Daniel Shepard

Practical Strategies to Enable Protection

Cybersecurity Project Specs for Building Automation Systems

BY DANIEL SHEPARD, MEMBER ASHRAE

As integration of technology expands within building automation systems, the importance of cybersecurity cannot be overstated and the need for robust cybersecurity measures becomes increasingly crucial to ensure operational readiness and uptime. To safeguard the confidentiality, integrity and availability of these systems, it is essential to develop comprehensive project specifications that address cybersecurity requirements. This column provides practical recommendations to designers writing project specifications for the cybersecurity of building automation systems, emphasizing the importance of proactive planning and collaboration. This will lead to resilient protection against evolving cyber threats and lower the potential risks of cyber-based vulnerabilities associated with smart buildings.

Understanding the Project Scope

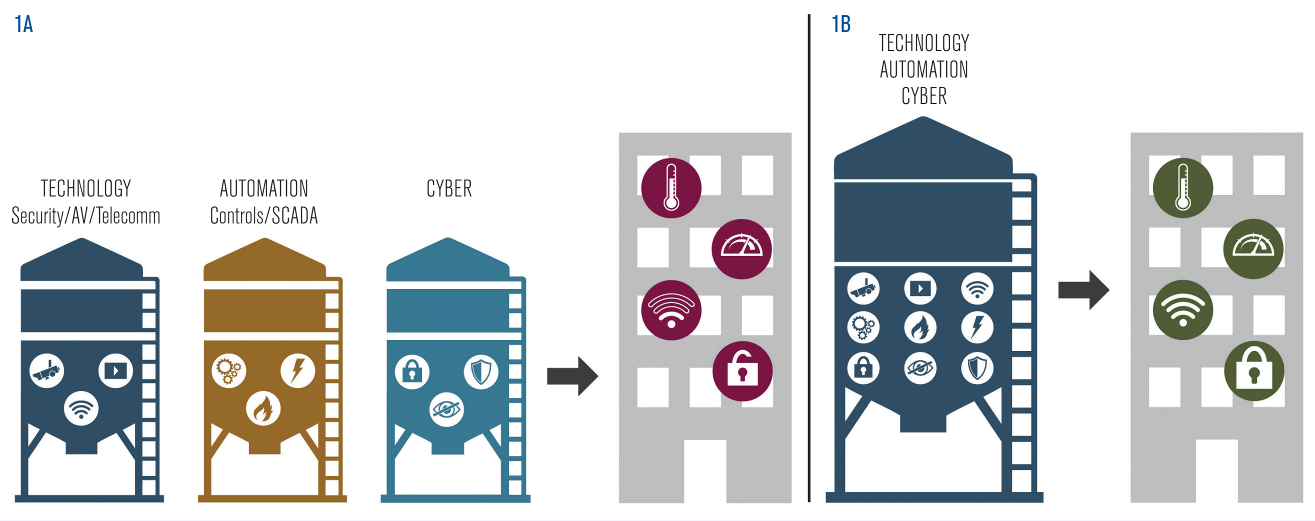
Before delving into the specifics of writing project specifications, it is crucial to gain a comprehensive understanding of the project scope. This involves identifying the key components of the building automation system (BAS), including hardware, software, network infrastructure, any potential interfaces with other field level control systems and any owner-specific compliance standards. By establishing a well-defined scope, stakeholders can develop targeted cybersecurity strategies and select appropriate cybersecurity controls tailored to meet the desired functional end state without impeding functionality. This knowledge will serve as the foundation for developing effective cybersecurity project specifications.

Collaborative Approach for Best Results

Writing project specifications for BAS cybersecurity should be a collaborative effort involving stakeholders including building owners, facility managers, IT professionals, mechanical and electrical engineers, cybersecurity experts, vendors and integrators. This collaboration leads to diverse perspectives, resulting in specifications that align with industry best practices

Daniel Shepard is the Control System Cybersecurity Department manager for Dewberry Engineers Inc., in Huntsville, Ala.

FIGURES 1A AND 1B Breaking the siloed design paradigm. it is incumbent upon the design team to break the traditional siloed design paradigm and understand each other's design considerations.



and any of the owner's regulatory requirements. A siloed design approach (*Figure 1a*) will not result in a functional and cyber-secure BAS; it is incumbent upon the design team to break the traditional siloed design paradigm and understand each other's design considerations (*Figure 1b*).

For example, if a client wants their BAS to centrally monitor and control multiple facilities from a single point of presence, the designer responsible for designing the telecommunication network—which the BAS will communicate on—will need to know the appropriate ports, protocols and services needed to support that communication. They will also need to know distances between buildings, so they can design the correct telecomm transport medium (e.g., copper, fiber or wireless) to support the network architecture design. Then, based on the design decisions of the automation and telecomm professionals, the cybersecurity designer will have to take into account those elements provided by the other design disciplines to make sure no cyber risk exists associated with the other designers' approach.

If each discipline does not consider the others' requirements, a high probability exists that the design will lack the necessary design features to accommodate a fully functional, cyber-secure BAS. Collaborating up front and throughout design can generally reduce cost, schedule and performance risk related to integrated technology solutions.

Incorporating Essential Cybersecurity Design Elements

When writing project specifications for the cybersecurity of BAS, consider these essential design elements.

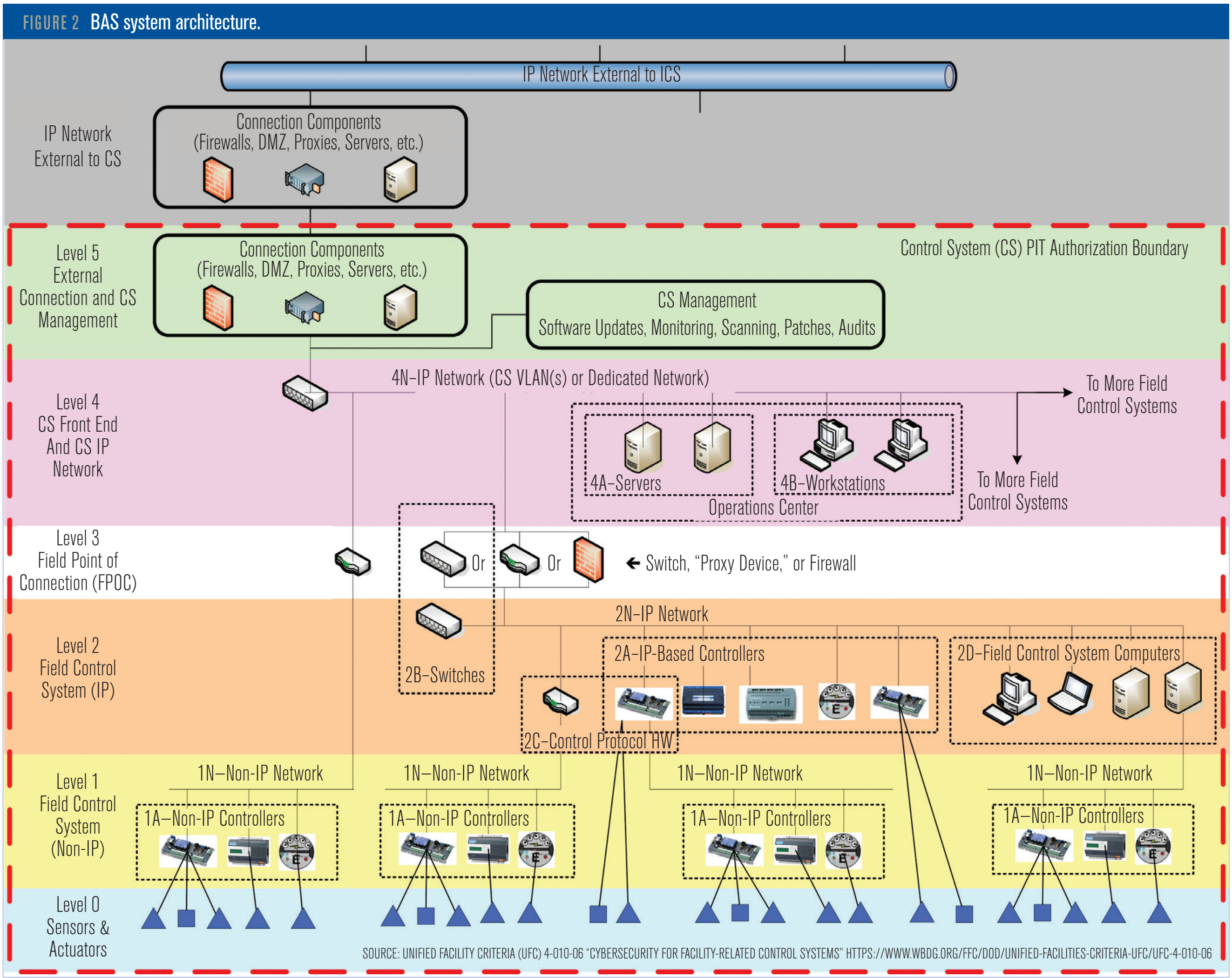
System Architecture

It is important for the cybersecurity designer to understand the full BAS system architecture (*Figure 2*) being proposed to meet the client's requirements. Multiple levels are within the BAS architecture, and many control system reference models can be used on which to base the architecture design. A common thread among these reference architectures is the way they are represented by functional levels.

Many people believe cyber-based vulnerabilities only reside within the IP level of communication. Although more potential exists to have cyber-based threats and vulnerabilities present at the IP level, understanding the potential threats and vulnerabilities associated within each level can aid the designer's ability to implement cyber-based design countermeasures to lower the risk of a potential exploit. For example, level 1 devices at the field control level that are non-IP devices, such as a VAV box controller or an intelligent (networked) thermostat, can pose some cyber risk.

A few basic design measures can be specified to limit the risk exposure posed by these devices, such as disabling or, at a minimum, prohibiting any secondary network connections other than connections to the level 1 network. Other measures could include implementing the use of passwords or PINs on the devices when possible. Designers must evaluate each level of the reference architecture and the capabilities

FIGURE 2 BAS system architecture.


IP Network External to ICS
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers, etc.)
Level 5 External Connection and CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers, etc.)
Control System (CS) PIT Authorization Boundary
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 CS Front End And CS IP Network
4N–IP Network (CS VLAN(s) or Dedicated Network)
To More Field Control Systems
4A–Servers
4B–Workstations
Operations Center
To More Field Control Systems
Level 3 Field Point of Connection (FPOC)
Or
Or
Switch, "Proxy Device," or Firewall
Level 2 Field Control System (IP)
2N–IP Network
2B–Switches
2A–IP-Based Controllers
2D–Field Control System Computers
2C–Control Protocol HW
Level 1 Field Control System (Non-IP)
1N–Non-IP Network
1N–Non-IP Network
1N–Non-IP Network
1N–Non-IP Network
1A–Non-IP Controllers
1A–Non-IP Controllers
1A–Non-IP Controllers
1A–Non-IP Controllers
Level 0 Sensors & Actuators

SOURCE: UNIFIED FACILITY CRITERIA (UFC) 4-010-06 "CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS" HTTPS://WWW.WBDG.ORG/FFC/DOD/UNIFIED-FACILITIES-CRITERIA-UFC/UFC-4-010-06

of the devices with the respective levels as they consider the appropriate cybersecurity control measures specified for the project.

However, most importantly, when looking at the system architecture, it is important to specify it to include system segmentation, network zoning, firewalls and demilitarized zones (DMZs). Clearly define how the various components of the BAS should be connected and segregated to minimize the risk of unauthorized access.

Access Controls

Detail the access control mechanisms that will be implemented to protect the BAS. Specify user roles, privileges and authentication methods. Consider the use of multi-factor authentication when feasible, strong password policies and secure user management practices. Additionally, emphasize the importance of regular access control audits and user account management processes.

Network Security

Outline the specific network security measures to be implemented. This includes the use of secure protocols such as SSL/TLS encryption for data transmission. Specify intrusion detection and prevention systems (IDS/IPS), as well as network monitoring tools to identify and respond to potential threats. Make sure network equipment, including routers, switches and firewalls, adhere to industry best practices for security configurations. At the field point of connection (FPOC) level, the device should have a "deny all/permit by exception" policy applied. The FPOC should be set up with the most restrictive set of access control list (ACL) possible, as it is the demarcation point in the control system between the field control system and the BAS front end.

Incident Response and Recovery

Include provisions for incident response and recovery in the project specifications. Specify the development and implementation of an incident response plan in coordination with the owner. The plan should outline the steps to be taken during a cybersecurity incident. Define roles and responsibilities and incident reporting procedures and communication protocols. Additionally, establish backup and recovery procedures, allowing for business continuity in case of a security breach.

Vendor and Supplier Requirements

Clearly state cybersecurity requirements for vendors and suppliers involved in the BAS install. Specify minimum security standards to, such as secure coding practices, vulnerability management and regular patching and updates. Request detailed documentation and evidence of compliance with relevant cybersecurity standards. Designers should also account for installer-owned computer equipment used in construction. The designer should specify requirements that the installer's computer equipment must have anti-malware software, up-to-date operating system patches and user-based authentication.

Compliance and Regulation

Consider any industry-specific compliance requirements or regulations that must be addressed in the project specifications. Examples may include data privacy regulations, industry-specific security frameworks (e.g., NIST Cybersecurity Framework), or regional cybersecurity standards. Specify the necessary measures for compliance and the documentation and reporting processes required to demonstrate adherence.

Conclusion

Developing comprehensive project specifications for the cybersecurity of BAS is crucial to safeguarding smart buildings against potential cyber threats. This column offered some recommendations for writing these project specifications. ■

Advertisement formerly in this space.