# Best Practices for Securing an Intelligent Building Management System (iBMS)

by Mike Bielby
Allan Björck
Jonas Bülow
Julie Cunningham
Brett Leida
Jonathan Meran
Henrik Nilsson
Shawn Slavin
Gregory Strass

## Executive summary

System integrators, network administrators, and facilities personnel need to apply best practices for securing an intelligent building management system (iBMS) throughout its lifecycle. Once stand-alone systems, iBMSs are now routinely networked to IT data centers, remote access servers, and public utilities. This paper describes how to secure an iBMS throughout the design, installation, and operating phases of its lifecycle. Best practices for addressing various aspects of security are described, including network infrastructure protection, threat detection and mitigation, and device hardening.

998-2095-02-31-12AR0

Schneider Electric

# Table of Contents

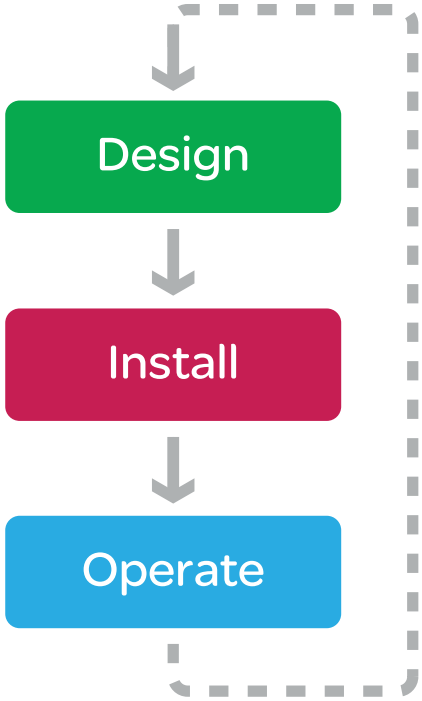
# Introduction

An effective intelligent building management security plan mitigates risk throughout the design, installation, and operation phases of a system's lifecycle. Many organizations focus their efforts on creating a secure design and take minimal steps to maintain security moving forward. This is analogous to building a protective wall around a castle and opting not to place guards in the watchtower; eventually someone will devise a way in. Only by creating and executing a plan to address security throughout the entire lifecycle of the system, can an organization effectively manage risk. The creation of such a plan requires the coordinated efforts of parties responsible for the system throughout its lifecycle; such as system integrators, network administrators, and facilities personnel. Every contributor must become familiar with the unique challenges of securing an intelligent building management system.

Intelligent Building Management System (iBMS) security is a relatively new concern for many organizations. Once proprietary, stand-alone systems, intelligent building management systems are now routinely networked to other systems including IT data centers, remote access servers, and public utilities. Many proprietary technologies have been phased out in favor of industry standard solutions. This has resulted in substantial growth in the use of open protocols. While these innovations offer real benefits to iBMS consumers, their use requires careful assessment of their impact on security. To mitigate the security risks, organizations should apply best practices for securing their systems.

This paper presents the key aspects of securing an iBMS throughout the design, installation, and operating phases of its lifecycle. Best practices for addressing various aspects of security are described, including network infrastructure protection, threat detection and mitigation, and device hardening.

The goal is to provide responsible parties with the basic knowledge to develop a comprehensive plan that addresses the iBMS security needs of their organization. The information presented is general and should not be interpreted as a one-size-fits-all approach to security. Any well-balanced security plan takes into account the size of the facility, the impact of a potential breach, and projected installation and operation costs. Each organization should evaluate its tolerance for risk, quantify its willingness to invest in mitigation measures, and act accordingly.




iBMS Lifecycle

# Design for Security

The primary focus of the design phase is to establish a boundary around the iBMS and provide ways to control and monitor access. The decisions made during this phase determine many of the security options available in later phases. Therefore, it is essential to solicit input from the people who will be responsible for the installation and operation of the system. Physical security, network infrastructure, and device selection are important elements of the design process.

> "The mantra of any good security engineer is 'Security is not a product, but a process'."
>
> *Bruce Schneier,*
> *Security Specialist and Author*

## Physical Security

No security plan is complete unless it addresses the need for physical security. Physical security prevents unauthorized access to the iBMS' devices, networks, and information. Without it, intruders have the means to circumvent all other methods of protection.

Consider the following when making design decisions:

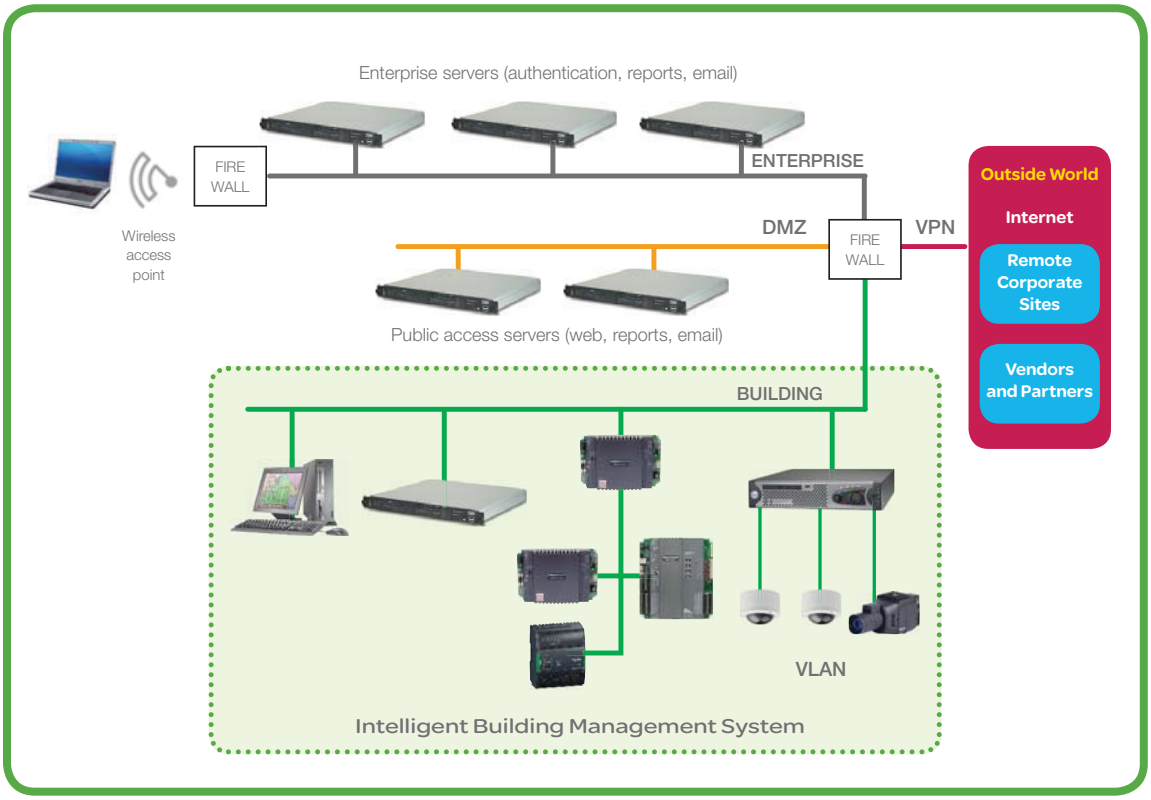
- Combine multiple barriers to access; such as building, room, and cabinet access control.
- Locate mission critical devices in access controlled areas or in locked cabinets. Preventing unauthorized physical access to network devices such as routers, firewalls, and switches is a must.
- Protect communication cable runs with conduit or ruggedized cable chases.

## Network Infrastructure

The network is the conduit that allows information to flow between the iBMS, the enterprise system, and the outside world. Intruders able to tap into the network can disrupt the flow of information. The example architecture diagram on the next page illustrates these practices.

# Design for Security (cont'd)

## Network Infrastructure Example




## Limit Network Access Points

- Isolate the iBMS as much as possible. Locating it on a virtual local area network (VLAN), for example, ensures that building traffic, including broadcasts to all nodes, remains within the logical boundary you establish.
- Think carefully before granting outside access. Each network entry and exit point must be secured. By granting access only when a valid reason exists, you can minimize risk and keep security costs down.

## Use Firewalls to Control Access

Firewalls contribute to security by controlling the flow of information into and out of network entry points. Using a set of user defined configuration rules; a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected. A single best practice applies to adding firewalls to your network design:

- Place a firewall at every transition point into or out of the iBMS network.

Providing recommendations for the proper selection and placement of firewalls is a detailed endeavor and is beyond the scope of this document.

# Design for Security (cont'd)

## Manage User Access

Secure user access is achieved through the use of authentication and authorization. Authentication is the means by which a user's identity is confirmed. Once authenticated, a user is authorized to perform certain functions as defined by their role within the organization.

- Restrict user access by capitalizing on solutions commonly deployed by IT departments, such as Central Authorization, Password Control, User Management, and Network Monitoring. Examples include Active Directory®, Kerberos, and Radius.
- Further restrict user access by establishing authorization requirements for individual devices such as routers, servers, embedded controllers, and workstations. The type of device will dictate the best approach.
- Consider stronger authentication methods for critical host devices such as:
  - Smart Cards or USB tokens
  - Biometric Authentication limits access based on a physical or behavioral characteristic such as a fingerprint.
  - Two-Factor Authentication limits access to users with both a password and a physical token.

## Restrict Remote Access

Providing iBMS access to remote users presents a unique set of security challenges. Addressing these challenges requires building additional protections into the network infrastructure. Even then, remote access should only be considered for systems that already have sufficient protection against external threats. Best practices for providing remote access include:

- Use a secure connection, such as a VPN, which provides encryption and authentication of remote sessions.
- Use secure protocols and applications such as HTTPS, SSH, and SCP/SFTP whenever possible and avoid Telnet and FTP.
- Evaluate the risks associated with SNMP (Simple Network Management Protocol) before incorporating it into your design. When using SNMP, limit access to authorized system administrators with known IP addresses.
- Restrict remote access by using Two-factor Authentication and by limiting access to required users only, such as system operators.
- To provide public access to information, create a demilitarized zone (DMZ), place a server within the zone, and mirror the required information onto the server.

### Firewall Basics

A firewall…

- Is either a stand-alone device or a software application running on a host
- Supports at least one internal and one external connection
- Filters information in the following ways:
  - Service control
  - Direction control
  - Behavior and content control (email, web)
- Functionality ranges from basic to complex:
  - Packet filtering
  - Application level – proxy server
  - Deep packet inspection
- Requires special expertise for proper selection and configuration

# Design for Security (cont'd)

## Selecting Components - Security Features that Matter

Consider the following best practices when selecting system components:

- Choose devices and protocols that support encryption, integrity, and nonrepudiation whenever possible. Encryption protects the information traversing a network by making it unreadable to unauthorized users. Integrity checks determine if any changes have been made to a network message. Nonrepudiation verifies the identity of an information source.
- Give preference to devices with logging capability, such as Syslog support. Event logging is available in a wide range of devices including routers, firewalls, backup systems, and access control systems. Logs can aid in early threat detection by recording significant network events, changes to firewall configuration, or user access to an area or device. Syslog is a logging standard that can be used to consolidate log information from multiple devices on a network.
- Look for tamper proofing, built-in locks, and other access control features when selecting mission critical components.
- Consider adding an Intrusion Detection System (IDS). An IDS is a stand-alone device or host based application that monitors system events in an effort to identify threats early. Events such as failed login attempts, traffic patterns, and changes to port configurations are evaluated. Choose an IDS that allows you to customize the rules used to define acceptable network behavior.

## Wireless Technology

Wireless networking technology offers several advantages over wired technology including lower installation costs and greater design flexibility. These advantages must be weighed against the increased security risk associated with its use. Best practices for the use of wireless technology are as follows:

- Choose wireless devices with built-in firewalls and support for the highest level of encryption available.
- Harden wireless access devices by following these steps:
  - Replace the default administrator name and password with strong alternatives.
  - Change the default System ID (SSID or ESSID).
  - Disable all identifier broadcasting.
  - Enable user authentication such as directory services or 802.1X.

# Install with Security

## Before You Begin

In preparation for system installation, consider the following:

- Throughout the installation process, the iBMS may be particularly vulnerable to attack. Consider temporarily isolating the system from the outside world until all the components of your security plan are in place.
- Update new and legacy equipment with the latest security patches.
- Security measures, particularly those designed for enterprise networks, can sometimes interfere with proper iBMS function. Anti-virus software, for example, has been known to disrupt workstation performance by consuming large amounts of processor time. While this occurs infrequently, it is important to have a method in place for evaluating system performance as security features are brought online.

The goal in this phase of the process is to properly configure the security features of each system component. Configuring firewalls, hardening system devices, configuring user accounts, and enabling threat detection are all tasks that contribute to secure system installation.

## Configure Firewall Rules

Firewalls use a set of rules, established by the user, as the basis for determining which traffic is allowed to pass in or out of the network. For example, a rule might block all access to a specific IP address or port. Proper configuration of firewalls is essential to securing the network and should only be performed by experienced personnel. Best practices for configuring firewalls include:

- Use a combination of rules to both permit authorized traffic and deny unauthorized traffic. A typical approach is:
  - Create rules that explicitly deny access
  - Add rules to permit only the required access
  - Add a broad-based rule to deny access to all remaining traffic
- Confirm that the firewall can detect TCP “SYN-flood” attacks by tracking the state of a TCP handshake (stateful firewall).
- Include rules to restrict outbound network traffic in order to minimize the spread of damage in the event of a breach.

# Install with Security (cont'd)

## Harden System Devices

By taking steps to harden system devices, you can close potential points of access into the iBMS and reduce the risk of an internal attack. The hardening process varies depending on whether the target is an embedded device or an off-the-shelf Windows or UNIX®/Linux® based computer running host software.

### All Devices

- Evaluate each device to determine what ports and services are available, and whenever possible, disable any that do not have a planned use. Port scanning applications can help expedite the identification process. Be sure to disable ports and services that were used temporarily for device commissioning but won't be needed during operation.
- Removable media, such as USB memory sticks and compact discs, are often the source of malicious software. The safest solution is to prevent the use of all removable media, by mechanically blocking ports, for example. For those applications where removable media is necessary, take measures to restrict port access and enforce media checking procedures (i.e. anti-virus scans).
- Enable the security features built into each device including encryption, firewall capability, access control, intrusion detection and prevention, and user authorization.

### Host Devices

- Install anti-virus software from a reputable vendor (i.e. Symantec, McAfee) and enable its automatic update features.
- Install and configure firewall software.
- Enable automatic operating system updates. Centrally managed updates are preferable.

**Examples of services to disable:**

- Proxy features on routers
- Identifier broadcasting on wireless devices
- Simple File Sharing on Windows based hosts
- Telnet, FTP

# Install with Security (cont'd)

## Configure User Accounts

User accounts establish access levels to the domains within a system. Best practices for configuring user accounts include:

- Replace all default vendor passwords with strong alternatives (twelve characters minimum with a mix of letters, numbers, and symbols). Likewise, remove all default logins (i.e. administrator) and system IDs.
- Disable every user's access to the system by default and add permissions only as required.
- Restrict each group of users to the lowest level of privileges necessary to perform their role.
- Prevent duplication of passwords across multiple sites.
- Use expiration dates to require users to periodically change passwords.

## Enable Threat Detection and Mitigation

Measures to detect and limit the impact of security breaches are an important component of any security plan. Consider the following best practices for detecting and mitigating threats:

- Create logs to monitor all aspects of the system including physical access, network activity, device activity, and firewall configuration. Consider system performance when setting logging parameters and collect log files in a central location to prevent unauthorized modification.
- If you are using an intrusion detection system, take the time to thoroughly understand the capabilities and limitations of the system you selected before configuring the alerts and active response rules that will govern its operation. Configuration rules should reflect the operating behavior of your network which may differ significantly from those of a typical enterprise network.

# Operate Securely

The need to address security does not end once a system has been installed. System monitoring, account management, patch management, and firewall maintenance are all important to operating a system securely.

## Monitor the System

Through vigilant monitoring of system parameters, you can detect security breaches earlier and take steps to limit the spread of damage. Monitoring guidelines include:

- Treat alerts from intrusion detection systems with the highest priority.
- Proactively scan the network for new hosts and out-of-date systems.
- Routinely review system logs for irregular activities. Indicators such as numerous failed login attempts, unusual credential card use, and increases in network load can provide early signs of a breach.
- Create an incidence response plan which describes the actions to be taken when system irregularities are detected.

## Maintain User Accounts and Access Lists

When a user changes roles within an organization or leaves altogether, it is important to have a documented procedure in place to remove or alter the level of access they have to the overall system. The procedure should address all types of access including physical, remote, network, and device level access.

## Manage Security Patches

Security patches provide protection against the never-ending flow of new threats. A good patch management plan combines policies, procedures, and qualified personnel in an effort to close security gaps without major disruption to the system. Best practices for patch management include:

### Take Inventory

Make a list of the devices that will require periodic security updates. The list should include network devices such as routers, firewalls, and VPN concentrators, as well as application and operating system software.

An annual report on data breaches, a subset of the overall security landscape, highlights the importance of system monitoring.

Out of 141 confirmed data breaches in 2009:

- 86% of the victims had log files containing evidence of a breach
- 61% were discovered by someone other than the victim

*Verizon 2010 Data Breach Investigations Report, Verizon RISK Team in cooperation with the United States Secret Service*

# Operate Securely (cont'd)

### Use Trusted Sources

- Use vendor issued firmware updates, service packs, and hot fixes.
- Whenever possible, use patches with digital signatures. A digital signature validates a patch's source and integrity.
- Stay up-to-date on newly released patches and vulnerability reports.

### Develop a Plan for Installation

A patch installation plan should include the following:

- A method of prioritizing patches. Most patches are routine updates that can be implemented according to a schedule. Others require immediate action to close a critical gap in security.
- Pre-approved patch installation tools that provide change management and security audit features.
- Procedures for vendor certification of patches, testing of patches prior to installation, and a staged installation process to minimize the risk of disruption from the change.
- The verification of digital signatures. Signed security patches should be verified just prior to installation to ensure that they have not been tampered with internally.

## Develop a Backup and Recovery Plan

A backup and recovery plan should identify responsible parties, list the items to be backed up, and provide specifics such as backup intervals, locations, and number of versions to retain. Verify that recovery procedures work as expected.

## Firewalls Require Special Attention

Firewalls must be properly managed by trained personnel to ensure continued system security. A firewall management plan should be developed to address the following requirements:

- Regular review of firewall configuration
- Strict change control measures
- Continuous monitoring of logs and relevant statistics

# Operate Securely (cont'd)

## Build iBMS Security Awareness

The people who interact daily with an iBMS play a critical role in maintaining overall system security. Security policies and procedures can easily be undermined, either knowingly or unknowingly, by a single individual. Personnel training is key to building awareness about the role each person plays in maintaining security within an organization. Training should include:

- Proper handling of account credentials
- Roles and responsibilities of each person in maintaining security
- Reasons behind various security policies and procedures
- Ways to recognize and respond to attempts by others to garner private information for the purpose of compromising a system (social engineering).

Security training works best if participation is mandated and the training itself is monitored for effectiveness.

## Perform Security Audits

Periodic security audits provide the means to ensure that systems, policies, and procedures devoted to security are effective and that no gaps exist. Security audits may include:

- Attempts to gain network or server access (penetration testing)
- Evaluation of past breaches to determine if potential for exploitation has been eliminated
- Attempts to acquire passwords from users
- Checks to verify that security procedures are being followed and security systems are not being bypassed
- Assessment of protection against new types of threats

An effective audit provides a comprehensive assessment of an organization's security and informs an ongoing process of improvement.

# Summary

Effective intelligent building management security requires more than a well thought out design. It requires continued vigilance throughout all phases of a system's lifecycle. The first step for any organization is the creation of a comprehensive security plan to manage the risks associated with each lifecycle phase. A common understanding of the best practices for securing an iBMS forms the foundation for the planning process. Armed with this information, network administrators, facilities personnel, systems integrators, and other contributors can evaluate alternatives and determine the best approach for their application.

## About the Authors:

The IT Security Team consists of people from various disciplines within Schneider Electric's Buildings Business, each with special expertise in building management system security. The team's mission is to identify new and innovative ways to improve the security features of our products and to document best practices for Intelligent Building Management System Security.

# Appendix

## Additional Resources

### Hardening Windows-based Host Devices

The Microsoft Security Compliance Manager is a free tool for hardening a Windows based system: http://technet.microsoft.com/en-us/library/cc677002.aspx.

Guide to General Server Security:
http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

### Security and Vulnerability Information

Centre for the Protection of National Infrastructure: http://www.cpni.gov.uk/

Common Vunerabilities and Exposures: http://cve.mitre.org

National Vulnerability Database: http://nvd.nist.gov

U.S. Computer Emergency Readiness Team: http://www.us-cert.gov

### Patch Management Guidelines

NIST Guide to Producing Operational Requirements for Security Measures:
http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf

### Firewall Selection and Use

NIST Guidelines on Firewalls and Firewall Policy:
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

ISCA Labs Network Firewall Selection:
https://www.icsalabs.com/sites/default/files/How%20to%20select%20a%20Network%20Firewall.pdf

ISCA Labs Certified Products: https://www.icsalabs.com/products?tid[]=4217

## References

*Guide to Industrial Control Systems (ICS) Security - National Institute of Standards and Technology (NIST),* Keith Stouffer, Joe Falco, Karen Scarfone – 2008

*Securing Control Systems, Department of Homeland Security,* December 2008

*Recommended Practice for Patch Management of Control Systems, Department of Homeland Security,* December 2008

*SANS Glossary of Terms,* http://www.sans.org/security-resources/glossary-of-terms

*Protecting Industrial Control Systems from Electronic Threats,* Joseph Weiss, 2010

*Verizon 2010 Data Breach Investigations Report,*
Verizon RISK Team in cooperation with the United States Secret Service

**Schneider Electric**

One High Street,
North Andover, MA 01845 USA
Telephone: +1 978 975 9600
Fax: +1 978 975 9674
www.schneider-electric.com/buildings