SbC Primer

Introducing *Secured by Cimetrics™ (SbC)*

As building control systems increasingly adopt Internet Protocol (IP) network technologies, the security of these systems is quickly coming under the microscope of corporate IT departments.

Regrettably, the BAS industry to date has not provided truly secure systems other than relying on decades-old isolation paradigms or securing systems using VLAN/VPN networks as their default "best practice."

As the benefits of BAS devices' use of enterprise networks become more apparent, this IT-unfriendly stance cannot continue if the industry is to deliver the value of data in BAS systems. Management of thousands of IP devices across vast property portfolios, with many that need the ability to interoperate, cannot be accomplished without a new approach to the problem.

The release of BACnet/SC (see ASHRAE white paper) adds a much-needed secure layer, but it does not address the problem of managing a vast number of devices as a holistic system.

This Primer introduces *SbC*, an industry-supported and vendor-neutral solution to the cybersecurity challenge. SbC proposes a framework that provides tools for BAS and IT stakeholders alike to secure systems and provide an interoperable way to manage smart buildings.

The seriousness of this challenge cannot be overstated.

- In the US, the average security breach has an impact of $8M, in addition to significant inconvenience and loss of goodwill to occupants when the usability of a facility is impacted.
- Satisfying the requirement of IT and cybersecurity departments is presenting the BAS channel with a challenge due to the incongruity between typical BAS skill levels and the inherent complexity of cybersecurity.
- The dominating BAS networking standard BACnet currently has no native cybersecurity protection; the recently released BACnet/SC is a significant move to secure BACnet devices but does not fully address system security.
- While some vendors are bringing proprietary security solutions to the market, these are generally not interoperable or scalable as they are often a patchwork of solutions, not a holistic approach.

What the industry needs is an industry-wide, interoperable, and resilient framework built on BACnet/SC to manage BAS/OT systems and devices securely, using IT infrastructure and best practices. Such a framework must work for the entire range of buildings - from small, single commercial buildings to multi-site global portfolios.

Such a framework, broadly supported by industry leaders, would achieve the following:

- Provide a consistent approach to cybersecurity that building owners and operators can rely on to provide their IT departments with the tools needed to take on the responsibility for cybersecurity.
- Significantly position the BAS industry as an active and responsible party in the battle against cyber threats to our buildings.
- Provide OEM vendors with a way to offer components, devices, and systems that are secure, manageable, and interoperable without resorting to proprietary mechanisms.
- Provide the tools, technologies, and best practices for installers of BAS systems to successfully sell, install, and maintain systems, rest assured that the systems conform to an industry-supported framework.

Over the course of 2020 to 2022, a group of industry leaders gathered to collaborate on creating such a framework. This work is now being brought to market as *Secured by Cimetrics*.

Working through the needs of device and system vendors, considering the requirements of IT organizations, and being sensitive to the demands of the BAS distribution channel, *SbC* is a framework to secure BAS systems from edge devices to the cloud.

- *SbC* is a mark trusted to bring all the necessary technologies and best practices together to ensure building systems are secure.
- *SbC* is designed with two key audiences in mind: BAS professionals and IT organizations. It provides a bridge between these groups that have a common goal of securing buildings.
- Built on, and abiding by the openness of the interoperable BACnet/SC standard from ASHRAE, *SbC* brings BACnet into the IT realm of today's cyber security-conscious enterprises.
- *SbC* goes beyond just securing BACnet/SC devices. The framework includes the secure management of past BACnet devices as well as non-BACnet devices commonly found in buildings today.

For Building Owners/Operators

Faced with post-pandemic challenges and grueling economic pressures, building owners and operators are also agonizing about the cybersecurity of their facilities.

Relying on both IT and OT departments is easier said than done. The two have different norms, tools, and conflicting objectives; IT's prioritization is on the Confidentiality, Integrity, Availability (CIA) triad, while OT's is on Availability, Integrity, and Confidentiality (AIC).

In today's paradigm, you, the building owner/operator, are bearing the risk of cybersecurity attacks, where the damage to operation, business, and reputation from a cybersecurity breach can be significant.

In reality, no one person in your organization is accountable for the cybersecurity of your buildings.

The impact of this reality is significant:

- The cost of a security incident is estimated at $8M for a successful breach (US).
- Ask your IT department if they have visibility of OT devices in your building. Chances are they do not.
- OT's priority on the availability of *your* facility can lead to the installation of unsanctioned networks and devices not under the auspices of IT, increasing your risk.

Because of the above, incident detection often falls between IT and OT responsibility areas, a critical follow-on response and recovery activities to attacks is often incongruous with your risk mitigation objectives.

By providing management tools and best practices that solve both IT and OT challenges collaboratively, you can manage and reduce your cybersecurity risk, and minimize the potential disruptions to your building.

For more than two decades, the building automation industry has widely adopted BACnet as the standard for devices, networks, and systems. Your buildings are likely to have a significant number of BACnet devices today.

Enter *Secured by Cimetrics*

SbC is a security management framework conceived by industry collaboration to enable both IT and OT stakeholders to holistically manage BAS/OT devices using IT tools and best practices.

SbC bridges the IT/OT gap while reducing complexity and risk, and future-proofing your buildings.

SbC is an open industry-created framework that promotes competition to give you choice and manage your costs.

SbC gives IT departments the tools to secure OT devices, and OT departments the tools to securely manage their devices according to IT/CISO policies.

For Specifying Engineers

For decades, specifying engineers have become a critical part of the design and installation of smart BAS devices/systems in smart buildings.

Over the years these systems have become increasingly more complex and have continually stretched the traditional skillsets of specifying engineers.

There is no subject as critical for buildings as security from cyber threats, and there is nothing more important than for specifications to include language that protects such systems from cyber breaches.

It falls to specifying engineers to include specification language to ensure systems are secure. Without this, the reliability of building automation systems cannot be assured, and the building is at risk over its lifetime.

The reality is that engineers must satisfy IT departments regarding the cybersecurity of systems they specify.

Consider the following challenges:

- IT departments now demand a comprehensive approach to how BAS systems are secured as part of control/automation specifications.
- The complex and ever-changing cyber landscape makes highly prescriptive and granular specifications impractical.
- Cybersecurity risk mitigation is no longer a nice-to-have, it is essential for all specifications.

By recognizing an industry-wide interoperable and resilient cybersecurity framework to manage buildings, you can ensure you are specifying the best technology and practices that would be accepted by IT and BAS implementers alike.

A broad industry-wide framework ensures BAS security is based on the latest technology and best practices. Such a framework provides for an easy-to-use specification language and guidance for holistic security.

A secure and interoperable framework would encourage system vendor competition and future-proof buildings you specify by mitigating the risks to you, contractors, installers, owners, operators, and IT departments.

***SbC* helps to secure the systems you specify.**

Specify *SbC* as a framework to interoperably secure BACnet-based control and automation systems.

SbC is an industry-backed, multi-vendor framework to secure BAS networks, ensuring the core interoperability tenet of BACnet.

SbC is designed to satisfy the needs of BAS installers and IT departments alike.

SbC leverages you and the industry's familiarity with BACnet, the ASHRAE standard for automation and control with IT standards.

For the BAS Channel

Sellers and installers of building control and automation systems see first-hand the opportunities that come from adopting IT-based systems: remote management, integration, analytics, energy efficiency, and much more.

Channel professionals also see the challenges IT-based systems bring, especially protecting such IP networks from cyber-attacks to corporate information systems.

It is common to have IT department staff be gatekeepers in the installation of any networks that touch corporate information infrastructure. They are part of project meetings from day one!

While some organizations are ramping up expensive and hard-to-find IT skills, the fast-moving cybersecurity landscape makes it hard to counter IT/CISO professionals whose job it is to be very well informed and demanding.

What if you can turn IT gatekeepers into strategic assets to help you?

Consider the following:

- Channel sales staff are now required to propose their solutions to IT departments from the start.
- Typically, less than 5% of BAS channel staff have adequate IT credentials/experience.
- Aggressive IT integrators are bidding and winning projects, relegating you to a sub-contract role.
- You are responsible for the security of systems you install for many years beyond handoff.

Using an industry-wide BACnet managed framework that secures devices/systems to the demands of IT, while addressing the need to manage BAS, is the best way to secure projects with existing skills, use labor efficiently, return a healthy bottom line, and minimize risk.

This approach will enable you to lead the conversation with security and make conversations with IT easier.

This approach leverages the value of BACnet, removing the reliance on proprietary solutions in a way that IT professionals would consider secure.

Secured by Cimetrics **is <u>your</u> strategic asset.**

SbC provides retrofit opportunities to secure older BACnet devices, non-BACnet systems and an opportunity to grow your business into the profitable IT landscape.

SbC mitigates ongoing cybersecurity risks for your organization and your client's buildings.

SbC provides IT-centric white papers and collateral validated by both the BAS and IT industries.

SbC provides guidance and specs on selling and implementing secure multi-vendor BACnet systems.

SbC enables easy and secure access to BAS data for analytics, FDDO, integration, and other purposes.

For IT Organizations

With the proliferation of IP BAS/OT devices in buildings comes the task of managing and mitigating a new attack vector through these networks that comprise thousands of devices, often in hard-to-reach locations of facilities.

Many OT installers resort to installing Internet-accessible shadow networks, creating new attack surfaces and challenges to IT/CISO departments, often for decades.

IT departments have the responsibility and accountability for the security of these BAS/OT networks, but seldom do they have the tools or resources to manage their risks.

This is a significant risk for building owners/operators, expecting IT to take on a task they are not equipped to do.

What if the security of BAS/OT devices can be managed using standard IT tools and processes?

Such a new approach would provide the following:

- Mitigation of OT security attack surfaces from devices not previously detectable by IT tools.
- Enables IT departments to manage IP addresses needed by OT using existing network tools.
- Significantly reduce BAS/OT-related UDP broadcast traffic and unwanted network storms.
- Remove the need for parallel and risky OT networks not managed or sanctioned by IT.
- Use of firewall-friendly encrypted TLS as the network transport protocol.

Managing OT cybersecurity using a framework designed for IT enables you to use IT technologies, practices, and policies based on the NIST Framework to identify, protect, detect, respond, and recover from OT breaches.

Such a framework has to be built on commonly used IT protocols such as TCP/IP with TLS and DHCP. The framework must also integrate with SIEM, SOAR, and Syslog tools that are in place today at IT departments.

Such a framework must provide control of BAS/OT devices, including risk profiles and the ability to isolate suspicious segments in cooperation with BAS staff.

Such a framework provides layers of security, in-depth strategies, and complements IT measures such as NGFW and VPN/VLAN, which are adopted by most enterprises.

Using *SbC* to manage BAS/OT

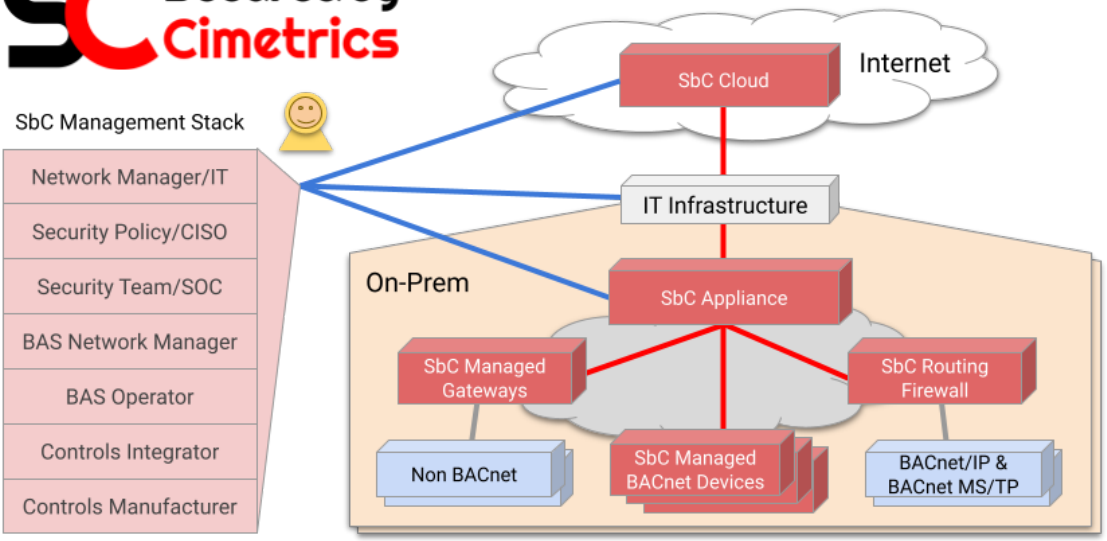
SbC is an industry-wide framework supported by all major vendors in the BAS/OT industry.

SbC isolates and manages BAS/OT systems on IT infrastructure using modern IT techniques.

SbC integrates with SIEM, SOAR, and other tools on-prem and/or in the cloud.

SbC provides peace of mind and mitigates risks.

Secured by Cimetrics



Architecture Components

The simplified architecture of *Secured by Cimetrics* is shown above. The key elements are:

***SbC Managed BACnet* Devices**: BACnet/SC devices with an added layer enabling them to be managed.

SbC Appliance: On-prem device or software responsible for the management of devices.

SbC Routing Firewall: Provides a way to securely bring BACnet/IP and MS/TP into the security framework.

***SbC Managed* Gateways**: These provide a way to securely manage gateways to non-BACnet devices.

SbC Cloud: An Internet-based tool to remotely manage multiple SbC sites.

Key Features

- Secure device onboarding
- Device certificate management
- Asset management & IAM
- Management of routing firewall policies
- Network & security configuration
- Device backup &restore
- Server/controller recovery
- Version/firmware tracking
- IT integration (SIEM, SOAR, etc.)
- Authentication & authorization
- Legacy BACnet (IP and MS/TP) migration
- Securing Non-BACnet devices
- IT standards (TCP, TLS 1.3, and WebSockets)

Interoperable • IT Secure • Scalable

Secured by Cimetricks is an industry-wide, interoperable, and resilient framework to manage BAS/OT systems and devices securely, using IT infrastructure and best practices from small single commercial buildings to multi-site global portfolios.

Secured by Cimetrics is an outcome of consensus building collaboration with

Automated Logic
Cimetrics
Delta Controls
Honeywell HBS
Johnson Controls
Padi
Schneider Electric
Siemens Smart Infrastructure
Trane Technologies

securedbycimetrics.com • sbc@cimetrics.com