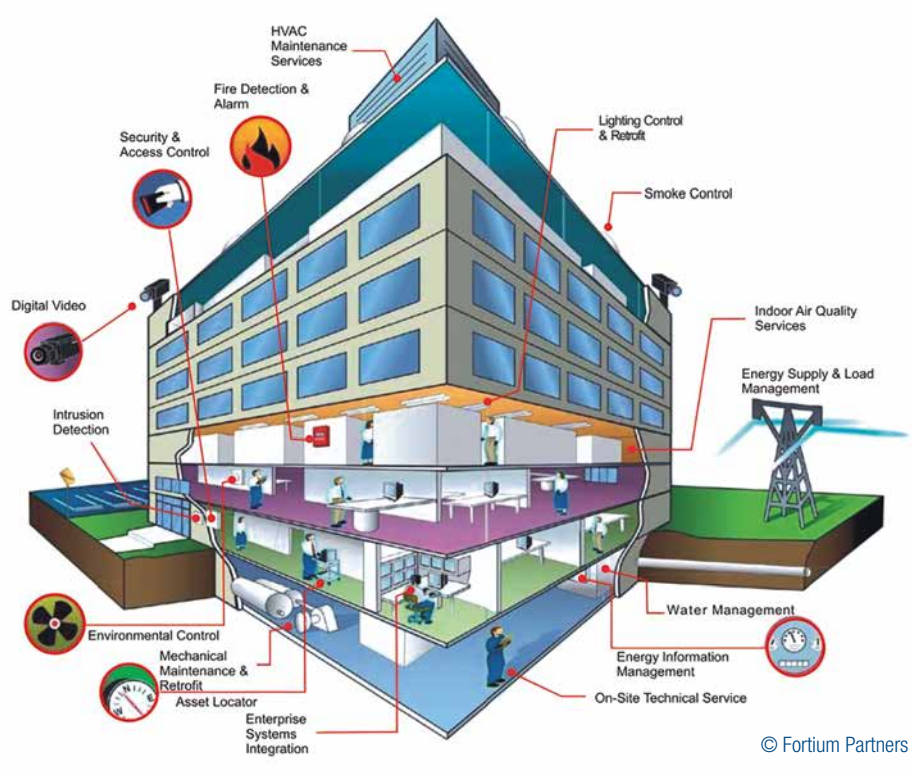


Graphic 4. NIST 8228 IR claims they have no standard or framework for Building IoT. BACnet provides commercially viable network-level security for Building IoT. Building management can refer suppliers of the B-IoT third parties for coaching on how to secure (or harden) the B-IoT devices.

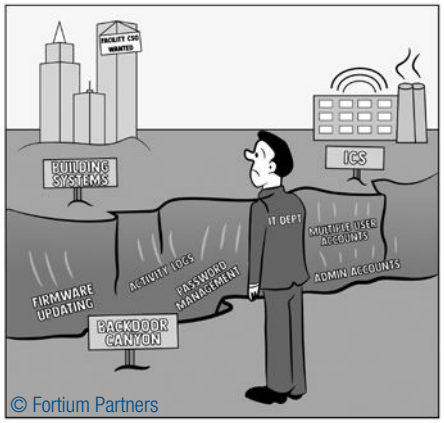
and results of annual security improvement for each system or set of devices, plus additional important detail such as key engineers at the primary supplier and back up suppliers.

- Encourage facilities management to retain an FM-CSO (Facilities Chief Security Officer) to augment the department's technical understanding of B-IoT and BACnet. This relationship is like that of a CEO and a CFO who has technical understanding of generally accepted accounting principles and financial services.
- An F-CSO could be part time or full time, depending on the size and complexity of the organization. An F-CSO would support the suppliers, and review the set of security controls each supplier might identify to secure their devices. The F-CSO would help select security technologies for B-IoT and nurture a healthy relationship with the IT department.

These special considerations might be included by the BACnet IT working group and training programs.



Graphic #6. Buildings are getting smarter and filled with sensors. Facilities Management, Building Automation and Industrial Control Engineers will bear the responsibility for security at least until manufacturers include security concerns in the design of Building IoT and even then there will be the years-long transition from older to newer Building IoT.



Graphic #5. As much as IT might like to help, Building IoT do not interoperate with IT's management tools. Responsibility for security Building IoT and other Building Systems belongs to Facilities Management and their suppliers of Building IoT.

Before 2019, many of us did not realize that B-IoT undermines so much of our ability to secure IT or systems connected to the BACnet core technology. Similarly, before 2020, there was not a whole lot that we could do about it. Now, so much has changed with BACnet becoming the standard for building automation, development of BACnet SC, plus 2019's advance of several security technologies for B-IoT.

Fortunately, both the strategy and technology for securing B-IoT are sufficiently mature and better cybersecurity is at our fingertips. There is nothing to hold us back, but ourselves. Perhaps BACnet and the BACnet/SC community will set a standard of care that leads to buildings that are both smarter and more secure.

© Rakow

Dr. Joel Rakow
Partner | Fortium Partners
joel.rakow@fortiumpartners.com | www.fortiumpartners.com

FORTIUM Partners

ABOUT THE AUTHOR

Securing building systems and other IoT against cyber attacks, Dr, Rakow delivers pragmatic solutions. He is available to lead and advise Executives, Senior Management, Cybersecurity Personnel, Property Owners and Management, and address boards of directors and large groups.

Rakow is a Partner in the Cybersecurity Group at Fortium Partners. He is a former Harvard Post-Doctoral Fellow and Advisor to the U.S. Secret Service. He was awarded Microsoft Partner of the Year and Implementation of the Year, and PC World Magazine's Best Product of the Year for 3 years. You can find out more about Dr. Rakow at https://www.linkedin.com/in/joel-rakow/

EnOcean to BACnet Gateway – A New Way to Bridge These Networks

The Contemporary Controls' EnOcean to BACnet gateway integrates EnOcean devices into a BACnet network. The gateway allows users to discover and select EnOcean devices for inclusion on their network. It will then create new virtual BACnet devices having BACnet objects.

By selecting the appropriate EnOcean Equipment Profile (EEP) for the EnOcean device, the gateway knows which BACnet objects to create for this virtual BACnet device and how to map the received EnOcean data to these objects. As more EnOcean devices are added to the gateway, more virtual BACnet devices will be created. All of these BACnet devices exist on their own virtual network. This allows BACnet head-ends to easily discover these devices and receive the EnOcean data via BACnet.

For multiple EnOcean devices of the same type, many BACnet head-ends provide the ability to copy/paste these virtual BACnet devices including their objects, schedules, trends, graphics, and alarms to simplify integration. Objects from the first virtual BACnet device, along with its selected features, can be copied for each identical EnOcean device in the facility, saving considerable effort.

All the configuration occurs via the built-in webpages using a standard browser. Our gateway provides the Received Signal Strength Indicator (RSSI) level for the last received EnOcean transmission as one of its BACnet objects for the virtual device corresponding to the EnOcean device sending the message. This will allow BACnet head-ends to understand the stability of the EnOcean network. The head-end will know that the rest of the objects from this virtual BACnet device are now valid and can be utilized.

Contemporary Controls
info@ccontrols.com | www.ccontrols.com

CONTEMPORARY CONTROLS

The Development and Success of "The Integrator" in the City of Ottawa

Nepean Sportsplex Recreational Facility

For over a decade, the City of Ottawa has made great strides to develop, implement and operate a BACnet BAS "Integrator". This is a web-based application (B-AWS) that provides a common front end for data from multiple sites, vendors and equipment to simplify control, monitoring and troubleshooting of HVAC systems. This system enables unique interoperability and allows for a more effective and cost-effective system that brings data from all sites, vendors and systems into one intuitive front end.

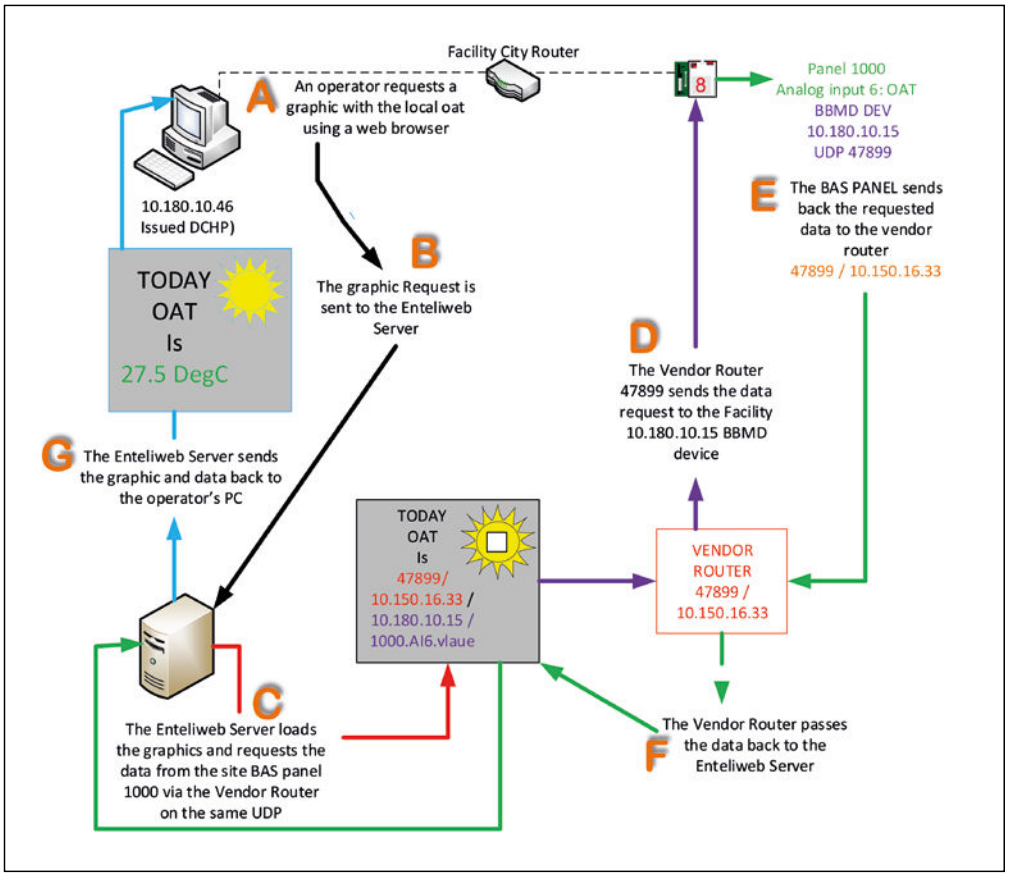
The City of Ottawa is a very early example of a user who was able to effectively integrate more than two vendors together, and one of the first municipalities to administer its own integration.

The Integrator is maintained by a team of energy engineers and technicians within the City of Ottawa, collectively referred to as the 'BEEM' Team - **B**uilding **E**ngineering and **E**nergy **M**anagement.

Challenges that Led to The Integrator Project

In 2001, the City of Ottawa amalgamated, merging 17 different municipalities into one. The City of Ottawa now owned upwards of 900 buildings, each with their own preferred BAS control vendors. For the 8 full time HVAC mechanics on staff, this presented a significant challenge to learn and master multiple systems, software and interfaces from various vendors. There were some building automation systems in which only one, or no, staff member had the knowledge of how to change a set point or schedule the system. This resulted in additional equipment being purchased to override a system, purchasing vendor maintenance, and ineffective controls.

Rooftop unit graphic



Vendors' traffic is separated by UDP ports

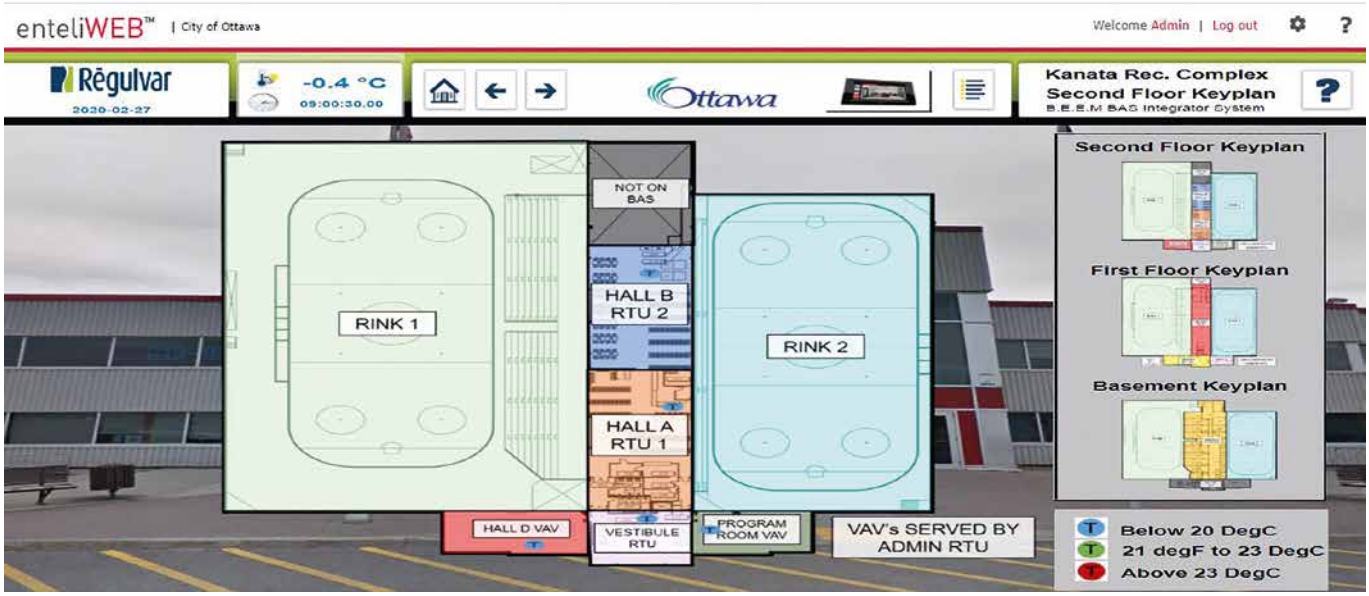
The Integrator

With a budget of US$ 900,000 and allowance for an additional full-time staff member, the City of Ottawa embarked on The Integrator project. Senior controls technician, Christopher Fellows, was hired to assist Rozon with development and implementation. Initial concerns were expressed that if development was sourced from a third party, there would be reliance on a particular vendor. If the City built its own software, then the system could be maintained entirely by internal staff. After an extensive review, the City of Ottawa began to build its own system and a support team to ensure no future reliance on external vendors for system maintenance or modernization.

Rozon remembers, "At the time, 2010, not a lot of integration was happening anywhere. A good integration system would involve two vendor packages, but rarely did you have more than that. And even at a plug fest you could see just 7 different vendors compared to the 14 that we use. So, at the time it was quite a challenge."

With numerous BAS control vendors, the City was also struggling to take advantage of automation capabilities and was unable to capitalize on competitive market pricing for additions and retrofits. A few years after the amalgamation, Jean Paul "JP" Rozon began working for the city as an energy management and building automation professional. The City of Ottawa standardized on BACnet as the BAS protocol early in BACnet development; however, not all vendors were familiar with the protocol and its benefits, and not all had implemented it to the scale the City was attempting. Rozon recognized enabling the disparate systems to work together congruently would be more effective for City staff. In 2009, the City of Ottawa decided that an integrated front end for the different systems would provide ease of use and cost savings, and Rozon was tasked with creating an Integrator.

A focus group was established to develop a standard for the Integrator. The goal was to create one common front end to ensure all facility staff could access data remotely for monitoring, alarming and troubleshooting.



Key plans showing color-coded systems

Rozon recalls that the team, "did a lot of seemingly little but important things to make it easier for staff to understand the different systems. Standards were created to use consistent graphics across the different vendors. Naming conventions were developed, displays used one color for output points, one color for input points and one color for set points. A library, community center, fire station, and sports complex may all have different systems, but now it's easy for a mechanic to look at any vendor's system without having to reorient themselves."

The team also built key plans for each site. An alarm on the Integrator front end alerts staff responsible for that site of an issue; for example, temperature complaint in a gym. Rozon describes what happens next, "An alarm is shown on the Integrator interface. Clicking on the alarm shows the gym on the facilities map. You can look at the temperature, and when you press the link, it'll bring up air handling unit two, so you know what unit is feeding the gym and are able to investigate and correct the issue."

The Integrator also allows for customization. Data can be pulled from specific devices and units to review for trends. Troubleshooting and optimization is significantly easier. Personnel can be assigned different access levels. Alarms are most useful to the staff in charge of the specific sector where the alarm is occurring, and not all users. While standardized, the interface is also set up to be specific to the user to provide the necessary access and control levels for their position.

Implementation and Growth

Ottawa now has 138 different sites communicating to the same front end via the Integrator. It can interface with controls from 14 different vendors, with BACnet adopted as their standard. Today, not all sites are on this standard, however, despite the limitations, the data is still accessible through the Integrator.

Christopher "Chris" Fellows, BAS Project Manager, "All our HVAC mechanics now have a tablet and they can sit on the roof and troubleshoot by controlling set points and watching dampers open and close. They can do that real time, see the temperatures change. Meanwhile, they can look at a building they were in earlier in the day to make sure it's working properly and answer a call and look at a third building all from their tablet."

Education

Despite the project's success, it was equally important for the team to reach out and educate staff about how the Integrator works as well as champion the benefits of the new system. Chris Fellows explains, "One of the things we've done is we offer four half day sessions on building automation. We spend half a day on building automation, then half a day on HVAC principles, and half a day on energy principles, and then half a day on troubleshooting. So, at the end of the two days, given over a one-month period, our facility staff have a much better grasp of BAS and HVAC systems in terms of comfort problems, mechanical problems, operational problems…and it's been great in making sure the facilities staff understand how their systems work."

Vendor Communication

The City of Ottawa Building Automation System specification is 32 pages long and covers all control requirements for a new installation. In order to communicate more efficiently to vendors, consultants and contractors with smaller projects, the BEEM group also created a much shorter four-page Application Specific Controller specification application for things like roof top units or VAV boxes. This ensures that if only one piece of equipment is being replaced, there is a much more clear, focused and concise requirements document available.

The specification is a living document, with one or two meetings and revisions a year. The BEEM group works closely with City IT to ensure safety and security of their systems against malware, or other incursions.

What's Next?

Building on the success of the Integrator, the City of Ottawa and BEEM group is currently looking at integrating building automation with the planned replacement of the facilities booking system. This would allow for timing and set points to be set in accordance with the type of event booked. Different groups and locations may have different temperature requirements.

There is also the opportunity to expand or optimize other applications. Energy management for example. An energy module would allow data from variable speed drives to be extracted in order to calculate savings gained compared to when fans were running at 100%.

Elevators and fire safety systems are also on the radar as those systems all have challenges. Often there is a sole vendor responsible for a site that could potentially inhibit competitive pricing.

Other areas for future development include Security and Access, expansion into Cellular networking to bring more devices into The Integrator, and possibly working with other City infrastructure groups, such as public transportation.

Summary

With the help of the BACnet standard, the City of Ottawa was able to develop and implement a BACnet-based specification that made interoperability achievable and manageable. The Integrator integrates as many as 14 different BAS vendors harmoniously under a standardized web-based user interface.

Vendors and product lines are listed below.

Contractor, BAS Product Line

- Ainsworth, Schneider Electric
- Automated Logic, Automated Logic
- Cimco Automation Group, Delta Controls
- Crosstech Controls, Distech Controls
- Honeywell Building Solutions, Honeywell Controls
- HTS Engineering, Alerton
- Johnson Controls , Johnson Controls Metasys
- Lar-Mex , KMC Controls
- Modern Niagara, Distech Controls
- PSI Mechanical Services, Johnson Controls Facility Explorer
- Regulvar, Delta Controls
- REL Controls, Reliable Controls
- Seresco, Seresco Technologies
- Siemens, Siemens Apogee
- Wiles-Legault & Associates, Johnson Controls Facility Explorer

© Rozon

Jean Paul Rozon
Section Manager
Building Engineering & Energy Management (BEEM)
Recreation, Cultural & Facility Services Department
jp.rozon@ottawa.ca | engage.ottawa.ca/energy-evolution

Leveraging BACnet to Unify Lighting and HVAC Controls

Enatai Elementary, Bellevue School District

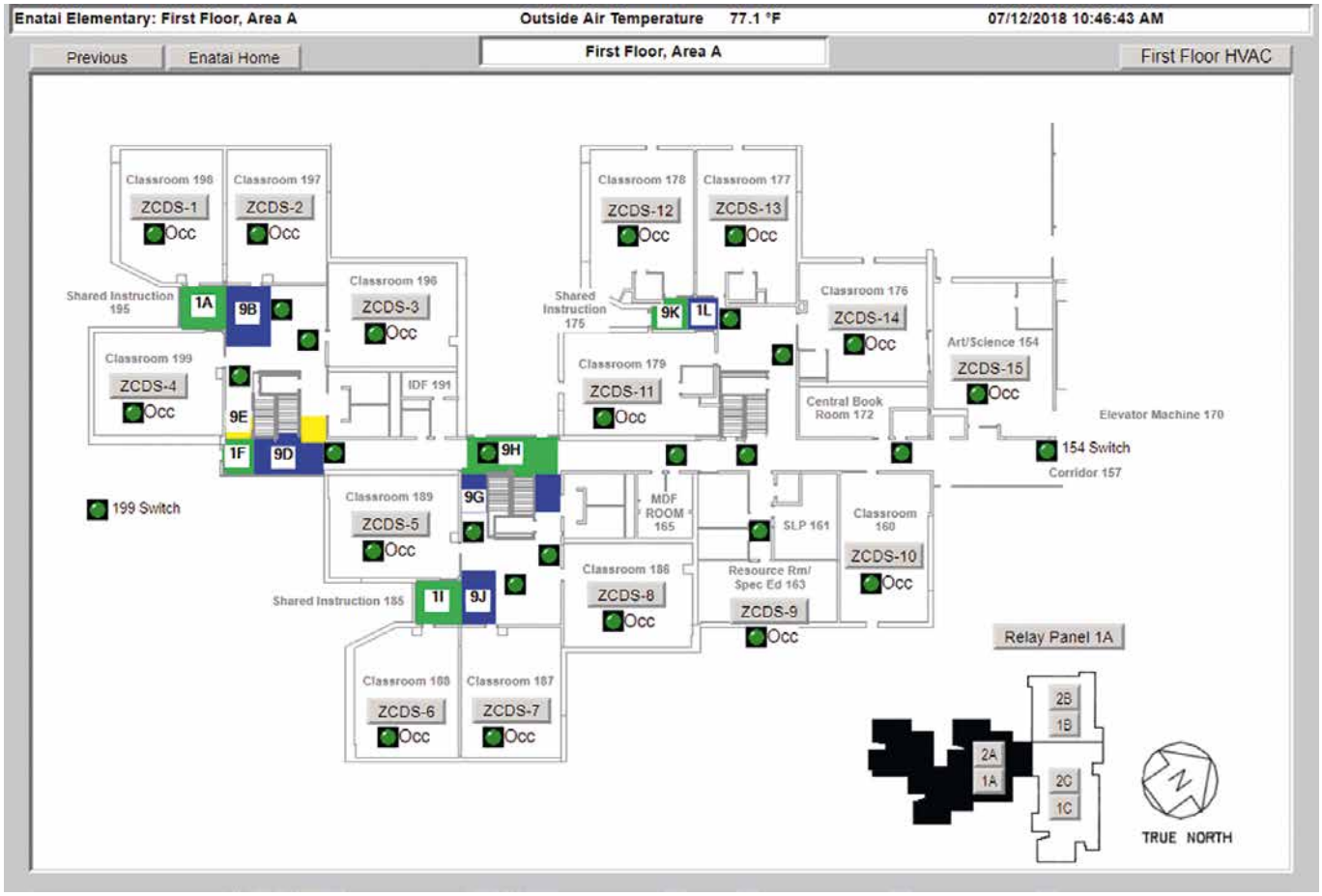
Bellevue School District Modernization Plan

Starting in 2002, the Bellevue School District (BSD) began replacing and updating schools that no longer met the needs of their growing community. BSD's goal with each new school is to exceed energy design requirements as defined by the 2012 International Energy Code. As of 2018, BSD has replaced 18 schools with state of the art facilities that incorporate the latest educational designs, technology and BACnet native controls to ensure students and teachers have an ideal learning environment. By making each new school as energy efficient as possible, BSD is ensuring they are maximizing their capital dollars, which will allow them to make the best use of their general funds. In 2015, as part of the ongoing modernization projects, Enatai Elementary was demolished to make way for an updated facility that will host elementary students well into the future.

BACnet Native Lighting and HVAC Control

BSD is determined to improve upon school designs with each facility replacement. When planning for the new Enatai, BSD decided their next improvement would be to house as many of their controlled systems under their BACnet platform as possible. Having worked with ATS Automation for many years, BSD was familiar with the environmental controls provided by the Alerton building management system (BMS) from their other schools. Once ATS demonstrated that they could efficiently control the HVAC equipment and incorporate all the lighting into the same BMS, BSD chose ATS to provide the HVAC and lighting controls for the Enatai facility. By selecting one vendor, staff at Enatai has access to ATS' expertise for both HVAC and lighting during the original installation and for long-term service. Now Enatai has one point of contact when it comes to the controls for their school — simplifying maintenance and operations. To integrate HVAC and lighting, ATS designed a system utilizing Alerton's Compass BMS and Blue Ridge Technologies' (BRT) BTL listed BACnet native lighting control platform.

Combined, Alerton and BRT provide a unified lighting control system without the use of proprietary gateways. Utilizing BACnet, BRT controllers are easily added to the Alerton BMS without needing any integration device. This solution allows BSD operators to use the same schedules for both HVAC equipment and lighting without the need to duplicate work in a separate lighting interface. ATS programmed a global BACnet schedule for lighting at Enatai in conjunction with BRT monitoring classrooms and common areas using occupancy sensors and photocells. These sensors are used for daylight harvesting and turnoff or dim lighting according to lumen levels and whether the area is occupied or not. Classroom lighting control features a traditional on/off switch in the front



Key plans showing color-coded systems

of all classrooms, as well as a separate adjustment panel near the teachers' desks.

Impact on Energy & Operations

By combining environmental and lighting controls, BSD has ensured that their high efficiency designs and equipment will continue to save the school money throughout the life of the building. "The strategy is that on day one the facility is already saving on utility bills," said Jeff Tweeten, HVAC/Utilities Control Specialist for the Bellevue School District. Tweeten continued "By saving on day one, the measured benefits are all about the efficiencies that directly impact the learning environment." With integrated lighting, Tweeten and his team can focus on what really matters — ensuring the learning environment is optimal for both students and teachers.

The new Enatai Elementary nearly doubled the size of the original school to 87,500 square feet. The school opened to the public in September of 2016 with over 500 students attending class during the academic year. The school also received $135,013 in utility incentives by Puget Sound Energy (PSE) for exceeding local energy code requirements and standard practices during construction.

In addition to lighting and environmental controls, the new Enatai elementary school features other energy efficient technology, such as geothermal heating and cooling, solar panels, heat recovery, AstroTurf, solar hot water loop and high efficiency sequences for mechanical equipment. Utilizing solar panels, Enatai recovers approximately 90,000 kWh per year. This harvested energy covers the majority of the school's lighting cost for the year. Enatai's energy use index (EUI) was also significantly improved from the previous facility. The school's combined electric and natural gas EUI is currently 17 and is expected to decrease as system tuning continues. The national median source EUI for K-12 schools is 141.

ATS Automation, along with Alerton and BRT, help Enatai maintain optimal performance with rock solid building controls and sequences, along with occupancy-based lighting usage and automated daylight harvesting. The BSD team is committed to advancing the BACnet based control strategies for their schools, ensuring that all of their campuses are both energy efficient and environmentally pleasing for everyone.

BACnet Controllers Optimize Chiller System

© Contemporary Controls

Chiller systems can consume 35% or more of all the energy needed for building climate control. Chilled water, used in conjunction with air handler units (AHUs), cools and dehumidifies the air in mid-to-large commercial, industrial, and institutional facilities. Significant energy cost savings can be obtained by optimizing chiller operation.

A pharmaceutical manufacturing facility in Cali, Colombia, South America, utilized BACnet controllers to optimize the operation of their chillers serving numerous clean room laboratories where temperature control was critical.

A pharmaceutical manufacturer located in Cali, Valle, Colombia wished to improve chiller operation and in-plant temperature control, while retaining as much of the existing control system as possible. The facility utilized four chillers to provide temperature control to twelve ISO 9000 clean room laboratories – each with one air handler (AHU). BACnet/IP controllers were chosen for use with an existing PLC to dynamically control the chillers.

BACnet/IP networks communicate over the "Internet Protocol" which allows devices to talk to each other using the protocol rules of IP and Ethernet. By selecting BACnet/IP, the existing control system could be networked to new controllers dedicated to the AHUs, "smart" control valves added to the chilled water system, and a supervisory controller running an optimization program and display showing an overview of the entire system. Operation over Ethernet allowed data transfers at speeds up to 100 Mbit/sec to occur, for near instantaneous response to cooling demand.

The BACnet controllers were configured to read, transfer, and utilize area cooling information within the facility. The PLC controller did not support BACnet, so a gateway functioning as a BACnet server as well as an Ethernet/IP client mapped PLC points to BACnet/IP. The BACnet controllers were then configured to create BACnet/IP clients that would initiate commands to the gateway which in turn transferred data to-and-from the PLC. An industrial computer, running a proprietary chiller optimization program, was installed as a BACnet/IP client that dynamically controlled the chillers to obtain the desired energy savings. The optimizer algorithms would change the chilled water setpoint, sequence and rotate chillers in order to maintain only the necessary chillers running at the most efficient capacity based upon demand as well as adjust flow rates in the chilled water distribution system.

Space temperature in each laboratory had to be accessed from the PLC. Real-time energy consumption was obtained by transferring data from power meters connected to the PLC. Air handler status and control was turned over to the BACnet controllers. Supply air setpoints, cooling valve setpoints, and chiller setpoints needed to be sent to the optimizer. The BACnet controllers complied with the B-ASC device profile and offered a convenient mix of 8 universal inputs, 4 binary inputs, 4 analog outputs and 4 relay or triac outputs. Unique to the units were 48 web components which link wire sheet readable/writeable data to web pages, as well as 24 virtual points which link wire sheet readable/writeable data to a BACnet client. Five of these controllers were dedicated to the air

handlers, while a sixth was utilized for chilled water control. Their outputs commanded damper position, chilled water flow rate (using added energy control valves) or power usage. The BACnet controller inputs in turn were utilized to monitor AHU supply air temperature, airflow, Delta T, and setpoints. A touchscreen, supplied as part of the optimizer system, offered the facility an interface to the chiller operation as well as an energy usage display.

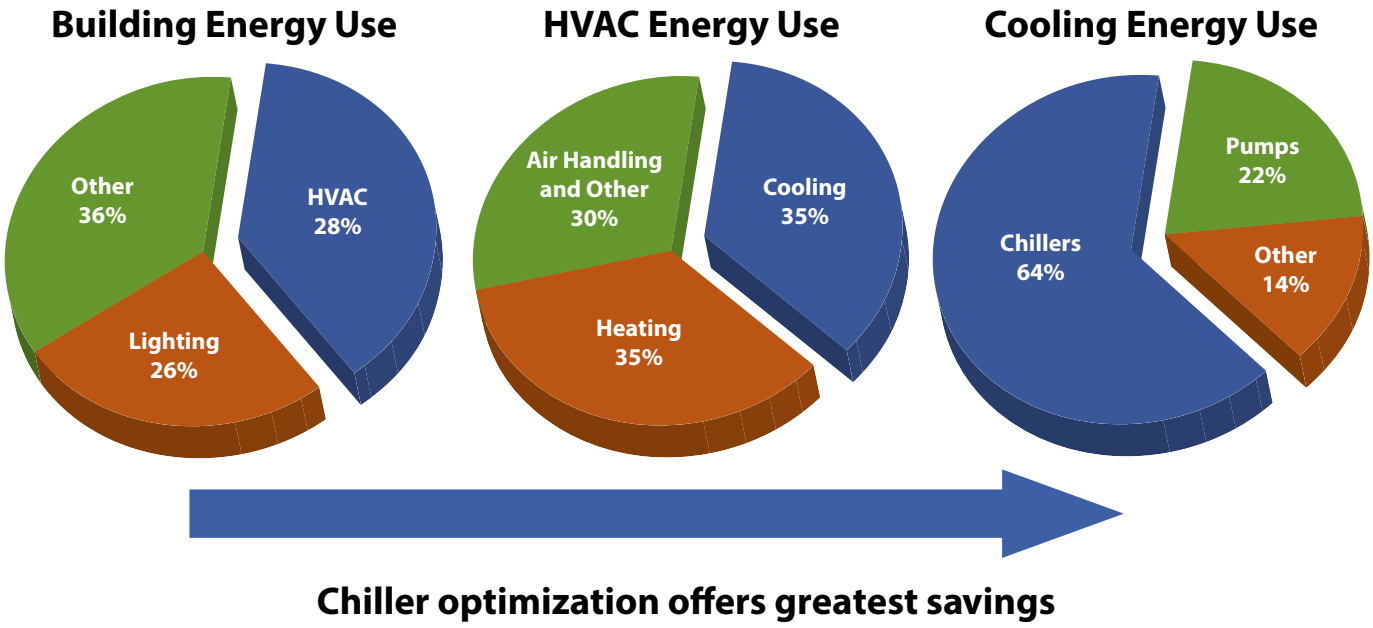
Energy valves were fitted to the cooling coils on each of the air handling units-one per laboratory. The valves could be operated in any of six modes; position control, flow control, or power control with or without delta-T control. One BACnet controller was assigned to two or more air handlers. Depending upon energy valve operating mode, the BACnet controllers could be commanding damper position, flow rate, or power usage. In addition, each controller used physical inputs to obtain air handler temperature in and out, as well supply-air fan verification. Cascaded PID loops created the 0-10V cooling setpoint that was sent to each energy valve.

This chiller optimization project demonstrated that existing industrial control systems can be made to operate with technologies intended for building automation. BACnet/IP, being an IP based protocol, lends itself well to the enhancements provided by the Internet. Because of this, the BACnet controllers could be accessed remotely via a VPN connection. A VPN capable router was installed at the job site as part of the IP network. It has the capability to communicate to any number of clients over a secure virtual private network. The optimizer graphics, BACnet controller webpages, program wiresheets, and web pages from the energy valves were all available for remote monitoring and supervision, greatly enhancing project support. BACnet made the difference.

© Contemporary Controls

Contemporary Controls
info@ccontrols.com | www.ccontrols.com

Energy Saving Opportunities



© Contemporary Controls

BACnet Interface for People-Movers at Manchester Airport

Passenger transport at Manchester Airport. © Manchester Airport

Twenty-four airlines operate to countries all over the world from Terminal 2 at Manchester Airport. Today there are literally millions of BACnet devices in use worldwide, many of them in municipal facilities such as airports. BACnet is not restricted to just communicating HVAC points. It is also suitable for monitoring ancillary equipment including lifts, escalators and moving walkways.

Otis Elevator Company was selected to provide the people-mover solutions for Terminal 2. They turned to Contemporary Controls Ltd (CCL) in Coventry, UK for assistance with the integration of their elevators, escalators, and moving walkways with the Delta Controls' enteliWEB Building Management System (BMS) serving as the head-end. Working within the specifications, CCL developed a solution that met the requirements for either a lift or escalator.

Contoller for Lift and Escalator Solutions

The BAScontrol22 (BASC-22R) 22-point unitary controller was chosen for this application because it supports BACnet/IP and Sedona programming over an Ethernet connection. The controller has a convenient mix of physical I/O points, including 8 universal inputs, 4 contact closure inputs, 4 analog outputs, and 6 relay outputs. 48 web components and 24 virtual points are supported as well and are web-page configurable. Two 10/100 Mbps Ethernet ports allow for BACnet/IP communication over a daisy-chained Ethernet connection.

For the Terminal 2 installation, voltage-free contacts from the Otis equipment served as the customer's monitoring interface. Each binary point appears to the head-end as a BACnet binary object (BI or BV). There were six points on each lift (elevator) and five points on each escalator or moving walkway requiring some of the universal inputs to be converted to binary inputs. Alarm status, multiple out-of-service conditions, fire recall and power failure conditions are monitored on each device, with staff at the head-end station able to monitor operation and dis-

The BAScontrol22 provides the BACnet interface for people-movers at Manchester Airport.

patch the appropriate personnel based upon the problem reported. The controllers were in confined spaces such as elevator shafts and as such required environmental protection. Contemporary Controls Ltd designed and provided IP66 level enclosures with gland protection for all input and output wiring. Each enclosure features a mains power disconnect, low-voltage power supply, and the BASC-22R controller.

Elevator related BACnet Objects

All the status points were binary. However, BACnet analog points (AI, AV or MV) could be provided if analog signals were available at the customer connections. Analog information such as power consumption and walkway speed could be useful and easily accommodated by the controller.

The main approach to integrating elevators/escalators into a BACnet system is to use the BACnet object group for this purpose. BACnet has three elevator related objects – the Elevator Group Object, the Lift Object and the Escalator Object. The Elevator Group Object is an object which contains the other lift and escalator objects that represent the lifts and escalators within the building. The Lift object contains the status of the lift such as the car's position, car mode, status, passenger alarm, the lift's energy usage and any faults. The Escalator object contains the escalator direction, mode, energy usage, status, passenger alarm and fault information.

The advantage of using the BACnet elevator related objects is that this is a standardized approach suitable to all vendors of people-moving equipment. As demand for people-moving equipment integration increases, more head-ends will support these objects.

Contemporary Controls
info@ccontrols.com | www.ccontrols.com

New to the BACnet International Family

Member of BACnet International

BACnet International is the global organization that encourages the successful application of BACnet through interoperability testing, educational programs and promotional activities. BACnet International complements the work of other BACnet-related groups whose charters limit their commercial activities.

BACnet International community membership includes a who's who list of top tier companies and industry professionals involved in the design, manufacture, installation, commission and maintenance of control and other equipment that use BACnet for communication.

We are proud to welcome the following new members to BACnet International.

Gold Member

ARMSTRONG

Armstrong Fluid Technology
With over 1200 employees worldwide, operating seven manufacturing facilities on four continents, Armstrong Fluid Technology is known as an innovator in the design, engineering and manufacturing of intelligent fluid-flow equipment. With expertise in demand-based control, digitalization, fluid-flow, and heat transfer, Armstrong Fluid Technology provides energy-efficient, cost-effective solutions to building professionals and owners around the world.

23 Bertrand Ave
Toronto, Ontario, M1L 2P3
Canada

MSA The Safety Company

MSA Safety – Sierra Monitor
Sierra Monitor, an MSA Company, addresses the industrial and commercial facilities management market with Industrial Internet of Things (IIoT) solutions that target facility automation and facility safety requirements. Their distinguished track record in industrial sensing and automation with IoT technologies such as wireless, cloud connectivity and data services put them at the forefront of the emerging IIoT trend.

1991 Tarob Court
Milpitas, CA 95035,
United States

Silver Member

CONNEX SOFT

ConnexSoft GmbH
ConneXSoft is a software development company specializing in connectivity for Industrial Automation. The specific focus is on the Facilities and Energy management markets. ConneXSoft provides data acquisition servers, objects and engineering tools for native integration into HMI/SCADA systems of Industrial Automation market leaders to enable vertical solutions in these markets.

Lohenstrasse 4
D-82166 Graefelging
Germany

CRESTRON

Crestron
Crestron is a leading innovator and manufacturer of advanced control and automation systems for the office, campus, and home, reinventing the way people live and work. With integrated solutions to monitor, manage, and control audio, video, and lighting, shades, and climate, Crestron streamlines technology to improve the quality of life for people in corporate boardrooms, conference rooms, classrooms, hotel rooms, auditoriums, and in their homes.

6 Volvo Drive
Rockleigh, New Jersey, 07647
United States

Silver Member

Douglas Lighting Controls
Douglas Lighting Controls, a member of the Panasonic group and a subsidiary of Panasonic Lighting Americas Inc., engineers, manufactures, and markets digital lighting controls for commercial buildings, campuses, parking garages, and sports complexes across North America. Douglas systems include networked and stand-alone solutions using wired and wireless technology to optimize lighting for building code compliance, energy efficiency, ease-of-use, and comfort.

280-3605 Gilmore Way
Burnaby, BC V5G 4X5
Canada

Engineered Air
Engineered Air is one of North America's largest manufacturers of Heating, Air Conditioning, Ventilation, Refrigeration, Energy Recovery and Heat Transfer Products. Their integrated sales, design and manufacturing groups enable the company to produce equipment that is designed to fit unique project requirements. Engineered Air proudly serves customers across North America in commercial, industrial, institutional, waste water, cleanroom, food processing industries.

1401 Hastings Cres SE
Calgary AB T2G4C8
Canada

Meitav-tec Ltd
Meitav-tec provides innovative, tailor made solutions for temperature control. Driven by technological innovation and guided by a veteran, top expertise research and development team, Meitav-tec has ample experience in the design, manufacture, sale and support of temperature control solutions.

6 Sapir Street
Rishon-LeZion, 75150
Israel

Silver Member

MOXA
Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 65 million devices across the globe.

Fl. 4, No. 135, Lane 235
Baoqiao Rd. Xindian Dist.
New Taipei City, 23145 Taiwan, R.O.C

Paragon Controls Inc
Paragon Controls Incorporated manufactures airflow and pressure sensing elements, transducers, room/space pressure monitoring systems, and control systems for clients worldwide in the commercial ventilation, laboratory, healthcare, pharmaceutical, power, semiconductor, waste water treatment and various other light and heavy industrial markets.

2371 Circadian Way
Santa Rosa, CA 95407
United States

SDataway
Founded in 2007, SDATAWAY SA was born of a single idea – a concept to simplify firewall system management in the construction industry. Over the following years, the company continued to spark innovation in the building regulation sector and development of electronic and software products. SDATAWAY SA has successfully completed more than 600 Research & Development projects, each one developed by the skilled, multi-disciplinary team of engineers on site

Route de Montreux 149
1618 Châtel, Saint-Denis
Switzerland

New to the BACnet International Family

Silver Member

SoftDEL
Softdel delivers IoT design, consulting, development and integration solutions to a wide range of global product companies and OEMs to help them innovate faster. A suite of pre-built software stacks and tools not only help to reduce time to market but also make Softdel's solutions more affordable. Specialized domain-knowledge backed by consistent quality and an agile delivery system, makes Softdel a preferred partner for global companies, including many Fortune 500 majors.

One Dock Street
Suite 201,
Stamford, CT 06902
United States

Upgraded Member

BACnet International would like to congratulate the following companies on their strengthened commitment to the BACnet protocol and increasing involvement in the BACnet community. As part of these actions they have moved their membership to a higher tier. We thank them for their continued support and look forward to many more years of collaboration.

Gold to Platinum

EasyIO
EasyIO innovates at every level with distributed intelligence, less complexity in engineering, open compatibility, inclusive engineering tools and maintenance, and IT ready devices. From the edge to the cloud, they develop best in class products that provide the flexibility to choose the architecture that best suits their customers' needs.

31 International Business Park #03-02
Singapore 609921
Asia

Corporate Affliate to Gold

WAGO
Founded in Minden, Germany as an international company in 1951, WAGO Corporation specializes in electrical interconnection, industrial interface modules and automation products characterized by the original spring pressure connection technology. Its business is across Europe, North America, Latin America, Asia as well as other countries and regions.

Hansastraße 27
32423 Minden
Germany

THANK YOU

to our global members for supporting BACnet

BACnet International

Spread the Word!

Education • Library • Community

Currently, there are many resources on The BACnet Institute (TBI) that will help you as well as your colleagues stay connected and engaged. In fact, a better-informed community brings positive change, so take a moment to expand your knowledge of BACnet as well as encourage others!

Popular BACnet International AHR Expo sessions are online

The BACnet International Education Track at the 2020 AHR Expo received record-breaking attendance. Now all five of the sessions are available on TBI for you to experience, either again or for the first time. The sessions include *BACnet 101; BACnet Physical Connectivity; Design Considerations When Applying the BACnet Standard to a 'Smart Building' BAS; BACnet Edge Solutions;* and *HVAC as a Service*. Many more sessions from past events are available on TBI as well, so make sure to take a look.

Library continues to expand

With over 70 articles focused primarily on BACnet, the TBI library offers a variety of topics, in different languages and experience level. The top articles include "A Brief History of BACnet"; "Achieve BBMD Support with the BAS Router", "BACnet Test Framework- The Perfect Tool", "BACnet Protocol Analysis Using Wireshark"… and there are many more. Also check out the recently added, bi-lingual "Device Profile Families Facilitate Planning" article by Bernhard Isler. Check back often, since articles continue to be added.

Interactive courses fit into your schedule

There are currently three interactive courses available on TBI. First, BACnet Basics is a comprehensive course that covers all the basics of BACnet. If you don't know anything about BACnet or simply need a refresher, this is an excellent course to take. The second course is The Facility Manager's Guide to Building Automation Systems. You don't need to be a facility manager to take this course, in fact, this course is incredibly beneficial to anyone who works in the building automation industry. Lastly, our new course, BACnet Device Profiles, introduces learners to the various BACnet device profiles, defining the role of each in building automation. In addition, this course explains how the various profiles can be combined in a single device, while adhering to the rules behind the combinations. All courses are accredited for Continuing Education Units (CEUs).

If you haven't visited The BACnet Institute recently, you definitely should! AND, remind your colleagues to do so as well! To access all of these resources, or to sign up for a FREE account, visit www.thebacnetinstitute.org.

© BACnet International

Michelle Eriquez
The BACnet Institute | Education Manager
education@thebacnetinstitute.org | www.thebacnetinstitute.org

CEUs now available with all three interactive courses on TBI! (And they're all FREE)

BACnet International is authorized by the International Association for Continuing Education and Training (IACET) to offer CEUs for its courses.

BTL Testing Updates and BACnet Secure Connect

A 2017 market research study indicated that BACnet's global market share is over 60% of the Building Automation and Controls market. Product specifiers continue to require BACnet as the protocol and to require BTL Certification to ensure the correct implementation.

A BTL Certification indicates that a product has successfully passed rigorous verification by testing and demonstrates that it correctly implements rules and interoperability of the BACnet protocol. The BTL Certification includes a BTL Listing, BTL Certificate of Conformance, and the right to use the BTL Mark.

The BTL Mark may be displayed only on products that have successfully passed BTL Testing. Testing ensures that the device correctly implements all of the BACnet functionality it contains as governed by ASHRAE standard 135.1. The BTL Working Group defines the BTL Test Plan and governs the testing.

New Release of BTL Test Package

Test Package 18.0 has been published on the BTL website: www.bacnetlabs.org/page/test_documentation

With this release of the BTL Test Package, test coverage has been extended to include most functionality contained in Protocol Revision 18, along with some functionality from later Protocol Revisions (BACnet Secure Connect).

Test Package 18.0 replaces Test Package 16.1.3 as the current test package. The BTL Working Group has set the Transition Period to end February 1, 2021. During the Transition Period, vendors may choose to have their product tested with either test package for those products having Protocol Revision 16 or lower. Products with Protocol Revision 17 or higher must use Test Package 18.0. Any product currently in BTL Testing will continue with Test Package 16.1.3

Development of BTL Tests for BACnet Secure Connect

BTL Testing for BTL Certification of BACnet Secure Connect (BACnet/SC) products is separate from the BACnet/SC Interoperability Acceleration Program. BTL Testing for BACnet/SC is handled in the same way as any BACnet functionality, and that testing is now available. These tests were published in July 2020, as Add-BTL Test Package 16.1-bj. These and other addenda have been included in Test Package 18.0, published October 30, 2020.

The BACnet/SC Interoperability Acceleration Program provides a testing environment (BRITE, described below) in which manufacturers may connect with partners to test their BACnet/SC functionality.

(See more details concerning this program on the BACnet International website here: www.bacnetinternational.org/secureconnect.)

The BRITE (part of the BACnet/SC Interoperability Acceleration Program) should not be confused with BTL Testing for BTL Certification.

Updates to BTL Testing Policies Pertaining to BTL Certification

In January 2019, the BTL Working Group provided the ability for Regression Testing for Renewal of a BTL Certificate. (See BTL Testing Policies document on the Test Documentation page of the BTL website.) This addition to the BTL Testing Policies allows manufacturers to renew their BTL Certificate without having to do complete re-testing of their product. The BTL Certificate Renewal Testing may be done at the same Protocol_Revision of the original BTL Testing; it will include appropriate tests from the current BTL Test Package.

The BTL Working Group updated the Product Retesting Selection Policy in November 2019 to better clarify what tests should be applied for BTL Certificate Renewal and for Product Retesting Requirements. Developers should review the most current BTL Testing Policies document. This document may be found on the Test Documentation page of the BTL website.

Manufacturers and BACnet users should be careful not to confuse expirations and renewals of BTL Listings and BTL Certificates. BTL Listings may not be renewed. Once the BTL Listing on a product expires, it must be updated and undergo BTL Testing at or above the current minimum Protocol_Revision level to have a new BTL Certification. However, as a re-test of the previous BTL Testing, some tests may be eligible to be skipped. Manufacturers should provide a complete and accurate BTL Checklist (current version) for an estimate of testing hours and cost for either re-testing or a BTL Certificate Renewal testing.

The ability to renew a BTL Certificate gives manufacturers added flexibility for the longevity of their product lines.

© Hayes

Emily Hayes
BTL Manager, Certifications and
Listings Manager and BTL Working Group Chair
btl-manager@bacnetinternational.org | www.bacnetinternational.org

ABOUT THE AUTHOR

Emily Hayes began work with BACnet International in 2014 as BTL-Coordinator, coordinating BTL Testing at the BTL Lab. In 2017, Emily took over leadership of the BTL Working Group as chair. Additionally, she led the transition from the BTL Listing Program to the BTL Certification Program. She became BTL Manager in January 2019.

Emily maintains professional membership in the Project Management Institute (PMI), North Carolina Chapter of PMI (NCPMI), and Institute of Electrical and Electronics Engineers IEEE.

Emily has a BEE from Auburn University and an MSEE from Duke University. She has maintained a Project Management Professional (PMP) Certification since 2010.

BACnet Secure Connect Interoperability Acceleration Program

Cybersecurity in building automation systems is becoming more important as the industry embraces connected buildings and Smart Cities. BACnet Secure Connect was created to address an important part of the cybersecurity puzzle.

BACnet/SC Interoperability Acceleration Program

The BACnet Secure Connect Interoperability Acceleration Program is a collaborative industry project administered by BACnet International. Its goal is to accelerate successful adoption by helping suppliers rapidly incorporate BACnet Secure Connect in their products. It gives participants access to education, software and a supportive technical community for BACnet/SC.

Suppliers participating in the program have the opportunity to rapidly get their technical staff up to speed on the BACnet/SC technical specification as well as critical implementation issues.

Program Tools

As part of the program, a reference implementation of BACnet/SC was created and made available to participants. This application includes a set of capabilities and scripts that can be used across multiple platforms and enables manufacturers to rapidly develop and test their own BACnet/SC implementations in-house.

Also released to program participants was the System Test Bench, a set of configurable tools built on the Reference Implementation. The System Test Bench enables rapid creation of network environments with BACnet/SC nodes, hubs and routers to support testing of BACnet/SC devices in various system configurations.

The Reference Implementation and System Test Bench are provided to participants as part of the BACnet/SC Interoperability Acceleration Program. For those companies not currently part of the program, immediate access to the reference implementation and test tools can be obtained by joining the program. The software is expected to become available through an open source repository in July of 2021.

Product Testing

To test BACnet/SC interoperability, BACnet International is proposing an online BACnet/SC interoperability testing environment called BRITE (BACnet Remote Interoperability Test Environment). BRITE consists of a neutral online connection point where BACnet device manufacturers can participate in interoperability testing with other manufacturers, and a section where participants can connect and look for partners. It is supported by the BACnet/SC reference implementation, which provides the hubs and certificates required to connect multiple manufacturers together along with centralized interoperability support tools and network diagnostic features.

While any manufacturing company can join the BRITE program, each test session is private, only allowing access to the specific BACnet device manufacturers participating in that test session.

BACnet/SC Interoperability Acceleration program participants will receive discounts and early access to this testing.

Accelerating the availability and adoption of interoperable BACnet/SC products is an important objective for the whole BACnet community. To learn about the BACnet/SC Interoperability Acceleration Program, and determine how you can benefit from participation, visit bacnetinternational.org/secureconnect or contact David Nardone, BACnet International Regional Operations, at Dave@BACnetInternational.org.

© Ruel

Richard Ruel
Program Manager
BACnet/SC Interoperability Acceleration Program
rich@bacnetinternational.org | www.bacnetinternational.org

ABOUT THE AUTHOR

Richard Ruel has an extensive 25+ year expertise in all aspects of Building Automation and Energy Management Systems. He began his career in Building Automation Systems and Direct Digital Control as a Technical Service Engineer and went on to serve as Teletrol's Director of Technical Services where he was responsible for product revisions and application engineering. Richard most recently was business lead and responsible for the Teletrol EMS product line for Philips Lighting, where he traveled extensively on Philips Lighting and Teletrol's behalf throughout Europe and Asia supporting and training their BAS/DDC/EMS systems. Currently, Richard serves as Testing Services Manager for BACnet Testing Laboratories.

His credentials include member of AEE and past president of ASHRAE - Granite State Chapter.

TÜV SÜD Newest BACnet Recognized Testing Organization

BACnet International is happy to announce that TÜV SÜD Industrie Service GmbH is now a Recognized BACnet Testing Organization. It is one of four such recognized testing laboratories in the world. TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. They specialize in testing, certification, auditing and advisory services.

Recognized BACnet Testing Organizations (RBTOs) conduct BACnet product testing to confirm products' compliance with the BACnet standard. Their test reports are the basis for BTL Certification and Listing.

"Our testing operations establish whether the BACnet standard has been completely and correctly put into practice", says Christian Bauerschmidt, Managing Director of TÜV SÜD Industrie Service GmbH. "Successful conformity testing provides product manufacturers with third-party proof of their products' flawless communication capabilities. Correct implementation of the BACnet protocol is one of the paramount requirements to ensure products from different manufacturers can be integrated smoothly into a building automation system."

The new Building Automation Laboratory expands the portfolio of product testing and certification services provided by the existing TÜV SÜD Industrie Service Centres of Competence for Refrigeration & Air-Conditioning and Firing & Heating Technology.

As a Recognized BACnet Test Organization, TÜV SÜD Industrie Service is authorized to test the entire range of building automation components, spanning sensors and actuators, application-specific control units, freely programmable DDC systems and control and operating systems.

"We've very happy to welcome TÜV SÜD Industrie Service as the newest BACnet testing organization," said Andy McMillan, President and Managing Director of BACnet International. "They share our commitment to raising the quality and conformance of BACnet products available on the market."

More information on BACnet device testing can be found on the BACnet Testing Laboratories site here. For information on TÜV SÜD testing, visit tuvsuv.com/bacnet.

NEW BTL-LISTED PRODUCTS, August 2019 – August 2020

Manufacturer	Product Name	Model
ABB	M4M20, M4M30	M4M20SBA /, M4M 20 BACnet, M4M30SBA /, M4M 30 BACnet
Abies Technology Inc	BACnet IP Thermostats/ Transmitters/ Controllers	Tx^1B, Hx^1B, Sx^1B, Wx^1B, Vx^2B, XYB-E, XYB-W where x^1 is A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U x^2 is C, K,
Accuenergy (Canada) Inc.	AcuRev 1310 Series Power and Energy Meter	AcuRev 1312, AcuRev 1313, AcuRev 1314
Alerton	Alerton VisualLogic IP Controller	VIP-363-HOA, VIP 363-VAV
Alerton	Visual Logic Unitary Controllers	VLC-1188-E, VLC-16160-E, VLC-1600-E, VLC-550-E, VLC-853-E, VLC-651R-E, VLC-660R-E, VAV-SD-E, VAV-SD2A-E, VAV-DD-E, VAV-DD7-E
ALRE-IT Regeltechnik GmbH	KTRBUu217.456	KTRBUu217.456#x^1 (UA23000x^2) where x^1 is 21, 07, 09, 27, 55, 57, 28, 59 or 56 x^2 is 0, 2, 3, 4, 5, 6, 7, 8 or 9
Automated Logic	OptiFlex BACnet Building Controller	OF1628, OF1628-NR, OF028-NR, OFBBC
Automated Logic	OptiFlex BACnet Building Controller - Non-Routing	OFBBC-NR
Automated Logic	OptiFlex BACnet Gateway	G5CE
Automated Logic	OptiFlex BACnet Router	G5RE
Automated Logic	OptiFlex Integrator	OFHI
B.E.G. Bruck Electronic GmbH	ROUTER2-DALISYS-BACnet-REG	93355
Carlo Gavazzi Automation	MONITORING GATEWAY AND CONTROLLER	UWP30RSEXXX
Carrier	i-Vu XT BACnet Link	XT-LB
Carrier	i-Vu XT Router	XT-RB
Carrier	TruVu MPC Controller	TV-MPCXP1628
Carrier	TruVu MPC Controller, non-routing	TV-MPCXP1628-NR
Carrier	TruVu MPC Processor	TV-MPCXP
CoolAutomation Ltd.	CoolMasterNet	7,9
Crestron Electronics, Inc.	Crestron 3-Series Control Systems	AV3, PRO3, RMC3, ZUM-FLOOR-HUB, CP3x^1, DIN-AP3x^2, DMPS3-x^3-C, DMPS3-4K-x^4-Cx^5, MPC3-x^6. where x^1 is null, -R, or N, x^2 is null or MEX, x^3 is 200 or 300, x^4 is 100, 150, 250, 350, or 50, x^5 is null or -AIRMEDIA x^6 is 101, 102, 201, 302
DEOS AG	OPEN 4100 EMS	DS-OPEN 4100 EMS C1, DS-OPEN 4100 EMS C2, DS-OPEN 4100 EMS C1/R, DS-OPEN 4100 EMS C2/R
DEOS AG	OPEN 600 EMS	DS-OPEN 600/x^1 EMSx^2, DS-OPEN 600H/x^1 EMSx^2 where x^1 is 0 or 5, x^2 is null or /N

DEOS AG	OPEN 810 EMS	DS-OPEN 810/x^1 EMS + x^2 where x^1 is 0, 5, 12 or 32, x^2 is null, DALI or M-Bus
Dwyer	AVPT	AVPT-X^1-X^2-X^3-X^4-B-X^5 where X^1 is S or H, X^2 is U or M, X^3 is 01, 02, 03 or 04, X^4 is C1, C2 or M1, X^5 is FC, NIST or null"
Ebtron	Gold Series GTC116e	GTC116e, GTC108e
Ebtron	Gold Series GTM116e	GTM116e, GTM108e
GEZE GmbH	GEZE Cockpit	GEZE Cockpit
GFR- Gesellschaft für Regelungs-technik und Energieeinsparung m.b.H.	ems5 building controller	ems5.CP05E
Global Control 5 S.A.	iSMA-B-AAC20 Series	iSMA-B-AAC20, iSMA-B-AAC20-D, iSMA-B-AAC20-M, iSMA-B-AAC20-LCD, iSMA-B-AAC20-LCD-D, iSMA-B-AAC20-LCD-M
Greystone Energy Systems Inc.	Horticulture Sensor	GH2WMx^{1}x^2, GH2SMx^{1}x^2, GH3WMx^{1}x^2, GH3SMx^{1}x^2 where x^1 is BB or CB, x^2 is XX, R1, or R2
Honeywell International	CentraLine EAGLEHAWK NX	CLNXEHx1x2x3100A, CLNXEHSERIESx2x3, where x1 is blank, P, S, x2 is 00, 14, 26, x3 is D, ND CLNXEH26ND100A-KIT
Honeywell International	CIPer30	WEB-C3036EPUBNH, WEB-C3036EPVBNH
Honeywell International	CIPer50	WEB-EAGLENX26D, WEB-EAGLENX26ND, WEB-EHSERIESNX26D, WEB-EHSERIESNX26ND WEB-EAGLENX26x^1, WEB-EHSERIESNX26x^1 where x^1 is D, ND
Honeywell International	HBS Comfort Point NX	CPNXEHPx^{1}x^{2}100A, CPNXSERIESx^{1}x^2 where x^1 is 00, 14, 26, x^2 is D, ND
Honeywell International	HBS Comfort Point NX	CPNXEHPx^{1}x^{2}100A where x^1 is 00, 14, 26, x^2 is D, ND
Honeywell International	Honeywell Enterprise Buildings Integrator	R600
Honeywell International	IQX12	IQX12-00100-0024A, IQX12-00050-0024A, IQX12P00050-0024A
Honeywell International	OEM Multivalent Controller NX	MVCNXEHx^{1}x^{2}x^{3}100A, MVCNXEHSERIESx^{2}x^3 where x^1 is P, S, x^2 is 00, 14, 26, x^3 is D, ND
Johnson Controls	Johnson Controls GLAS Thermostat	SiO_2-01000, SiO_2-01100, SiO_2-00100
Johnson Controls	SNE Series of Network Engines, SNC Series of Network Control Engines	M4-SNE10500-0, M4-SNE11000-0, M4-SNE110L0-0, M4-SNE22000-0, M4-SNC25150-0, M4-SNC16120-0, M4-SNC25150-04, M4-SNC16120-04
Lennox International	IntelliGen Refrigeration Controller	28918001
M2S Electronique Ltee	TX-COMMERCIAL-WIFI	TX120-WIFI
METZ CONNECT GmbH	BMT-Modules	BMT-x^{1}x^{2}x^{3}1108x^{4}x^5 where x^1 is F-, null, x^2 is Multi-I/O, TP, AI8, AO4, AOP4, CI4, DI10, DI4, DIO4/2, DO4, SI4, TO4, x^3 is -IP65, IP65 230 V, x^4 is 9313, 8813, 8213, 8513, 8713, 9013, 8113, 8413, 8313, 8305, 8613, 8913, 8013, x^5 is 70, 02, 0270, 32,3270, 19, 1970, 19IP, 26, 2670, 26IP, 21, 2170, null

NENUTEC ASIA PACIFIC PTE LTD 7030 Ang	NSVA VAV Smart Actuator	NSVA0000B, NSVA0000BL, NSVA0200B, NSVA0200BL, NSVA0222B
OEMCtrl	OptiCORE LS-1628u	LS-1628u
OEMCtrl	OptiCORE LS-CPU	LS-CPU
OEMCtrl	OptiCORE OEM Gateway	GW-1000
Phoenix Contact	ILC 2050 BI	ILC 2050 BI, Article No. 2403160 ILC 2050 BI-L, Article No. 2404671
Piscada AS	Piscada BAS	Piscada BAS 3.0
Samsung Electronics Co., Ltd.	b.IoT Server	AST-BL1A: b.IoT Lite, MST-BL1A: b.IoT Lite, AST-BS1A: b.IoT Standard, AST-BE1A: b.IoT Enterprise
SAUTER	BACnet native Client for SAUTER Vision Center	YZP480F000, YZP480F200, YZP480F999, YZP481F200, YZP481F210, YZP481F220, YZP481F230, YZP487F101
SAUTER	EY-modulo 6 Building Controller	EY6AS80F021
SE-Elektronic GmbH	BACnet Building Controller E-DDC	E-DDC2.3, E-DDC2.3M, E-DDC FG01, E-DDC FG01M, E-DDC3.2, E-DDC3.2 MOD, E-DDC3.2, RS232, E-DDC3.2 S, E-DDC3.3, E-DDC3.3 S, E-DDC3.4, E-DDC3.4 S, E-DDC4.0, E-DDC4.0 S, E-DDC5.0, E-DDC5.0 H, E-DDC5.0 S, E-DDC5.0 SH, E-DDC5.3, E-DDC5.3 S, E-DDC5.3 SH, E-DDC6.3, E-DDC6.3 PA, E-DDC-A4.3, E-DDC-B5.0, E-DDC-B6.0, E-DDC-B9.0, X-RUS2.1, X-RUS3.0, X-RUS3.1, GW-BC-SE, MC 700-SE, MODBUS-GATEWAY, ROUTER-BC, ROUTER-GSM, BACnet-SE, BACnet-SE-IP, DHBACNET
Shenzhen MEK Intellisys Pte Ltd	IoT/Smart Building/Network Controller	KXM-IP0080, KXM-16P, KXM-16P-D
Shenzhen MEK Intellisys Pte Ltd	IoT/Smart Building/Network Router	SG-100-BM, SG-100-BS1
Shenzhen MEK Intellisys Pte Ltd	IoT/Smart Building/Network Router	SG-100-B
Siemens	Compact actuating room automation station	DXR1.E02PLZ-112, DXR1.E09PDZ-112, DXR1.E09PDZ-113, DXR1.E10PL-112, DXR1.E10PL-113
Siemens	Compact actuating room automation station	DXR1.M09PDZ-112, DXR1.M09PDZ-113
Siemens	Desigo CC	V5.0
Siemens	Desigo Control Point	PXM30.E, PXM40.E, PXM50.E PXG3.W100-1, PXG3.W200-1
Siemens	Desigo DXR2 Automation Stations	DXR2.Ex^1x^2- x^3, DXR2.Mx^1x^2- x^3, where x^1 is 18, 11, 12, 10, 9, x^2 is null, P, PX, T, x^3 is 101A, 101B, 102A, 102B DXR2.E17C, DXR2.E17CX
Siemens	Desigo PXC3 Automation Stations	PXC3.E16A-100A, PXC3.E72-100A, PXC3.E72A-100A, PXC3.E75-100A, PXC3.E75A-100A
Strato Automation	BACplus-MSTP	BP848, B848
SysCom Automationstechnik GmbH	SB-BACnet	SB-BACnet
TCS	UbiquiSTAT	US4010, US4110, US4020, US4120, US4040, US4140, US4050, US4150
Trend Control Systems	IQX12	IQX12-00100-0024A, IQX12-00050-0024A, IQX12P00050-0024A

BACnet Topics Captured at 2020 AHR Expo

If you missed a BACnet International session at this year's AHR Expo, no worries. The sessions have been captured and are available online on The BACnet Institute educational site at www.thebacnetinstitute.org.

Session Title	Speaker
BACnet Edge Solutions - Ideal for IoT	**Roy Kolasa,** *Honeywell* **Pat Tessier,** *Honeywell*
This session will cover BACnet IoT Edge solutions and applications, considerations for design and specification, implementation, and success stories.	Roy Kolasa supports Open System Integration and New Product Development for Honeywell globally with over 25 years experience in the HVAC Controls Industry. Pat Tessier is the Global Offering Leader of Building Automation and Energy Services at Honeywell International helping to shape the controls industry by developing award-winning, innovative products that leverage the latest technology to meet customer's evolving needs.
HVAC as a Service – How soon is now?	**Lindsey Allen,** *MSA Safety*
By combining big data, analytics, and the Cloud, HVACaaS converts operational data into an untapped revenue opportunity for equipment manufactures. The subscription-based service allows manufacturers to connect field equipment to the cloud, enabling them to monitor their deployed systems and compare performance, load, etc. For building owners, this means reducing energy and maintenance costs.	Lindsey Allen is an experienced marketing professional with a demonstrated history of working in the information technology and SaaS industry. As Marketing Manager for Sierra Monitor, she oversees a broad range of department responsibilities including analyzing industry trends and demand for products and services, defining go-to-market strategies, guiding teams through product launch processes, as well as turning around underperforming products.
BACnet Physical Connectivity	**Coleman Brumley,** *Setra Systems*
In the world of BACnet, there are multiple options for physical connectivity. This session will explore the pros and cons of each connectivity option, including a look at the new secure connection, BACnet Secure Connect (aka BACnet/SC). We will also briefly explore how these different options can work in the world of B-IoT.	Coleman Brumley is currently a Senior Software Engineer at Setra Systems. With over 15 years of experience with BACnet, he was recently appointed Vice Chair of ASHRAE SSPC 135. Brumley served as convener of the ASHRAE SSPC 135 Internet Protocol Working Group for 7 years, and is the current convener of the Protocol Stack Working Group. Brumley is not only a product developer, but also a widely recognized speaker, teacher and contributor in multiple BACnet forums. He was the recipient of the prestigious 2015 Swan Award and the 2015 BACnet International Leader of the Pack St. Bernard Award. He has over 20 years of experience in database, communications and human interface technologies.

Design Considerations When Applying the BACnet Standard to a 'Smart Building' BAS	**Grant Wichenko,** *Appin Associates*
With a standard that is 1,374 pages in length, a BACnet BAS project can seem overwhelming. However, you don't have to learn all the details in the Standard; you need to focus on how the Standard helps you achieve the required project outcomes. In this presentation, Grant Wichenko will share design considerations that will ensure a more successful BACnet-based 'Smart Building' BAS integration	Grant Wichenko, P. Eng., is President of Appin Associates, a 40-year-old Consulting Engineering firm based in Winnipeg, Canada. Grant is actively involved with BACnet, serving as chair for the Applications Working Group of the SSPC-135, and as a member of both the SGPC-13 (DDC Guideline Specification) and ASHRAE 201P (Smart Grid) committees.
BACnet 101: An Introduction to BACnet	**Edward Tom,** *Yaskawa*
BACnet is a highly used open building automation protocol that continues to grow. This session will teach you about the basic building blocks and design philosophy that have made and continue to make BACnet so popular. Learn how BACnet can help you now and into the future as the Building Internet of Things (B-IoT) continues to grow.	Edward started from the ground up with his career. After graduating, he began as a field engineer getting his feet wet before moving on to become an application engineer and applying his degree with what he had learned in the field. This has provided him the ability to an effective product manager at one of the largest VFD manufacturers in the world.
While registration on The BACnet Institute educational site is required to access these sessions, it is free. Sessions are available in the Library section of the site. Please make sure to take advantage of the other educational resources available on the site as well.	

Calendar of BACnet International Events

2020		
November 12, 2020	BTL Working Group Meeting	Teleconference
December 3, 2020	BTL Working Group Meeting	Teleconference
December 17, 2020	BTL Working Group Meeting	Teleconference
October 5 – 7, 2021	PlugFest Interoperability Workshop	Durham, NH

Subject to change. For more information, contact David Nardone, BACnet International, david@bacnetinternational.org or visit www.bacnetinternational.org

BACnet International Journal 18

The BACnet International Journal is a global 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. Special attention is given to members and activities of BACnet International.

Online Distribution
The BACnet International Journal is posted to www.bacnetinternational.org and distributed to all members.

Editor
MarDirect Marketing Direct GbR
Bruno Kloubert
Responsible according to the press law
Aachener-und-Münchener-Allee 9
52074 Aachen, Germany
Phone: +49-241 88970-800
Fax: +49-241 88970-999
URL: www.bacnetjournal.org

Board of Directors
Andy McMillan, President and Managing Director, BACnet International
Dennis Swoboda, Chair, Blue Ridge Technologies
Erica Johnson, Vice-Chair, QA Cafe
Paul Bartunek, ABB
James Burke, Johnson Controls
Brad Hill, Honeywell International
Raj Jayaraman, Burton Medical
Raymond Rae, CopperTree Analytics
Nancy Stein, Siemens
Michael R. Wilson, Automated Logic

Publisher
BACnet International
2900 Delk Road
Suite 700, PMB 321
Marietta, GA 30067
Phone: 770-971-6003
Fax: 678-229-2777
info@bacnetinternational.org

Advertising
MarDirect Marketing Direct GbR
Phone: +49-241-88970-805
Fax: +49-241-88970-999
E-mail: vonhelden@mardirect.de

Picture Credits
BACnet International, MarDirect and specified companies

ISSN 2191-7825

BACnet International

Continually Raising Building Standards

BACnet International is an industry association that facilitates the successful use of the BACnet protocol in building automation and control systems through interoperability testing, educational programs and promotional activities.

ASHRAE BACnet™

BACnet is leading the world in Building Protocol Standard: It plays a significant role in building automation projects worldwide.

BACnet® TESTING LABORATORIES BTL

Achieving the Mark of Distinction: The BACnet Testing Laboratories (BTL) Mark provides users with assurance that a product has passed the industry standard BACnet conformance tests conducted by a recognized, independent testing organization. The BTL Mark is a mark of distinction, achieved by more than 900 products, that many building owners and control system designers look for as a must-have in order to be eligible for a project.

Discover More Today: **www.bacnetinternational.org**