ISSN 2191-7825

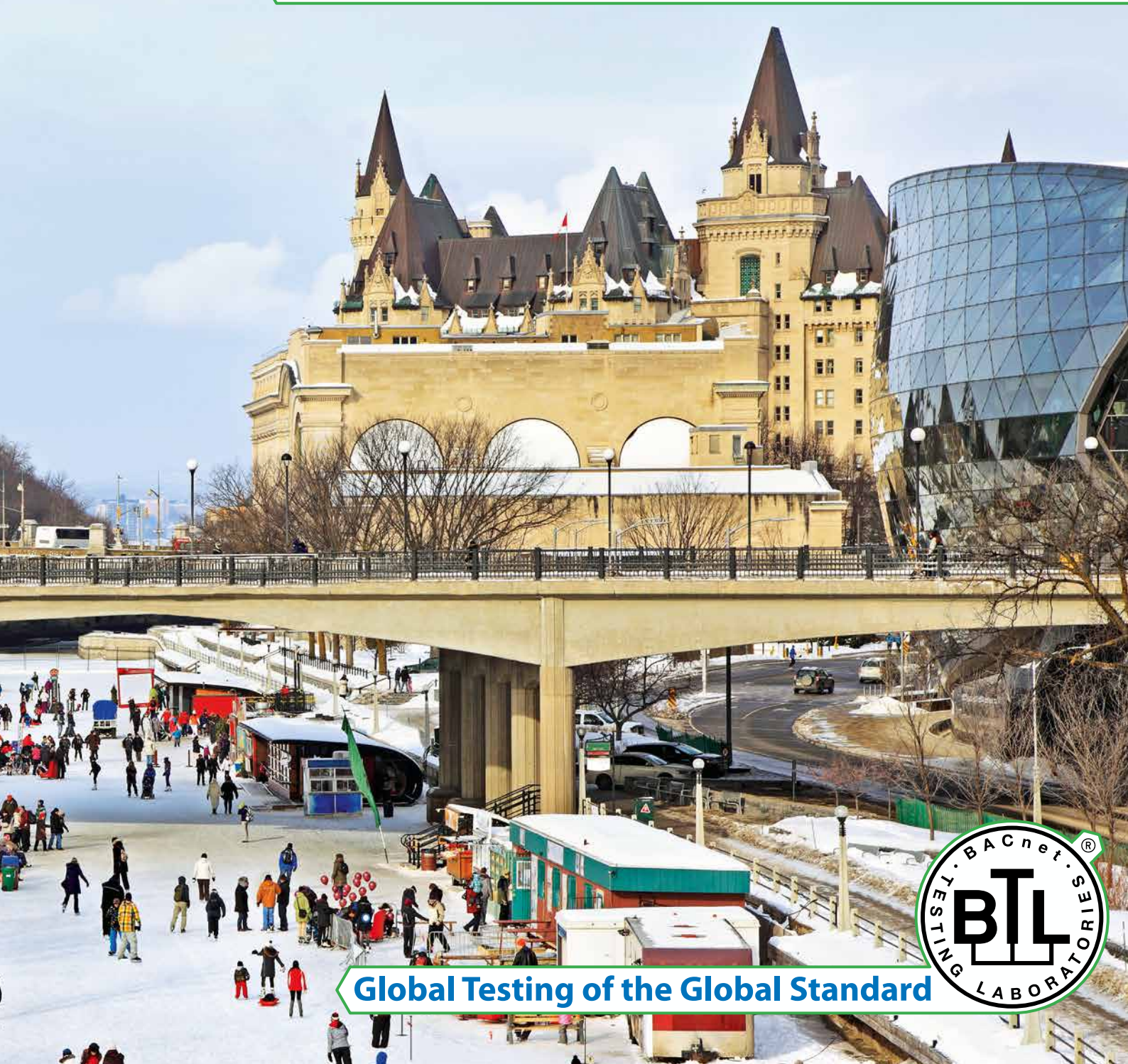
www.bacnetinternational.org

BACnet International JOURNAL

Issue 18

This Issue

BACnet Security: The Big Picture



Global Testing of the Global Standard

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

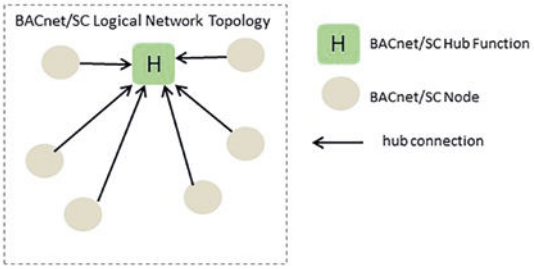


Figure 1 ©ASHRAE www.ashrae.org

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.

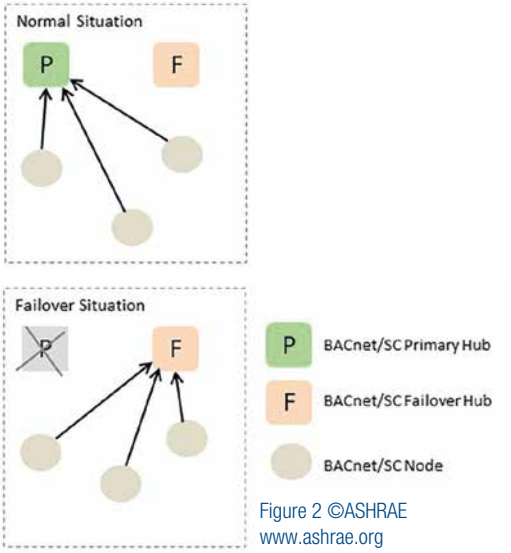


Figure 2 ©ASHRAE www.ashrae.org

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.

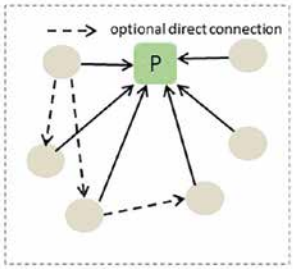


Figure 3 ©ASHRAE www.ashrae.org

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).

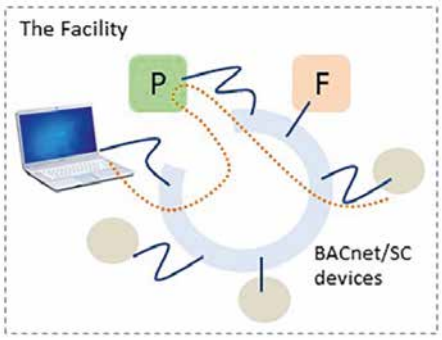


Figure 4 ©ASHRAE www.ashrae.org

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.

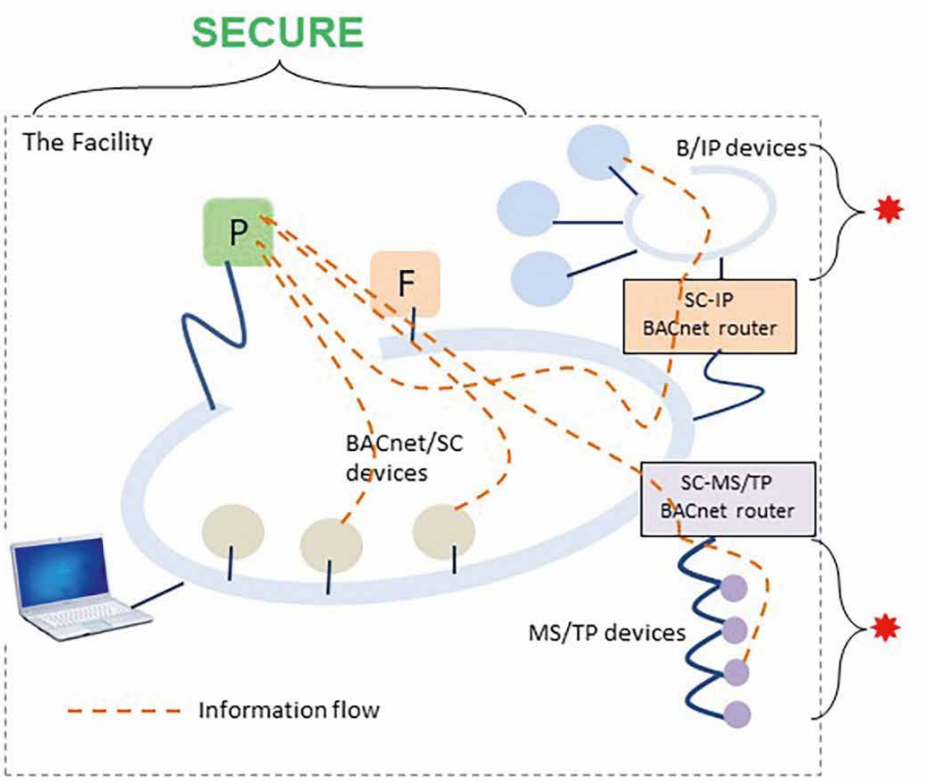


Figure 5 ©ASHRAE www.ashrae.org

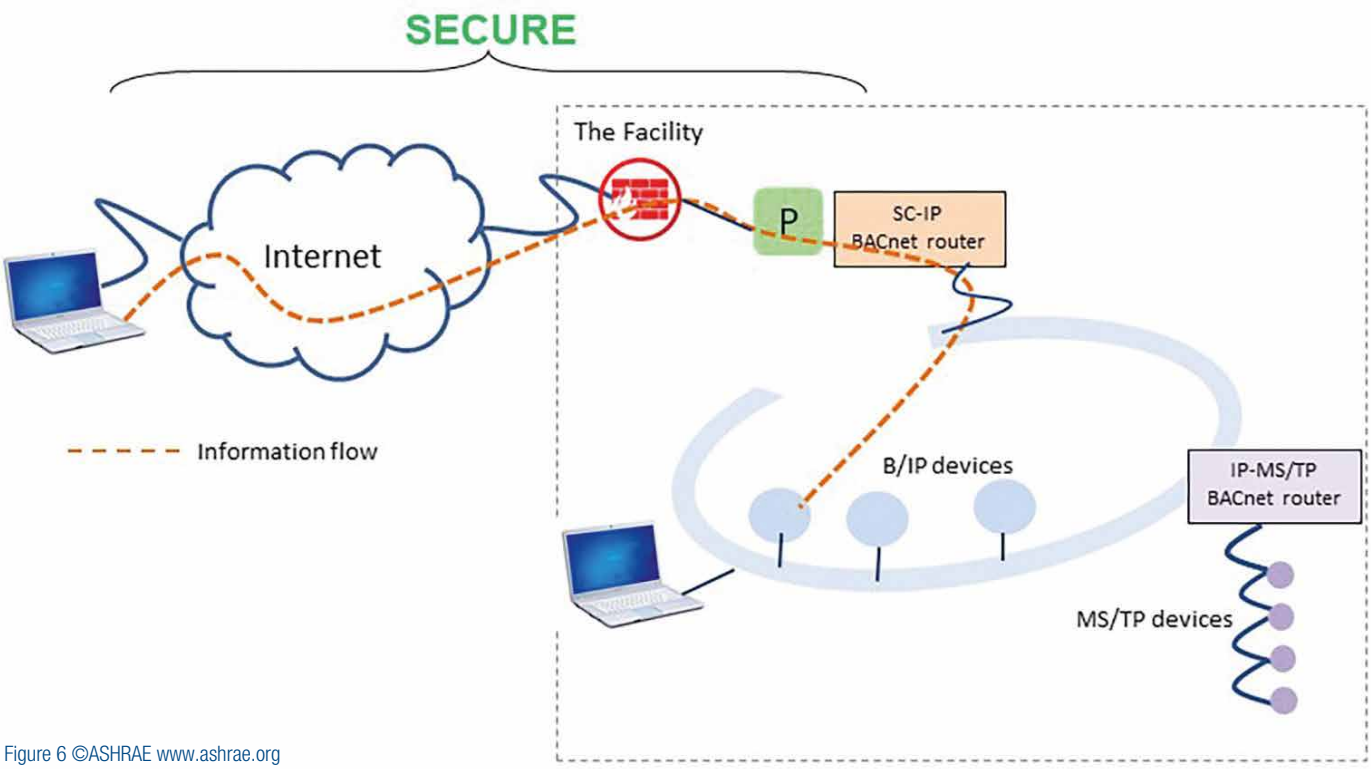


Figure 6 ©ASHRAE www.ashrae.org

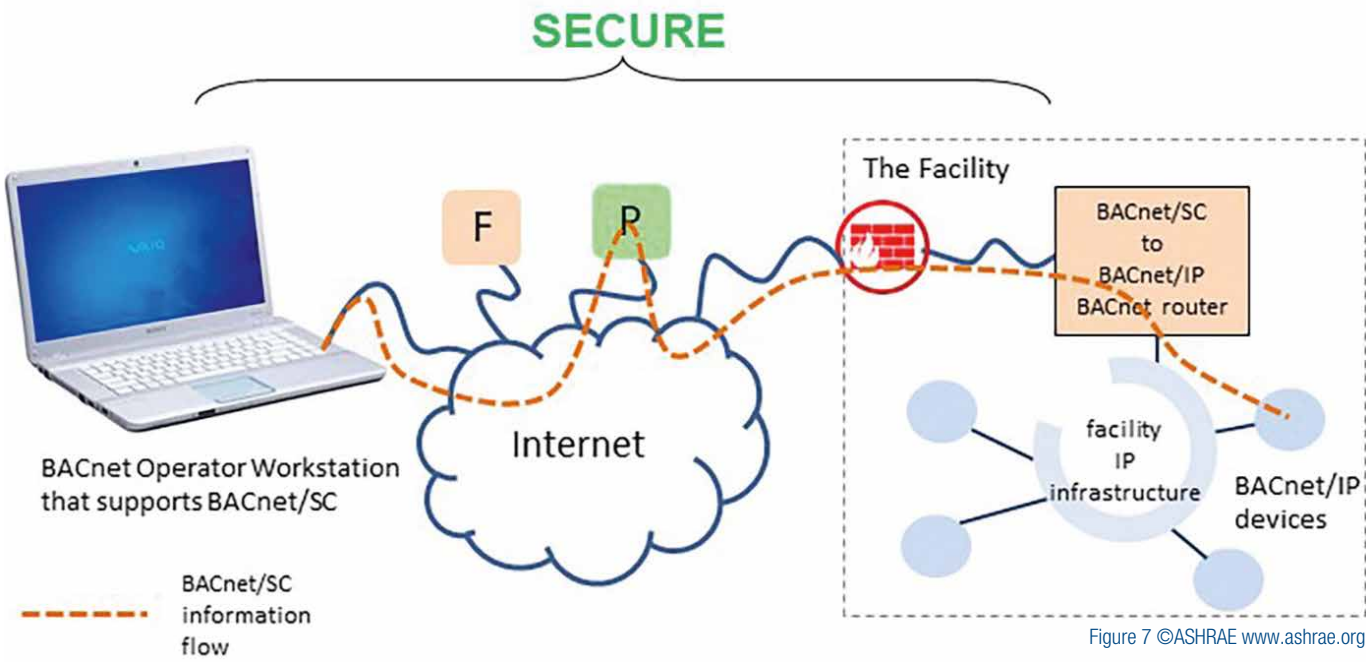


Figure 7 ©ASHRAE www.ashrae.org

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.