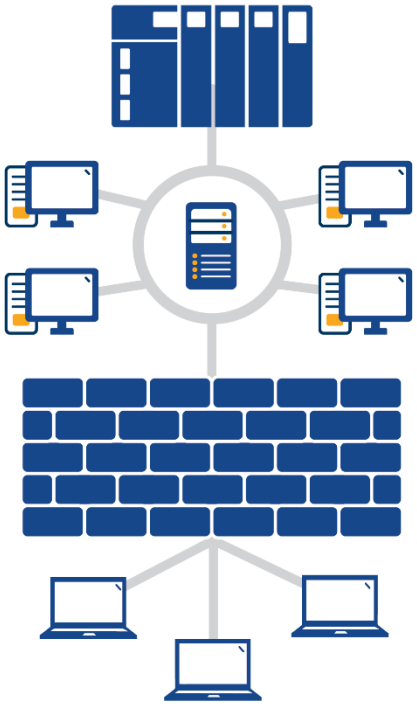
Introduction

Although there is a wealth of cybersecurity knowledge for including best practices to secure networks and network-connected devices, many building engineers and operators lack the expertise. As a result, Building Automation Systems and Building Management Systems (BAS/BMS) can have long-standing unresolved cybersecurity vulnerabilities. The migration from separated control panels with an isolated operator computer located within the building to distributed digital control (DDC) expands the "attack surface" of the BAS/BMS by connecting all of the field devices. When a vendor installs a Real Time Energy Management (RTEM) system with the existing BAS/BMS, it is critical to address existing vulnerabilities to minimize the cyber risks to the building's infrastructure.

This document provides recommended security practice guidelines for an RTEM system, including implementing the high-security standards that IT currently applies in BAS/BMS and RTEM systems. RTEM vendors should work with each customer's IT department to protect the RTEM system and the connected BAS/BMS.

Involving the IT Department Early



Involving the IT department early in the planning process when expanding BAS/BMS or adding a RTEM system is a good project management procedure. This allows trained IT staff to provide input on how to prevent compromising the building's existing cybersecurity measures. Trained IT staff can identify security weaknesses early, giving the team plenty of time remediate without affecting the project.

BAS/BMS equipment—such as programmable logic controllers (PLC), variable frequency drives (VFD), and control panels are capable of communicating over a standard computer network or can be made network compatible using a readily available off-the-shelf network bridge. Automation and control equipment require network connectivity, and as a result, the building's IT department or IT service provider often are asked at the last moment to provide network outlets in mechanical rooms, electrical rooms, risers, ceilings, and throughout the building. These additional network outlets, as well as their connected equipment, all add vulnerabilities unless access is restricted only to authorized devices or staff.

Unlike IT equipment, BAS/BMS and RTEM equipment do not have IT certifications, such as from Microsoft or Cisco, to demonstrate security practices. Consequently, many IT departments assume the BAS/BMS or RTEM vendor has ensured system security and these measures have been evaluated by the personnel making the purchasing decision. Identifying who is responsible for the BAS/BMS and RTEM

system cybersecurity early in the evaluation or purchasing process is recommended. Tasking an IT department to secure unfamiliar BAS/BMS and RTEM equipment under the scheduling crunch of a construction project is burdensome and unreliable. Qualified RTEM vendors will consider cybersecurity practices and expertise as an unique differentiator.

Many IT departments already have policies and procedures for approving third-party devices or allowing remote log-in to the network. It is essential to communicate these policies and procedures, as well as network constraints, to vendors early in the purchasing or planning process. Many RTEM vendors also require that their technician's have internet access during the installation and commissioning phase. Requesting the involvement of the IT department to provide this access protects the building's systems.

Cybersecurity Requirements for RTEM

This section contains recommendations of initial requirements to ensure a well-protected RTEM system. All items do not apply to all RTEM systems. However, vendors solutions should demonstrate a commitment to cybersecurity—these recommendations are also applicable to internet-connected BAS/BMS and building systems, such as remotely manageable CHP onsite generators. Cybersecurity requirements for a RTEM system are layers of protective measures spanning from the building data sources, to internet connectivity, to cloud resources where data resides.

A suitable RTEM system should address the following layers of protective measures:

- Internet Connectivity Protection
- On-Premise Equipment Protection
- Local Network Protection
- Web Portal Access Protection
- User Credential Protection

The specific recommended cybersecurity practices for each layer is described as follows.

Internet Connectivity Protection. Secures the communication path between the building and the RTEM system's cloud-based resources, including authenticating the sources of the on-premise data and the sources of the returning messages between the cloud and the building. Employing or enforcing the following as a minimum set of measures for securing internet connectivity is suggested:

- Transport layer encryption on all internet communications

- Transport layer authentication on all internet communications
- Transport layer data integrity measures to verify data has not been forged or tampered
- IP filtering to limit the destination of the outbound traffic
- Closing unused communication ports on all NICs
- No use of public IP addresses for the on-premise portion of the RTEM system

Examples of common transport layer security measures are the use of HTTPS, SSL, or VPN to encrypt communications over the internet.

On-Premise Equipment Protection. Secures the RTEM system's on-premise equipment to prevent attacks. The security provisions should include protecting physical access to the on-premise equipment, local access to communication ports, and eliminating default login credentials allowing entry into the on-premise equipment.

The following minimum measures for securing physical access to on-premise equipment are recommended:

- The panels or housing of the equipment should be secured by locks
- Access credentials are not located on the enclosure
- Encrypt data on all removable storage installed with on-premise equipment

The following minimum measures for securing the firmware/software installed within the on-premise equipment are also recommended:

- Disable unused communication ports
- Enforce authentication and encryption when using active communication ports to access equipment's firmware and software
- Enforce tracking of the firmware and software installed for known vulnerabilities
- Enforce assigning building and device specific administrative credentials during commissioning
- Employ encryption and authentication of all software/firmware updates before installation

Enforce the following minimum measures for securing local (on-premise) and remote login access to on-premise equipment:

- Two-factor authentication
- Strong passwords such as capital and lower-case letters, numbers, and special characters in passwords
- Periodic password changes
- Access lockout after repeated fail login attempts

- Password changes at commissioning (e.g., first login)

Local Network Protection. Secures the RTEM system's on-premise wired and wireless network that connects RTEM equipment such as sensors, meters, and database servers by an unauthorized device. Sources of on-premise data are authenticated as well as sources of on-premise commands by employing:

- Network segmentation to keep RTEM system network separated from corporate or business networks
- Auditing the RTEM network to maintain a list of authorized devices and their locations
- VLANs to separate network traffic by protocol (e.g., BACnet IP, Modbus IP)
- MAC address filtering to limit network traffic to only authorized devices
- Authentication on all wired and wireless networks (e.g., 802.1X authentication protocol)
- WPA2 on all Wifi wireless network (e.g., avoid WEP, WEP)

Web Portal Access Protection. Permits only authorized and authenticated users on the RTEM system's web portal, dashboard, mobile applications, and reports. Employing the following minimum measures for protecting web portal access is recommended:

- SSL on all portal responses
- HSTS
- Public key or certificate pinning
- Secure cookies

Additionally, enforce the following minimum measures to protect authorized login credentials assigned to users:

- Two-factor authentication
- Strong password by policy such as capital and lower-case letters, numbers, and special characters in passwords
- Periodic password changes
- Access lockout after repeated fail login attempts

User Credential Protection. Prevent the disclosure of an authorized credential to an unauthorized person through mechanisms such as email phishing attacks, the sharing of credentials, and eliminating default credentials. Follow the minimum measures to protect all authorized credentials:

- Enforce individual credentials—no sharing of credentials

- Enforce strong password policy such as capital and lower-case letters, numbers, and special characters in passwords
- Employ login monitoring for suspicious patterns
- Users should be alert to “phishing” and other scam contacts by email, text, or phone
- Users should not to reuse their credentials on other sites
- Enforce no default credentials