Cybersecurity for Building Automation Systems

Best practices and practical approaches
for Building Automation Systems for Contractors

Mitigating Risk in Connected Buildings

NOTE: Trane believes the facts and suggestions presented here to be accurate. However, final design and application decisions are your responsibility.

In today's connected digital world, cybersecurity threats can be anywhere. Keeping confidential information confidential enters our minds every time we do an internet search, make an online purchase or complete a financial transaction. IT professionals take great care to manage and protect business systems, but your customers may start asking you about connected building systems.

Building Automation Systems (BAS) offer significant operational advantages for commercial building owners and occupants. They provide the applications and interfaces that make it easier to effectively manage indoor environmental quality (IEQ) and optimize energy efficiency. As connected systems they share many of the same cyber risks as traditional IT assets. With due diligence, the risks are manageable. The following information is an introduction to the best practices in BAS cybersecurity.

TIP:
BAS security should be given the same rigorous attention as other IT systems.

Common Questions and Concerns

As a BAS provider, Trane collaborates with thousands of building and IT professionals every year. We hear the same questions and concerns repeatedly across our customer base.

- How can I design my BAS system to secure it against cybersecurity threats?
- What's the most secure way for our BAS system to interact with other systems in our facilities?
- How do we provide access to the BAS system in a secure manner—both onsite and remotely?
- Is it possible to provide secure access to service providers? What are the risks?
- How can I be certain our BAS system is secure?
- What specific actions should we take to maintain a secure BAS system?

Three Key Areas of BAS Cybersecurity

BAS industry experts have addressed these common questions and concerns. The good news: There are some very practical best practices for designing, installing, and maintaining *secure* BAS systems.

These best practices fall into three main categories.

1. **Isolation** – designing the BAS as a standalone entity that is separated from other business systems, isolated from the internet, and protected from unauthorized physical access.
2. **Secure Access** – formalizing processes that provide secure on-site and remote access for employees and service providers.
3. **Operation and Maintenance** – establishing (and sticking to) set protocols and maintaining a regular schedule of system and software maintenance to maintain security over the long term.

Let's look deeper into these topics.

Isolation

A well-designed building automation system design and set-up must provide adequate separation from other systems *and* prevent access by unauthorized personnel. Isolation can be broken down into a few distinct categories.

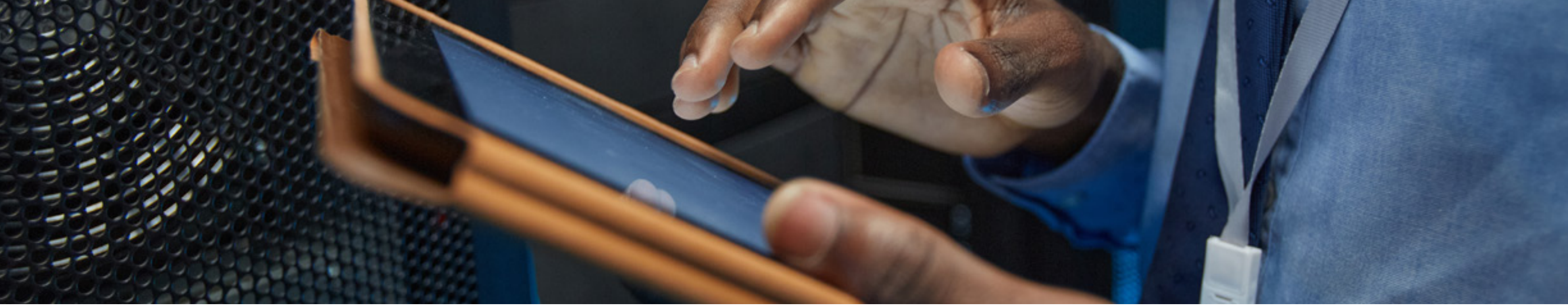
Physical Isolation. Access to BAS systems should be strictly controlled and limited to authorized employees and service providers. The solution can be as simple as keeping the primary BAS hardware in a locked room (such as an electrical closet) and controlling access to workstations that are being used for BAS operation and management.

Internal Network Isolation. A building automation system is very similar to other IT assets. The BAS network should only allow essential communication to mitigate unintended risk; all other communication should be prohibited. The BAS may be installed on a separate physical network, or a logical isolation may be utilized. A common example would be a Virtual LAN (VLAN).

TIP: Encourage your customers to consult their IT staff. They know best when it comes to making decisions regarding how networks should be installed and operated to maintain proper isolation in each unique situation.

Internet Isolation. Building automation systems should always be properly isolated from the internet to prevent unauthorized access. Typically, this is accomplished by using a firewall (router) that isolates the BAS network from incoming internet access.

TIP: Firewalls can be set up to allow the *outbound* BAS traffic which can enable secure remote access solutions (like Trane Connect™ Remote Access) to improve the productivity of servicing personnel.



Secure Access

It's important to make sure that personnel who need access to the BAS have it, including facility staff and service providers. Security practices should cover every possible user interface, both on-site and remote.

User credentials. A BAS commonly requires multiple user accounts, each with unique credentials that limit authorization to features that are necessary for the individual's role. One dedicated system administrator should have full access to the system. Only that administrator should be allowed to set up new user accounts and determine the level of access: view only, or view and change limited items.

On-Site Access. Best-practice security is accomplished by limiting access to the network where the BAS resides combined with user credentials, as discussed above. If a user has access to the network, the BAS is commonly accessed via a URL or an IP address in a web browser.

Remote Access. Remote access can be used to allow appropriate personnel to access the system from anywhere. "Personnel" may mean employees of your company as well as employees of your service provider. Remote access typically requires an additional layer of security in addition to the user credentials discussed above.

There are two common ways to establish secure BAS access from the internet.

1) Secure Remote Access Portal. This method uses a separate server (typically in the cloud) that controls secure access and allows users to request access to a site. This type of solution typically works in the following way:

- The BAS system connects securely to the Portal via the customer network or via a separate cellular connection.
- If the customer network is used, only outbound ports are used—no inbound ports are open.
- If a cellular connection is used, it established a secure connection (multiple methods can be used—such as a firewall or a private cellular network)
- Users can go to the Portal to request access to one or more sites. User authentication (user credentials, sites allowed) at the Portal is required.
- The Portal provides the user secure access to the sites that they are authorized to connect to.
- The Portal may support a combination of web browser, mobile app and service tool access.

2) Virtual Private Network (VPN). Facility IT staff can establish VPN access for employees and service contractors to provide remote access into the network where the BAS resides. This approach requires additional attention from the facility's IT staff. Be careful when granting VPN access to outside service providers. Depending on the level of BAS network isolation, VPN access may enable outsiders to access other systems within the facility where you don't want them to go.

TIP: The BAS should never be directly accessible from the internet (e.g., public IP address with open ports).

TIP: It is possible to use the Secure Remote Access Portal for both on-site and remote access. This single-access method simplifies IT by eliminating the need for VPN setup and maintenance. It also makes access consistent for users—whether they are on-site or off-site.

Operation and Maintenance

Once the BAS system is properly isolated and secure access is defined and implemented, the system must be diligently maintained. Cybersecurity best practices require ongoing attention to help maintain their effectiveness.

Here are some key considerations.

User ID and Password Best Practices

Unauthorized use of log-in credentials is a common approach for bad actors. The importance of assigning strong, secure User IDs and Passwords cannot be overstated. Proper access control and user management must be diligently maintained.

- **Use Strong Passwords.** Avoid using passwords that are easy to guess. A good BAS system will establish and enforce rules for password strength.
- **Never Share Passwords.** Unfortunately, this happens far too often. It is one of the most likely ways for unauthorized users to gain access. Every authorized user should have a unique ID and password, which provides a way to track who has logged into the system, and when.
- **Provide Temporary Passwords for Service Providers.** Log-in credentials granted to service providers and others from outside the organization should have strict limitations. Remove access immediately once the contracted work has been completed. In certain cases, it may be acceptable to assign trusted service partners permanent "read-only" access that is easily upgradable to allow changes on a temporary basis.
- **Remove Users Who No Longer Need Access.** This should go without saying, but we will. It's that important. When employees leave the organization, or service providers are no longer engaged - *remove their login credentials!* Block all system access points.

TIP: If the company has Active Directory services available, employees can be authenticated by the Active Directory services. This allows employees to use their business passwords for BAS access. It also ensures that employees who leave the company will be blocked from BAS access when they are removed from the main system.

System and Software Maintenance

Systems that are installed properly may not stay secure without consistent maintenance. The owner and/or operator of the facility must have a plan to keep their BAS system up-to-date and operating securely.

Every BAS system requires the following scheduled maintenance.

- **Regular Software Updates.** In today's digital world, software must be updated frequently to provide the most current protection against new and evolving cyber threats. Failing to keep software up to date increases risk. Many BAS providers issue updates annually, at a minimum, and more often if new vulnerabilities are identified. Watch for updates and act on them immediately. *Have a plan for regular software updates.*
- **Test the System for Internet Isolation.** It isn't uncommon for firewall settings to change, even inadvertently. Test the BAS for Internet exposure regularly, as part of ongoing scheduled system maintenance. *Early detection is the key to risk mitigation.*
- **Review User Credentials.** Establish a schedule to review all user log-in credentials in the BAS system regularly. Validate that all listed users still require the level of access they have been granted. *Remove any users who no longer need access.*

TIP: No in-house expertise? Service providers may be contracted to assist with cybersecurity upkeep.

Trane goes the extra mile

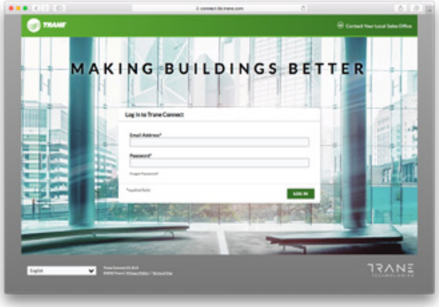
Cybersecurity is a priority for all of Trane's connected offerings. Here are some popular solutions available from Trane that can help make it easier for you to keep your systems secure.

Secure Cellular Connectivity

Is getting internet access to a site's BAS system a challenge? Do you need to keep the BAS System isolated from your business network? Trane offers multiple cellular connectivity options to fit your needs. Our most popular option is the plug-and-play Trane USB Cellular Module that provides private, encrypted communication between your Trane BAS system and Trane Connect Secure Remote Access.

Trane Connect™ Secure Remote Access

Our cloud-based customer portal provides secure remote access to your Trane BAS for remote monitoring and routine maintenance. In addition to other available services, Trane Connect Secure Remote Access supports web browsers and our suite of Trane mobile apps—so that you can easily access the Trane BAS system from any location.



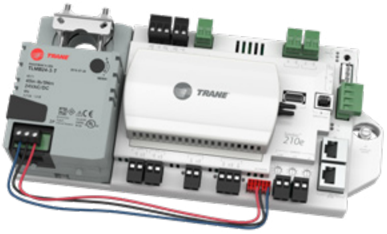
Customers can provide access credentials to any of their employees or service providers. With available admin rights, they can maintain your own list of people with their access credentials and site privileges. In all cases, building-level BAS system passwords remain in place, as an extra layer of security.

Trane Connect Secure Remote Access Features

- Secure connectivity from your building to the cloud via your network or a separate cellular connection.
- User access control both at the Trane Connect level and at your BAS system level.
- Authorized users can access the BAS system using either a web browser, or our suite of Trane mobile apps, using a PC, tablet or phone.

Controller Security

Trane controllers, including Concierge with Tracer SC+ and Symbio® unit controls, are designed to proactively provide protection against incidents using tools such as encryption, multiple layers of access control and authentication to protect your data. We provide complex cybersecurity features, straight out of the box.



Want more details? Your Trane Account Manager can connect you to our cybersecurity specialists.

Trane – by Trane Technologies (NYSE: TT), a global climate innovator – creates comfortable, energy efficient indoor environments through a broad portfolio of heating, ventilating and air conditioning systems and controls, services, parts and supply. For more information, please visit *trane.com* or *tranetechnologies.com*.

All trademarks referenced in this document are the trademarks of their respective owners.