Carrier

iVu

Carrier Technical Guide

A Modern Guide to Securing Building Automation Systems (BAS)

The New Frontier of BAS Security

The Challenge of Convergence

The modern commercial building is a sophisticated network where operational technology (OT)—such as HVAC, lighting, and security systems—is increasingly interconnected with information technology (IT) infrastructure. This convergence, while offering powerful benefits like enhanced efficiency and centralized control, also presents a complex and evolving cybersecurity landscape. For specifiers and IT professionals, the challenge is clear: how to design a building automation system (BAS) that is not only high-performing and efficient but also fundamentally secure.

According to Fortinet's 2024 State of Operational Technology and Cybersecurity Report, the study indicates that 73% of organizations experienced security intrusions impacting their OT systems, a figure that has increased from the prior year's report.[i] This trend underscores the industry's growing recognition that protecting building automation systems is crucial for safeguarding the broader enterprise network. This guide provides a technical framework for achieving this BAS security, focusing on network segmentation and the critical role of a specialized network router.

73%

of organizations experienced security intrusions impacting their OT systems in 2024, an increase from 49% the previous year.[i]

The Evolving Threat Landscape

The integration of BAS with corporate networks may increase the overall attack surface, potentially introducing new vulnerabilities. In certain situations, a cyberattack targeting a building's systems could result in more than just a data breach; it might interfere with building operations, affect occupant safety, or disrupt business continuity. To help reduce these risks, organizations should consider implementing a proactive and comprehensive BAS security strategy designed to support both operational resilience and data protection.

Carrier

[i] 2023 State of Operational Technology and Cybersecurity Report. (n.d.). https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

The Principle of Network Segmentation

What is Network Segmentation?

Network segmentation is a core cybersecurity practice that involves dividing a large network into smaller, isolated sub-networks. In building automation, the most critical segmentation is between the IT network (the primary customer network) and the OT network (the building automation network). This strategic separation, implemented via a router, creates a digital "firewall" that is essential for a robust BAS security framework.

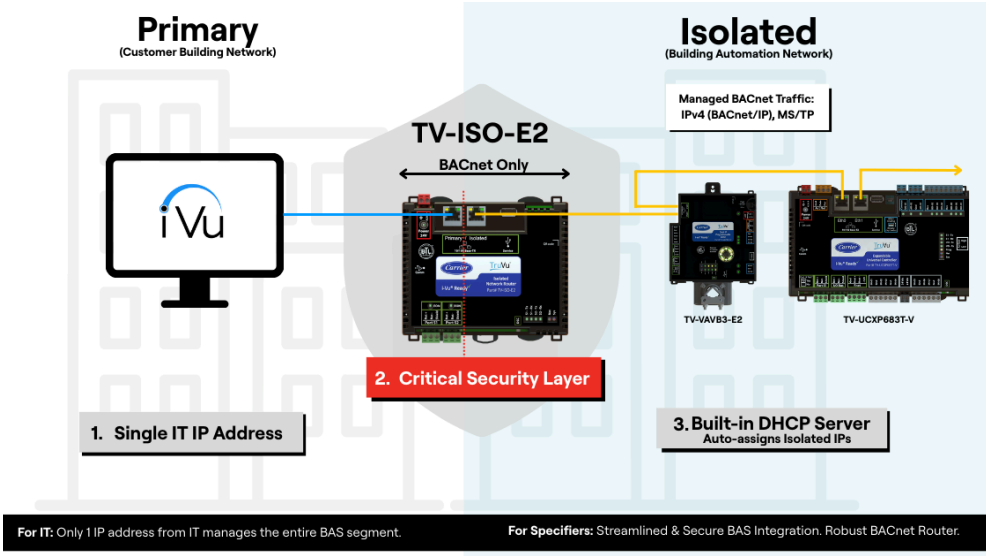
Benefits of Segmentation

Threat Containment: By isolating the OT network, a BAS security breach on one side cannot easily spread to the other. This containment is intended to minimize the potential damage from a cyberattack, helping to keep it from compromising critical infrastructure or sensitive corporate data. Actual results may vary depending on system configuration and implementation.

Reduced IT Complexity: A segmented network simplifies IT management by requiring only a single IP address from the customer's network to connect to all devices on the isolated network. This may reduce administrative overhead and may help streamline network policy enforcement.

Enhanced Performance and Reliability: By isolating building automation traffic, the router can manage communication more efficiently, ensuring that critical control commands are not delayed by other network activity. This may improve system response times and contribute to overall operational reliability.

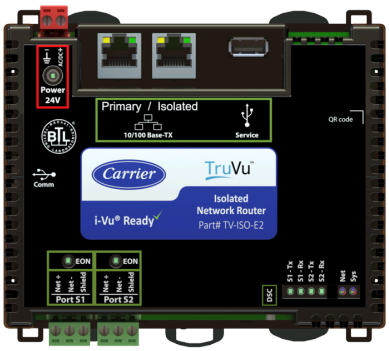
Actionable Insight: When drafting specifications, consider including a recommended requirement for a layered cybersecurity framework. It may be beneficial to highlight that the proposed solution should demonstrate the ability to integrate securely with the existing IT infrastructure while minimizing the risk of introducing new vulnerabilities. For IT teams, adopting a policy that restricts IT-facing devices on the OT network to a single point of entry, such as a router can help streamline BAS security management and reduces the number of potential attack vectors requiring oversight.



The Isolated Network Router: A Technical Deep Dive

A key piece of hardware in this architecture is a specialized router, like the Carrier TV-ISO-E2, which functions as a central hub for various building protocols. It allows for powerful integration capabilities across various environmental, energy, security, and safety systems into a single, unified platform.

Carrier TV-ISO-E2: A Specialized Router for Secure Integration



Technical Specifications

- **Part Number:** TV-ISO-E2
- **Power Requirements:** The device operates on either 24 Vac (±10%, 50-60 Hz, 50 VA) or 24 Vdc (±10%, 18 W).
- **Memory:** It is equipped with 8 GBs of eMMC Flash memory (120 MB available) and 512 MB of DDR3 RAM. User data is regularly archived to non-volatile Flash memory to help minimize data loss. The real-time clock can track time for up to 3 days in the event of a power failure.
- **BACnet:** Conforms to the BACnet Router (B-RTR) and BACnet Broadcast Management Device (B-BBMD) profiles as defined in Annex L of the BACnet standard. The device is certified to the BACnet standard ISO 16484-5 protocol revision 1.19 and protocol revision 19 (135-2016). Please see BTL listing page.
- **BACnet Secure Connect (BACnet/SC):** Supports BACnet/SC, utilizing TLS encryption over WebSocket connections for secure, IT-compliant communication. The device can function as a BACnet/SC Hub or Node to secure data transmission between networks. Support details are confirmed via the BTL listing page. Actual compatibility may depend on specific deployment requirements.
- **Compliance:** The router is compliant with multiple standards, including FCC, UL (UL916, UL864), Industry Canada, and CE/UKCA, demonstrating a commitment to meeting safety and performance requirements. Compliance should be verified for each installation.
- **Physical Dimensions:** The device has a compact footprint, with overall dimensions of 5.51 in. (14 cm) in width and 5.88 in. (14.93 cm) in height, designed for easy installation and to optimize control panel space. It weighs 0.75 lbs. (0.3402 kg).

Actionable Insight: When specifying a router, consider selecting one that is BACnet-compliant and listed to the most recent available protocol revision. This may support system adaptability and help facilitate integration with a wide range of devices. For IT teams, it may be beneficial to evaluate routers that indicate compliance with multiple standards, such as UL916 and UL864, as these certifications can reflect alignment with energy management and smoke control safety standards, which are important factors in a building's overall safety planning.

Router Features for Enhanced BAS Security and Integration

The isolated network router can provide a strong foundation for building automation by offering a suite of features designed to support BAS security, streamline deployment, and enhance performance.

Network Security Support: The router may function as a firewall, helping to establish a BAS security layer that separates the building automation network from the broader customer network. This architecture is intended to reduce the risk of unauthorized access and assist in mitigating cyber threats.

IT Friendly Design: By requiring only, a single IP address to connect to all devices on the isolated network, the router may help reduce administrative overhead and simplify network policy management for IT teams.

Simplified Deployment: A built-in DHCP server can automatically assign isolated IP addresses, which may ease network configuration and contribute to shorter installation time.

Routing Capability: The router is designed to support BACnet communication across common network types, including BACnet/IP, BACnet Secure Connect (SC), and MS/TP, helping promote compatibility with both current and future infrastructure.

Flexible Network Connections: The router includes one primary Ethernet port for IP/Ethernet/SC communication, one isolated Ethernet port for BACnet/IP, and two EIA-485 ports for BACnet MS/TP networks.

Actionable Insight: When specifying a router, consider one with a built-in DHCP server. This feature may help simplify installation and commissioning by automatically assigning IP addresses, potentially reducing labor costs and the risk of configuration errors. During network design review, evaluate whether the router architecture requires only a single IP address from the corporate network; this can be a useful indicator of a segmented network that may ease IT management.

Simplified Commissioning and Advanced Diagnostics

The router is designed to support both BAS security and user-friendly operation, with features that may assist in efficient troubleshooting, an important consideration for long-term system performance.

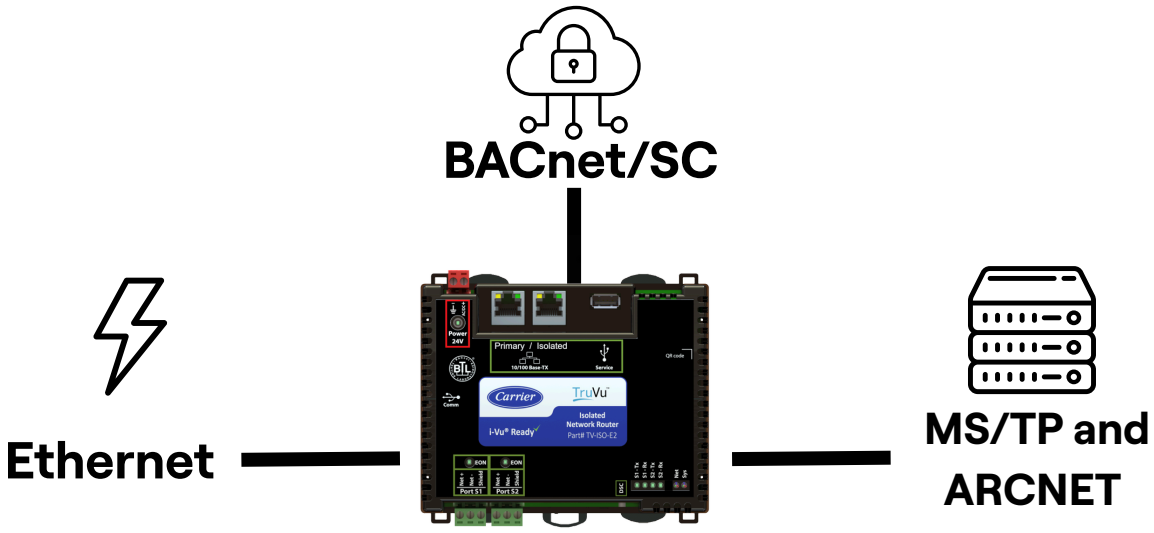
Configuration and Recovery: A dedicated USB port enables local, secure connection to a computer, which may simplify system setup and troubleshooting. This port is also compatible with Equipment Touch and wireless service adapters.

Diagnostics Capabilities: The router is designed to capture and store network data and statistics, which can be useful for troubleshooting and performance optimization.

Router Addressing: The device may be configured via a webserver interface, offering convenient access for setup and adjustments.

LED Status Indicators: The router includes multiple LED indicators, such as Tricolor NET and SYS LEDs for network and system status, POWER, S1 EON, S2 EON, and separate TX (Transmit) and RX (Receive) LEDs for each EIA-485 port, providing visual feedback on operational status.

Actionable Insight: When specifying a system, consider selecting one that offers diagnostic tools, such as network data capture and performance statistics. These features may support efficient troubleshooting and system optimizing post- installation. It may also be beneficial to ensure the system includes a dedicated service port, such as a USB port, for secure, local access. This can help facilitate direct troubleshooting without relying on broader network connectivity, which may be subject to additional security considerations.



Optimizing BACnet Communication

For building automation systems, efficient and reliable communication is a key consideration. The router includes features that are intended to support the optimization of BACnet traffic and enhance overall network performance.

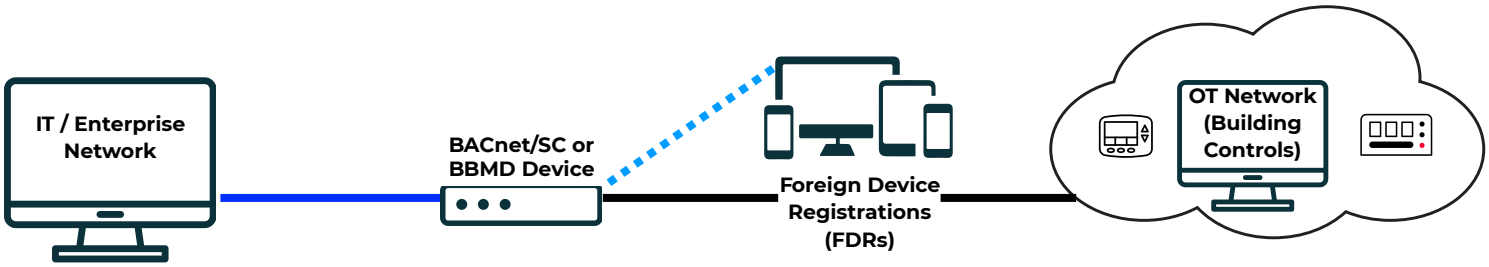
Broadcast Communication Support: The router is designed to function as a BACnet Secure Connect (BACnet/SC) device or BACnet Broadcast Management Device (BBMD), which are commonly used to help manage broadcast communication on BACnet/IP networks. In these roles, the router may assist in reducing network traffic, potentially improving response times, and contributing to a more stable system environment.

BACnet Device Integration: The device supports Foreign Device Registration (FDR), a feature that facilitates the discovery and registration of third-party BACnet devices. This capability may help streamline communication within the BACnet network and simplify integration efforts.

Communication Ports: The router includes high-speed EIA-485 ports capable of communicating with BACnet MS/TP networks at speeds ranging from 9,600 to 115,200 bps. The "End of Net termination" setting can be configured to "Yes" to assist in properly terminating the network segment, which may support reliable communication.

How a BACnet Broadcast Management Device (BBMD) Works

Manages broadcast messages and prevents them from flooding the network.



Actionable Insight: When developing specifications, consider including support for BACnet Secure (BACnet/SC) device or BACnet Broadcast Management Device (BBMD) functionality. These features are commonly used to help manage network traffic more efficiently and may contribute to a responsive, stable system, particularly in larger or more complex networks. It may also be beneficial to evaluate systems that support Foreign Device Registration (FDR), which can assist in streamlining the integration of third-party BACnet devices and potentially reduce the time and cost involved in expanding or upgrading the building automation system.

U.S. and Canadian Cybersecurity Frameworks

In both the United States and Canada, leading cybersecurity frameworks serve as voluntary guidelines and recommended practices for risk management. Specific regulations may apply to sectors designated as critical infrastructure.

NISTCybersecurity Framework (U.S.)

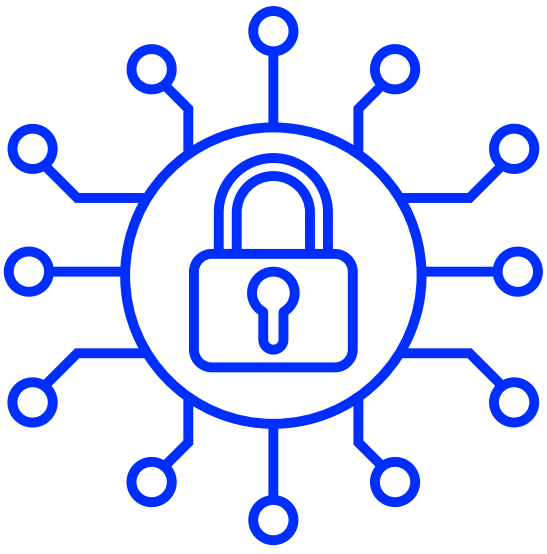
In the United States, the National Institute of Standards and Technology (NIST) provide the widely referenced Cybersecurity Framework (CSF), which is built on five core functions: Identify, Protect, Detect, Respond, and Recover.

The TV-ISO-E2 router is designed to support the Protect function by implementing controls that may help safeguard building systems. Its network segmentation features are intended to isolate building automation systems from broader IP networks, which may assist in limiting the spread of potential threats. Additionally, the router's support for encrypted BACnet/SC communication is designed to promote data confidentiality and integrity, key considerations within the Protect function.

Canadian Centre for Cyber Security (CCCS)

Canada's cybersecurity guidance is led by the Canadian Centre for Cyber Security (CCCS) which publishes resources such as the Cyber Security Readiness Goals (CRGs). These goals outline cross-sector practices aimed at improving the cyber resilience of essential services.

The TV-ISO-E2 router may align with aspects of the CRGs by supporting resilient network design. Its ability to establish secure zones and manage data flow is intended to assist with objectives related to BAS network security and access control. These features may contribute to broader efforts to reduce cyber risks in building automation environments, consistent with CCCS guidance for critical services.



Carrier

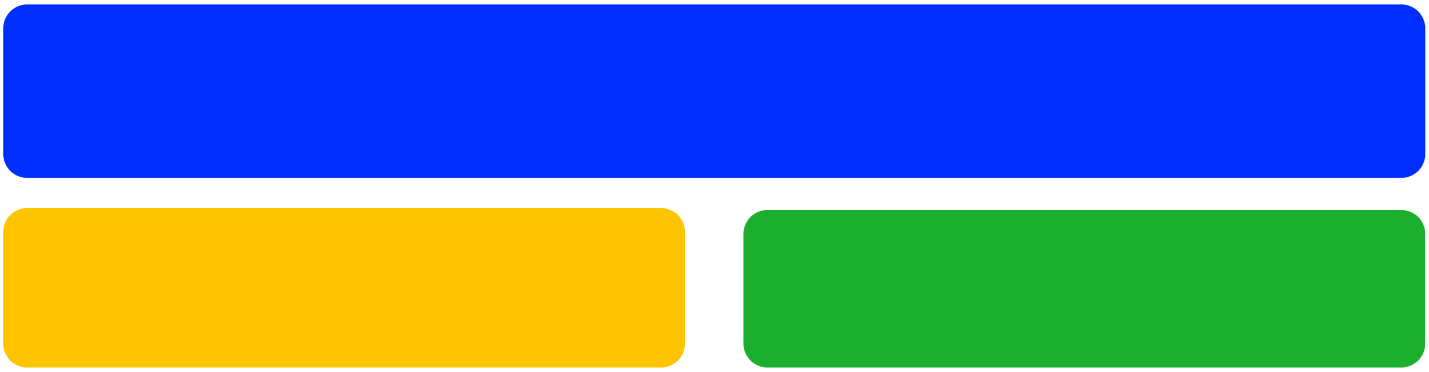
A Secure and Integrated Solution

The isolated network router serves as a key component within a broader strategy for secure building automation. This integrated approach is designed to support both system security and ease of installation, management, and maintenance.

System Integration Support: The router is engineered to work with pre-configured control programs and BACnet communication protocols. These features may contribute to a cohesive system that is easier to understand, monitor, adjust, and maintain.

User Interface Design: The system includes a graphic-rich user interface intended to provide a comprehensive view of a building's HVAC system. Facility staff can access the system from web-enabled devices, which may help them respond more efficiently to operational issues. Auto-generated graphics are designed to offer enhanced visibility and control over equipment.

Service and Support: These systems are delivered and supported by a network of authorized Controls Experts. This program includes training and certification designed to promote proper installation and maintenance of the i-Vu building automation system.



Sustaining BAS Security Over Time

A resilient and secure BAS system depends not only on technology, but also on the people and processes that support. When specifying a solution, it's important to consider long-term system viability and operational continuity.

Secure Development Practices: Consider selecting manufacturers that demonstrate a commitment to secure coding practices and conduct regular vulnerability assessments throughout the product's development lifecycle. These practices may help reduce exposure to evolving cyber threats.

Long-Term Value: Look for systems designed with long-term customer value in mind, including features such as backward compatibility. This can allow building owners to modernize their systems incrementally, potentially avoiding costly full-scale replacements, and helping to preserve prior investments while minimizing operational disruptions.

Ongoing Security Management: Cybersecurity is an ongoing process, not a one-time event. It may be beneficial to prioritize solutions that include comprehensive training and documentation. Additionally, systems that support automatic security updates and patching can help address emerging vulnerabilities more efficiently. For added assurance, consider solutions that undergo independent third-party security audits and penetration testing to confirm the effectiveness of their security posture.

Conclusion

By incorporating these insights into specifications, building automation systems can be designed to support efficiency, security, and resilience – positioning facilities to meet future challenges. One important consideration is selecting systems that are delivered and supported by a network of authorized, certified professionals. This approach may help promote proper installation and maintenance, contributing to the protection of a client's investment and reputation. Additionally, prioritizing solutions with an intuitive, graphic-rich user interface can empower facilities staff to respond more quickly to alerts, which may serve as an early line of defense against potential cyber threats.

To learn more about how a smart building automation system and a dedicated network isolation router can meet these specifications, contact your local Carrier Controls Expert.

iVu

For more information,
visit www.carrier.com/ivu or

Contact Your Local Carrier Controls Expert

Controls Expert Locator:
www.carrier.com/controls-experts

Catalog# 11-808-1234-01 11/2025