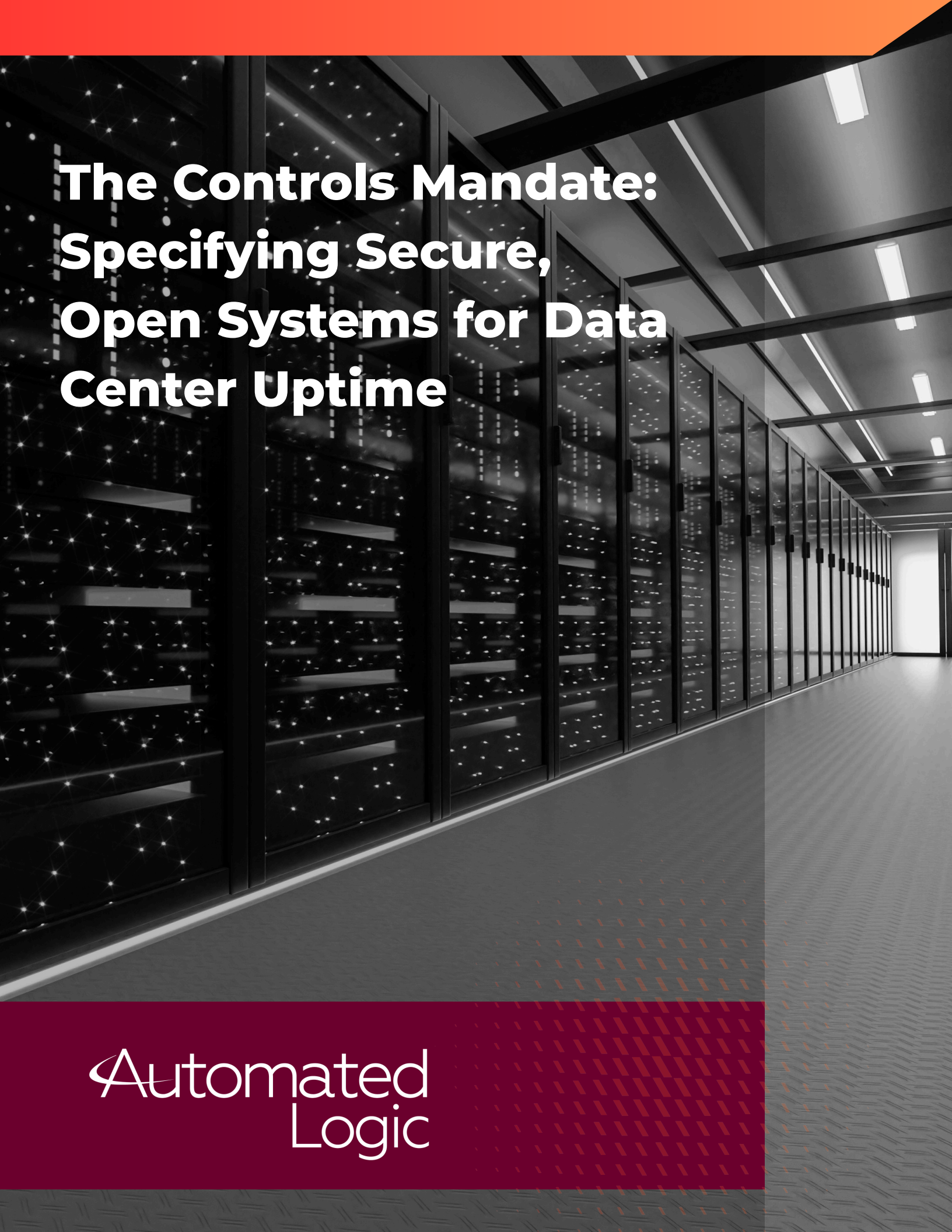


The Controls Mandate: Specifying Secure, Open Systems for Data Center Uptime

Automated Logic

According to a comprehensive 2025 study analyzing over 467,000 building management systems (BMS) across 500 organizations, three out of four companies operate facilities vulnerable to cyberattacks, often due to insecure internet connections tied to known ransomware exploits.[i] In mission-critical environments like data centers, where even a momentary loss of environmental control can lead to catastrophic logical downtime, this statistic underscores a vital reality: the era of the “air-gapped” operational network is definitively over.

To support long-term value and operational integrity, specifiers need a unified approach to building automation that champions open standards and resilient cybersecurity. BACnet Secure Connect (BACnet/SC) is designed to serve as that foundational standard. Advanced, secure networking architectures, guided by evolving frameworks like BACnet Secure Connect (BACnet/SC), offer a roadmap for this standard. This playbook explores the technical and operational benefits of specifying secure, scalable network architectures that protect your clients' investments for decades to come.

3 out of 4 companies are vulnerable to cyberattacks.[i]

Automated Logic

[i] Burns, J. (2025, June 26). Most building management systems exposed to cyber vulnerabilities, experts warn. Facilities Dive. https://www.facilitiesdive.com/news/most-building-management-systems-exposed-to-cyber-vulnerabilities-experts/751756/

1. The Cybersecurity Imperative in Mission-Critical Environments

Historically, building automation systems (BAS) operated on isolated, serial networks. Today's high-performance facilities demand deep IP-level integration to function efficiently, aggregate analytics, and optimize cooling loads. While this interconnectedness unlocks incredible data visibility, it simultaneously broadens the attack surface. Traditional building protocols were built for interoperability, not security, often transmitting data in cleartext across the network.

Modernizing this infrastructure requires addressing vulnerabilities at the protocol and routing levels. Rather than relying entirely on traditional IT infrastructure, such as complex VPNs or isolated subnets, to hide unencrypted BAS traffic, the industry is shifting toward architectures that inherently protect data in transit. Utilizing advanced encryption and strict certificate-based authentication helps establish highly secure communication tunnels between critical devices.

By demanding explicit, certificate-level authentication for every single device attempting to join the network, this protocol is designed to significantly mitigate unauthorized access. This architecture actively reduces the likelihood of the BAS becoming a "soft" entry point into the wider corporate network, a critical consideration for data centers housing highly sensitive client data.

Actionable Insight

Require native encryption and certificate-level authentication in your next Request for Proposal (RFP) for critical IP-level network controllers. Explicitly state that the automation platform must support streamlined device onboarding without placing undue burden on the IT department.

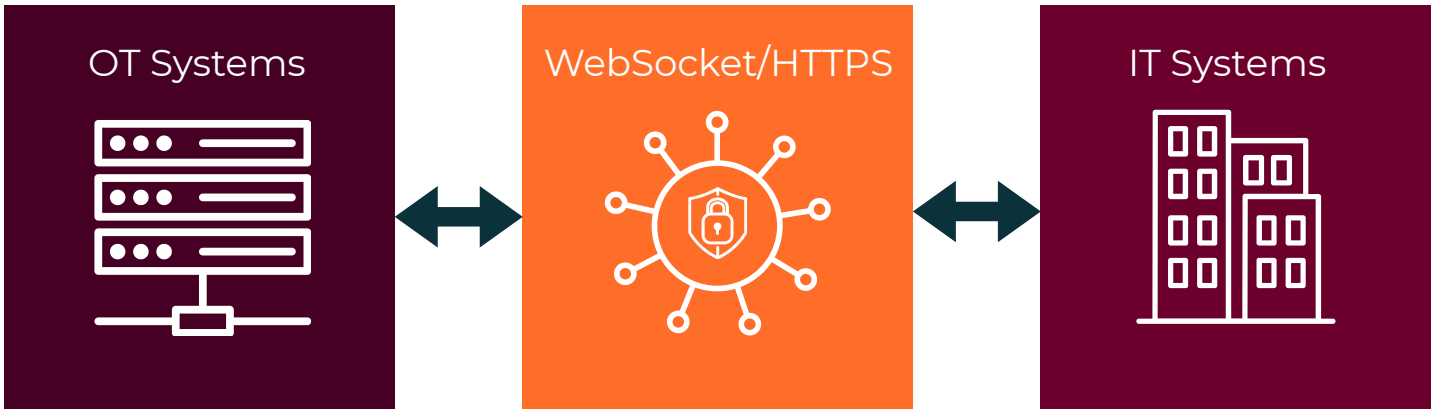
2. Bridging the IT/OT Divide with Simplified Specification

One of the most persistent bottlenecks in modern data center construction and retrofitting is the friction between the facility's OT engineers and the corporate IT security team. Traditional BACnet/IP relies heavily on network behaviors that IT professionals typically restrict. It requires complex configurations, such as UDP broadcasts, BACnet Broadcast Management Devices (BBMDs), and static IP allocations across multiple subnets, which routinely conflict with strict, zero-trust IT security policies.

BACnet/SC fundamentally alters and simplifies this dynamic. By routing communications through standard WebSockets, BACnet/SC traffic appears to the enterprise network as standard, outbound HTTPS web traffic (port 443). This elegant shift eliminates the need for dedicated VLANs, complex routing tables, or firewall exceptions just to achieve basic communication between control modules.

For specifiers, this translates to a vastly simplified specification and deployment process. IT departments readily understand and approve WebSocket architectures. By speaking the language of IT, modern control networks clear the path for rapid, conflict-free deployment, keeping mission-critical projects on schedule.

Simplified IT Integration Architecture



Encrypted Outbound HTTPS (443)

Actionable Insight

During the schematic design phase, schedule a joint working session with the client's IT and facilities teams. Position control architectures that utilize standard outbound web traffic as the baseline architecture to secure early IT buy-in, clearly demonstrating how it respects their firewall policies while delivering OT functionality.

3. Future-Proofing Investments and Advancing ESG Goals

Specifying a BAS is a strategic decision that heavily impacts a data center's lifecycle value, energy footprint, and Power Usage Effectiveness (PUE). As organizations increasingly prioritize stringent ESG (Environmental, Social, and Governance) reporting, the underlying network must be robust enough to support advanced, data-heavy sequences of operation, such as ASHRAE Guideline 36, which optimizes HVAC efficiency.

True futureproofing, however, extends beyond simply adopting the latest software iteration; it requires an architectural philosophy rooted in backward compatibility. A top-tier automation platform protects prior capital investments by allowing multi-generational hardware to coexist harmoniously on a modern, secure network.

Rather than forcing a costly and disruptive full-system rip-and-replace, specifiers can design systems where highly functional legacy equipment is bridged securely into a new BACnet/SC backbone using advanced routing hardware. Beyond the immediate capital expenditure of new controllers, forced system overhauls introduce massive hidden costs: extensive labor for rewiring, complex software reprogramming, and the severe financial risk of scheduled downtime in a mission-critical environment. An agnostic, standards-based approach can potentially reduce lifecycle costs and limit electronic waste, all while allowing the facility to continuously adapt to evolving energy goals and hardware innovations.

Actionable Insight

Audit the client's existing operational technology portfolio to identify viable legacy equipment. Specify a phased modernization plan where advanced control routing securely bridges older MS/TP or BACnet/IP networks into a centralized modern architecture, protecting the initial capital investment while modernizing the security posture.

4. Empowering Operations Through Advanced Visibility

While robust encryption and simplified IT integration lay the necessary architectural foundation, the ultimate success of a building automation system relies heavily on the people tasked with operating it. Data center facility teams working under high pressure need more than just secure data; they require immediate, actionable intelligence to maintain uptime.

To maximize the value of an open, secure network, the most advanced platforms drive operational efficiency via sophisticated visualization. Intuitive point-and-click navigation, high-definition factory-generated graphics, and real-time thermographic floor plans empower operators to act quickly and confidently.

In a data center context, this is invaluable. When an operator can instantly visualize thermal anomalies, such as a hot spot developing in a high-density server aisle, through clear, standardized graphical interfaces, they can accelerate troubleshooting and optimize cooling deployment before a critical threshold is breached. The technology acts as a force multiplier for the operator, transforming complex, encrypted network data into decisive, day-to-day operational actions.

Actionable Insight

When evaluating BAS vendor capabilities, mandate a live, hands-on demonstration of their operator interface. Prioritize systems that offer out-of-the-box thermographic floor plans and highly intuitive navigation to significantly reduce operator training time and accelerate critical incident response.

Conclusion

By adopting an open, secure framework like BACnet/SC, design engineers and specifiers provide data center clients with strategies that challenge competitors and rank among the most advanced in the industry. This approach simplifies IT integration, protects multi-generational investments through backward compatibility, and ultimately creates a secure, highly visual, and scalable foundation for the mission-critical facilities of tomorrow.

Automated Logic

Find a Dealer:
https://www.automatedlogic.com/dealers

1150 Roberts Boulevard, Kennesaw, Georgia 30144
770-429-3000 | automatedlogic.com | A Carrier Company

v05/26