MANAGED BACNET™ GUIDANCE

VOLUME 1: MANUFACTURER'S GUIDE

VERSION 1

Peachtree Corners

This publication was prepared under the auspices of the ASHRAE Multidisciplinary Task Group MTG.CYB, Cybersecurity for HVAC Systemsand Related Infrastructure.

For more BACnet resources and the most updated version of Managed BACnet, please visit:
https://www.ashrae.org/technical-resources/bookstore/bacnet

Updates and errata for this publication will be posted on the ASHRAE website at www.ashrae.org/publicationupdates.

MANAGED BACNET™ GUIDANCE

VOLUME 1: MANUFACTURER'S GUIDE

VERSION 1

Peachtree Corners

180 Technology Parkway · Peachtree Corners, GA 30092 · www.ashrae.org

Printed in the United States of America
Cover photograph by Alexey Yaremenko /istockphoto.com
Cover design by December Byrnes

First printing August 2025

ASHRAE Staff

Special Publications	Cindy Sheffield Michaels, Editor
	Mary Bolton, Associate Editor
	December Byrnes, Assistant Editor
	Michshell Phillips, Senior Editorial Coordinator
Publishing Services	David Soltis, Group Manager of Electronic Products and Publishing Services
	Jayne Jackson, Publication Traffic Administrator
Director of Publications and Education	Mark S. Owen

Acknowledgments

This document was developed by participants in an industry consensus-building activity on interoperable cybersecurity and network management functionality for building automation systems (BASs), focusing on those systems that use BACnet® as their primary communication protocol. In order to accelerate adoption of cybersecurity technology, Cimetrics convened a group of like-minded individuals and companies to engage in the consensus-building activity that began early in 2020 and concluded in early 2022. The charter was to develop guidelines and marketing collateral to help standardize BACnet cybersecurity implementations in products and systems through an open, consensus-based process. Two years of work from some of the cybersecurity experts in the BAS industry resulted in the creation of the predecessor of this document, which was available for free download from the Cimetric website.

We would like to thank the consensus-building participants, the outside reviewers, and their companies for contributing their time. In particular, we acknowledge the participation of the following people in the consensus-building process:

Chariti Young, *Automated Logic*
Doyle Davidson,* *Automated Logic*
Justin Mezzadri, *Automated Logic*
Ken Gilbert, *Automated Logic*
Lori O'Neal, *Automated Logic*
Andy McMillan,* *BACnet International*
Jim Butler,* *Cimetrics*
Jim Lee, *Cimetrics*
Keith Corbett,**Cimetrics*
Paul Rensing, *Cimetrics*
Anto Budiardjo, *Cimetrics, Padi.io*
David Ritter, *Delta Controls*
David Szutu, *Delta Controls*
Ben Murra, *Honeywell HBS*
Brett Yoder, *Honeywell HBS*
Alan Bronikowski, *Johnson Controls*
Carol Lomonaco,**Johnson Controls*
Chris Lane, *Johnson Controls*
Jane Wamsley, *Johnson Controls*
Joseph Klotz, *Johnson Controls*
Josh Edler, *Johnson Controls*
Steven Bushby, *NIST*
Chris Howard, *Reliable Controls*
Michael Osborne, *Reliable Controls*
Hu Dou, *Schneider Electric*
John Smith, *Schneider Electric*
Alina Matyukhina, *Siemens*
Andre Meier, *Siemens*
Bernhard Isler, *Siemens*
Kai Rohrbacher, *Siemens*
Klaus Hartke, *Siemens*
Oscar Camenzind, *Siemens*
Thomas Kurowski, *Siemens*
Zach Netsov, *Siemens*
Steve Jones, *The S4 Group*
Steve Fey, *Totem Buildings*
Mangaya Sivagnanam,* *Trane Technologies*

The following people (starred above and listed in alphabetical order) below directly contributed to the creation of this document by writing one or more of its sections:

Jim Butler
Keith Corbett
Doyle Davidson
Carol Lomonaco
Andy McMillan
Mangaya Sivagnanam

Contents

Acronyms .....

Chapter 1: Introduction 1

1.1 BACnet and Cybersecurity 1

1.2 Leveraging Existing IT and OT Cybersecurity Standards 2

1.3 How to Use this Guide 3

1.4 Fundamental Definitions 3

Chapter 2: Functional Architecture 5

2.1 Motivation 5

2.2 Functional Roles 6

2.3 Local Network and Security Manager 6

2.4 BACnet Devices 7

2.5 Secured BACnet Gateway 8

2.6 BACnet Firewall/Router 8

2.7 IT Systems 8

2.8 Global Network/Security Manager 9

2.9 BACnet Functional Roadmap 9

Chapter 3: Implementing BACnet/SC 11

3.1 Motivation 11

3.2 Important Aspects of BACnet/SC 11

3.2.1 Heartbeat Request 11

3.2.2 Operational Certificate 12

3.2.3 DNS/mDNS Support 12

3.3 BACnet Profiles and BIBBs 12
3.4 Addendum CD and Supported Ciphers/Key Algorithms 12
3.5 Capacity 13
3.6 Optional B ACnet/SC Behavior 13
3.6.1 Timeouts 13
3.6.2 Support for (Accepting) Direct Connections 14
3.6.3 Discovery of Device's Own Direct Connect URI 14
3.7 BACnet/SC Configuration 14
Chapter 4: IT Network Access 15
4.1 Motivation 15
4.2 Security Considerations 16
4.3 Product and Project Documentation 17
4.4 Network Access Control 18
4.5 Network Address Assignment and Name Resolution 19
4.6 Time Services 20
4.7 References and Related Resources 22
Chapter 5: BACnet/SC Device Oboarding 25
5.1 Motivation 24
5.2 Security Considerations 24
5.3 BACnet/SC Onboarding Guidelines 25
5.4 Interoperable Onboarding Guidelines 26
5.5 References and Related Resources 26
Chapter 6: BACnet/SC Certificate Management 27
6.1 Motivation 27
6.2 Security Considerations 29
6.3 Device Guidelines 30
6.4 Certificate Signing Guidelines 31
6.5 References and Related Resources 31
Chapter 7: Device Reset 33
7.1 Motivation 33
7.2 Security Considerations 34
7.3 Device Guidelines 34

7.4 References and Related Resources....35

Chapter 8: Identity Authentication 37

8.1 Motivation 37
8.2 Security Considerations 38
8.3 BAS User Guidelines 39
8.4 BAS System User Authentication Guidelines 39
8.5 References and Related Resources....40

Chapter 9: Authorization 43

9.1 Motivation 43
9.2 Security Considerations 44
9.3 Device Guidelines 45
9.3.1 Workstation/Server Capabilities 46
9.3.2 Device Capabilities 46
9.3.3 Online BACnet Authorization 47
9.4 References and Related Resources....47

Chapter 10: Secure Product Development and Vulnerability Management 49

10.1 Product Vulnerability Management Guidelines....49
10.2 References and Related Resources 49

Chapter 11: Firmware Updates....51

11.1 Motivation 51
11.2 Security Considerations 52
11.3 Device Guidelines 52
11.4 References and Related Resources 54

Chapter 12: Backup and Restore....55

12.1 Motivation 56
12.2 Security Considerations 56
12.3 Device Guidelines 57
12.3.1 General Capabilities 57
12.3.2 Online BACnet Backup and Restore 58
12.4 References and Related Resources 58

Chapter 13: System Diagnostics....59

13.1 Motivation 59
13.2 Security Considerations 60
13.3 Device Monitoring Guidelines 61
13.3.1 BACnet Device Object 61
13.3.2 Network Port Object 61
13.3.3 IT Device Monitoring 62
13.4 Network/Security Event Logging 62
13.4.1 Local Logging 63
13.4.2 BACnet Alerts 63
13.4.3 IT Protocols 63
13.5 Network Message Capture 64
13.5.1 BACnet Hub/Device "Above WebSocket" Message Capture 64
13.5.2 Full Network Message Capture 65
13.6 References and Related Resources 65
Chapter 14: Network Segmentation 67
14.1 Motivation 67
14.2 Security Considerations 68
14.3 Network Environment Guidelines 68
14.3.1 Network Isolation 68
14.3.2 IT Firewall Compatibility 69
14.4 BACnet Firewall/Router Guidelines 69
14.4.1 Monitoring/Filtering 69
14.4.2 Island Mode 72
14.5 References and Related Resources 72
Chapter 15: Mapping Recommendations to the BACnet Standard 75
Appendix A: A Brief History of BACnet Cybersecurity 81
References 83

Acronyms

ACE	authentication and authorization for constrained environments
BACnet/SC	BACnet Secure Connect
BAS	building automation systems
BBMD	BACnet broadcast management device
BIBBs	BACnet interoperable building blocks
BMS	building management systems
BRSKI	Bootstrapping Remote Secure Key Infrastructure
CA	certificate authority
CIA	confidentiality, integrity, availability
CSR	Certificate Signing Request
CVRF	Common Vulnerability Reporting Framework
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	denial of service
EAP	Extensible Authentication Protocol
EDE	engineering data exchange
EEPROM	Electrically Erasable Programmable Read-Only Memory
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	identification and authorization
IACS	industrial automation and control system
IoT	Internet of things
IP	Internet protocol
IT	information technology
MAC	mandatory access control
MFA	multifactor authentication
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
MUD	manufacturer usage description
NAT	Network Address Translation

NOC	network operations center
OT	operational technology
PAT	project address table
PEM	Privacy Enhanced Mail
PICS	protocol implementation conformance statement
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
SADR	SuperAgent Distributed Repository
SAN	Subject Alternative Name
SDL	Security Development Lifecycle
SIEM	security information and event management
SNMP	Simple Network Management Protocol
SOC	security operations center
SZTP	Secure Zero Trust Provisioning
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOFU	Trust on First Use
TP	True positive
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
UTC	Utilities Technology Council
VLAN	Virtual Local Area Network
VMAC	Virtual Machine Access Control
VPN	Virtual Private Network

1

Introduction

This document provides manufacturers with technical guidance on implementing products and systems that utilize BACnet® inherent security capabilities and align with information technology (IT) best practices. It is the first volume of an anticipated series of Managed BACnet™ books, articles, handouts, and worksheets in the field of data communication protocols for building automation and control networks, with future volumes set to address other actors in the building automation systems (BAS) value chain (such as owners, building operators, integrators and consulting engineers).

Note that Managed BACnet™ is a term trademarked by ASHRAE and may not be used other than in reference to this document series. No product or system can claim compliance or conformation with the documents in this series or be identified as implementing Managed BACnet™.

The BACnet Standard, ANSI/ASHRAE Standard 135, was initially developed at a time when cybersecurity of BASs was not a significant issue and alignment with IT best practices was not critical. That is no longer the case. The increasing interconnection of BASs with IT systems and the dramatic rise in cybersecurity risks are changing the requirements and expectations of BASs regarding cybersecurity and alignment with IT best practices.

This document aims to guide developers of BACnet products and systems about IT requirements and expectations. It addresses issues that may be of interest to others in the BAS community, including some integrators and knowledgeable end users but is not written with those audiences in mind. It is necessarily technical in nature and assumes familiarity with IT networking and BACnet concepts. Casual readers may find the most useful parts of this document are sections 1.1 through 1.4 and the recommendation summary table in Chapter 15.

This document focuses on product and system functionality, but it is important to recognize that system cybersecurity is achieved through the successful application of an effective, ongoing process by the organization that is managing the system. The NIST Cybersecurity Framewor (NIST 2018) can help organizations develop appropriate processes to assess and manage their cybersecurity risk. Well-designed products and systems are necessary to address cybersecurity, but they are not sufficient. Developing and applying a risk mitigation process is ultimately the responsibility of the managing organization and their service providers.

1.1 BACnet and Cybersecurity

The BACnet Standard and commercial product compliance testing have enabled broad interoperability among different vendors' BAS products. The release of BACnet Secure Connect (BACnet/SC)

combined with other optional features in the BACnet Standard, utilizes current IT technologies to address important elements of modern, interoperable cybersecurity functionality. However, cybersecurity is broader than BACnet and is advancing at a rapid pace, whereas ASHRAE's standards development process is intentionally measured. This guide is intended to bridge the gap between IT cybersecurity expectations of BAS and the cybersecurity functionality provided in the BACnet Standard at the time this document was written. As such, this document includes recommendations on topics not addressed in the BACnet Standard and it may be revised more frequently than the BACnet Standard itself. To ensure you have the latest version of this document check the version number of the most recent PDF on ASHRAE's website at https://www.ashrae.org/technical-resources/bookstore/bacnet.

This document references the BACnet Standard including relevant addenda[1]. It also references a broad set of other industry standards and best practices relating to cybersecurity.

A brief history of BACnet cybersecurity initiatives can be found in Appendix A. Note that the BACnet committee is continuing to develop new BACnet-specific network security technology. For an overview of some current and potential future work, see section 2.9.

1.2 Leveraging Existing IT and OT Cybersecurity Standards

At an industry level, investment in information technology (IT) is dramatically larger than investment in operational technology (OT), of which building automation is a part. In addition, building automation (and all OT) exists in a ubiquitous IT environment. So, it is no surprise that one objective of the BACnet community (and this document) is to take advantage of IT investment by leveraging IT cybersecurity and network management standards that complement BACnet/SC and are relevant to building automation.

There are so many cybersecurity standards and guidelines that are potentially relevant to OT that it can be difficult to know which of these are the most relevant to the manufacturers of building automation products and systems. One family of standards, ISA/IEC 62443, provides a framework for selecting relevant standards and guidelines, as it specifies general cybersecurity requirements for industrial automation and control system (IACS) components and systems that could be satisfied using a variety of technologies. Although, the ISA/IEC 62443 Standards were developed for industrial and process control, a subset of the requirements are generally applicable to building automation.

The ISA/IEC 62443 series is structured in several parts, each of which addresses a major topic. The following parts are particularly relevant to BAS manufacturers:

Part 3-3: System security requirements and security levels

Part 4-1: Secure product development lifecycle requirements

Part 4-2: Technical security requirements for IACS components

Parts 3-3 (2013) and 4-2 (2018b) of ISA/IEC 62443 were particularly influential during the development of this document.

It should be emphasized that this document is not intended to replace or modify existing industry standards related to OT cybersecurity. By including and restating specific requirements and recommendations found elsewhere, including the BACnet Standard, the authors of this document have attempted to highlight some good practices that are relevant to cybersecurity in BACnet systems.

1. Approved and published addenda for ASHRAE Standards are available at www.ashrae.org/addenda.

1.3 How to Use this Guide

This guide is organized into topic-specific sections, each of which includes background and other relevant information, and some of which include specific recommendations. Chapter 2 focuses on system architecture and design context for the subsequent chapters. Chapters 3 through 14 include specific recommendations in addition to references and commentary about their respective topics. Chapter 15 summarizes the most important recommendations and identifies which can be achieved by appropriate option selections available in BACnet and which are outside the current scope of the BACnet Standard.

Most recommendations have a unique identifier with the following structure: XX-YY, where XX is an abbreviation that refers to a major section of this document and YY is a number that identifies a recommendation within that section. The following list enumerates the abbreviations used in recommendation identifiers:

AZ	Authorization
BR	Backup and restore
BSC	BACnet/SC implementation
CM	BACnet/SC certificate management
DO	BACnet/SC device onboarding
DR	Device reset
FWU	Firmware update
IA	Identity authentication
NAC	IT network access
NSEG	Network segmentation
SD	System diagnostics
VUL	Vulnerability management

In the context of this document's recommendations, *shall* indicates manufacturers should assume that project specifications will require this functionality in secure systems, *should* indicates that users will prefer systems to be secured with this functionality, and *may* indicates users may choose to include this functionality in secure systems. Here are some examples:

> **NAC-9** Devices that support BACnet/IP (defined in Annex J of the BACnet Standard):
>
> **Shall** support IPv4, as required by the BACnet Standard.
>
> **DR-2** A device **should** provide the user with feedback about the success/failure of an attempted reset.
>
> **CM-7** Devices and management tools **may** use standard protocols for detecting certificate revocation, such as Online Certificate Status Protocol (X.509 OCSP) or Certificate Revocation List (IETF RFC 5280).

1.4 Fundamental Definitions

Addendum xx*:* an addendum to ANSI/ASHRAE Standard 135-2020.

ARCNET: the communication protocol defined in ATA 878.1-1999.

BACnet Standard*:* ANSI/ASHRAE Standard 135-2020, *BACnet—A Data Communication Protocol for Building Automation and Control Networks*, otherwise known as the BACnet Standard.

BACnet: the communication protocol defined in ANSI/ASHRAE Standard 135-2020.

BACnet BIBB, or simply a *BIBB*: a BACnet interoperability building block as defined in Annex K of the BACnet Standard.

BACnet device, or simply *device*: is a device that communicates using BACnet.

BACnet PICS: a protocol implementation conformance statement as defined in Annex A of the BACnet Standard.

BACnet system: a system that primarily uses BACnet for communication between its devices.

BACnet/IP: the communication method defined in Annex J of the BACnet Standard.

BACnet/SC: BACnet Secure Connect; the communication method defined in Annex AB of the BACnet Standard.

IETF: the Internet Engineering Task Force (see www.ietf.org).

OAuth: a protocol for authorization that was developed by the IETF.

OT: operational technology is a counterpart to IT that covers a wide range of automation systems including building automation, manufacturing systems, process control systems, utility automation systems, and others.

SSL certificate: digital certificate that authenticates the identity of a website or an IP-enabled device and enables the establishment of an encrypted connection.

TLS: network protocol Transport Level Security version 1.3 defined in IETF RFC 8446, unless otherwise specified.

WebSocket: network protocol defined in IETF RFC 6455.

2

Functional Architecture

This document identifies a collection of features for interoperable management of network and security functions in BACnet® systems. Devices can implement those features and claim support for a particular BACnet protocol revision and support for specific BACnet interoperable building blocks (BIBBs). The functional architecture describes how management functions, device functions, and external systems fit together to provide a complete solution based on BACnet/SC. The functional architecture also provides a framework for evaluating future network and security capabilities in BACnet.

2.1 MOTIVATION

BACnet/SC Configuration and Certificates—BACnet/SC devices need to be provided with configuration settings and cryptographic certificates (onboarded) to be able to connect to the network. Once connected to the BACnet/SC network, devices require ongoing configuration and certificate management. Devices from multiple vendors need to interact with a single site certificate authority and need to coordinate configuration management. The functional architecture defines manager and device roles for BACnet/SC configuration.

Support Owner Cybersecurity Processes—Cybersecurity is a process, not a feature, so a BACnet system needs to provide support for owner/operator processes implementing cybersecurity best practices. The NIST Cybersecurity Framework identifies categories of requirements for such processes, organized by the functions of Identify, Protect, Detect, Respond, andRecover (2018). The functional architecture defines roles to support cybersecurity processes for IT systems and elements within the BACnet system.

Zero Trust—The paradigm of a zero trust security posture in a system means moving responsibility for enforcing security to the endpoints in the system. This means requiring authorization of network requests by BACnet devices—not relying solely on authorization policy enforcement by servers or operator workstations. Endpoint authorization is one part of a defense-in-depth strategy—also including physical and virtual network isolation, features in network infrastructure (such as IT firewalls and switch/router-based monitoring), and user authentication and authorization in servers and workstations. The functional architecture identifies a trusted central server to manage BACnet device authorization policy using the OAuth model to minimize configuration burden on BACnet devices, which is consistent with addendum cp of the BACnet Standard.

System Migration—There is a need to support network/security management as existing systems are migrated to include BACnet/SC. The functional architecture identifies network and security features to be located at connections to existing BACnet networks and non-BACnet systems.

Integration with IT Network and Security Systems—At many sites, BASs need to interact with cybersecurity and network IT organizations. IT network protocols and tools evolve rapidly, so the architecture insulates BAS devices (which may have an installed lifetime of 10 to 20 years and lower capability than IT equipment) from quickly changing IT requirements.

Evolutionary—The functional architecture supports an ongoing roadmap for cybersecurity features in BACnet.

Multiple Management Models—The architecture includes network/security functionality that is delivered via distinct models: continuous active management of devices (e.g., monitoring or backup service), online services for devices to use (authorization server, receiver of notifications), and periodic management of devices (i.e., maintenance and onboarding—certificate management). Some management functions are then delivered by services which are always connected to the network, whereas others may be delivered by transient maintenance tools.

2.2 Functional Roles

Management functionality starts with the capabilities of the devices that are connected to a BACnet/SC network. They use secure communication (BACnet/SC), expose configuration and management interfaces, and may enforce authorization policy. Day-to-day monitoring and management of the devices is handled by the Local Network and Security Manager, which also acts as an interface to IT systems and broader, cloud-based management. Connections to existing BAS networks (e.g., BACnet/IP and MS/TP) are made via BACnet gateways and BACnet firewall/routers. The roles work together to allow the system to be managed and to implement cybersecurity processes.

2.3 Local Network and Security Manager

Day-to-day monitoring and management of the devices is handled by the Local Network and Security Manager. It is connected to the BACnet/SC network and is typically located on-site. The role

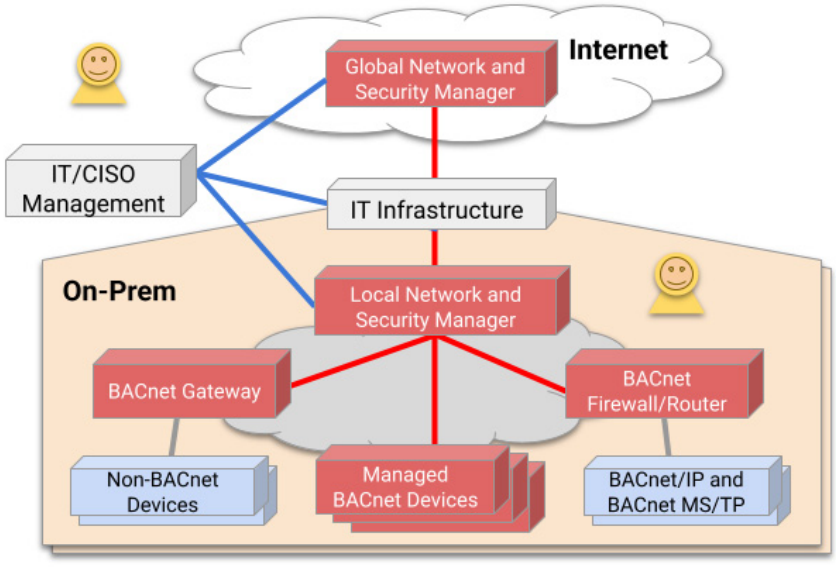

Figure 2.1 Generic Managed BACnet™ architecture.

of Local Network and Security Manager may be taken on by a BAS server, workstation, large controller, or maintenance tool. Like all BACnet/SC devices, a Local Network and Security Manager may also function as a BACnet/SC primary hub or failover hub.

Continuous Active Management—Some functions are ongoing active management, where the Local Network and Security Manager actively queries the devices—examples include monitoring for diagnostics and performing backups. The Local Network or Security Manager performs these functions in an unattended manner, but it could raise notifications to building management system (BMS) operators or IT systems.

Online Services—Some functions are provided by an ongoing network service that devices can access. For example, authentication and authorization servers (for BACnet/SC devices) are expected to be available on the network. Similarly, a Local Network and Security Manager may include a service acting as a receiver of network/security events, sent by devices as BACnet alert notifications (see Clause 13.2 of the BACnet Standard). BACnet devices would be preconfigured with the location and credentials of each of the online services they wish to use or support dynamic subscription if they wish to send notifications.

Periodic Management—Some functions are provided during commissioning and periodic maintenance, typically under user control (service personnel or on-site operators). The functions may be provided by a maintenance tool or by a privileged application in a BAS server or workstation. Examples of periodic management functions include network/security configuration changes, certificate management, firewall policy, authorization configuration changes, firmware updates, and device restore.

Interfaces to IT Systems—The Local Network/Security Manager may support interfaces to IT systems via common IT protocols. In some sites, IT systems may provide some functions that would otherwise be provided directly by the Local Network/Security Manager, such as certificate enrollment, user authentication, and event logging. The Local Network/Security Manager can function as a proxy for BACnet devices at such sites, so simple BACnet devices do not need to support a rapidly evolving set of IT protocols.

Local Network/Security UI—BAS servers and workstations provide a user interface to the building systems for local operators and service personnel. Those existing interfaces need to be extended or an additional user interface needs to be provided for viewing and managing network/security functions of the system.

Interface to Cloud Services—The Local Network and Security Manager may support interfaces to functions provided by an off-site Global Network and Security Manager.

2.4 BACnet Devices

The main responsibility of most BACnet devices is controlling building systems or equipment. They have certain responsibilities within the functional architecture to allow scalable, interoperable management of their network/security functionality.

Secure Local Capabilities—Vendor-specific tools or local management interface—onboarding, engineering, device reset, restore from backup, firmware updates, and restore.

Continuous and Periodic Management—A BACnet/SC device will support objects, services, and procedures to allow its network and security functions to be managed by the Local Network and Security Manager.

Ongoing Management Services—A BACnet/SC device will make use of services provided by the Local Network and Security Manager as needed. These BACnet devices would be preconfigured with the location and credentials of each of the online services they wish to use or would support dynamic subscription if they wish to send notifications.

2.5 Secured BACnet Gateway

A secured BACnet gateway provides the features of a BACnet/SC device for its network/security functionality. Its primary responsibility is data exchange between BACnet devices and devices (BACnet or otherwise) connected to networks using different protocols. It may have additional capabilities to enforce authorization policy or provide monitoring between the two systems.

2.6 BACnet Firewall/Router

BACnet defines a unique Network Layer and BACnet-specific router behavior between BACnet network segments. A BACnet firewall/router adds filtering and monitoring capabilities based on the content of BACnet messages (service type, source addresses, and destination addresses). A BACnet firewall/router also provides the features of a BACnet/SC device for its network/security functionality.

The BACnet firewall/router thus allows security policy to be enforced at connections to BACnet segments which are not BACnet/SC. It also allows BACnet systems to be segmented into distinct security domains (see Chapter 14).

2.7 IT Systems

IT organizations often provide some of the network infrastructure used by BASs and hence provide network and security configuration parameters for BAS devices. IT may wish to control the issuing of certificates at a site. IT groups may need visibility into BASs for diagnostics and security. There may be multiple IT groups interested in BAS systems, including a network operations center (NOC) reporting to the Chief Information Officer (CIO) and a security operations center (SOC) reporting to a Chief Information Security Officer (CISO).

The Local Network and Security Manager may provide interfaces to IT systems. Some IT systems may interact directly with the devices. Some functionality that IT systems may provide is as follows:

- Network configuration (DHCP, DNS, firewalls [VPN], routers [NAT], switches [VLAN])
- Onboarding/certificate management
- User authentication
- Device authentication (IEEE 802.1X)
- Network monitoring
- Security monitoring

At sites where there is no separate IT organization, the BAS group may have responsibility for managing the network infrastructure and for cybersecurity oversight.

2.8 Global Network/Security Manager

The Global Network/Security Manager provides off-site management functionality in situations where the Local Network and Security Manager is not sufficient. The Global Network/Security Manager may be hosted in the cloud or an organization's data center.

Remote Management—Some sites may not have IT organizations or on-site staff to oversee network/security functions. The Global Network/Security Manager may provide a remote interface for specialist staff or third-party service providers.

Multiple Site Management—Organizations with multiple sites may benefit from integrating management information from multiple Local Network and Security Managers. The Global Network/Security Manager may support applications across multiple sites.

Off-Site Secure Storage—There may be advantages to remote storage for information generated by the Local Network and Security Manager. For example, the ability to archive log files may be useful for forensics, since intrusions may occur many months before they are detected. Organizations may do off-site storage of backups.

Advanced Applications—Advanced applications (such as cybersecurity analytics or vulnerability tracking) making use of information from the Local Network and Security Manager may be provided by the Global Network/Security Manager.

Interfaces to IT Systems—The Global Network/Security Manager may support interfaces to IT systems via common IT protocols.

2.9 BACnet Functional Roadmap

Interoperable network/security features are added to the BACnet Standard via addenda, which must pass through an ASHRAE/ANSI approval process. Vendors then decide when to add features to products, conforming to a newer BACnet protocol revision. The industry then supports the development of conformance tests of new BACnet features under the auspices of the BACnet testing laboratories.

The management functionality described in this document exists within a roadmap of iterative adoption of proprietary and interoperable capabilities. The functionality descriptions then include the following:

- Guidelines for device and system best practices for implementing proprietary features
- Guidelines for implementing interoperable features that are approved parts of the BACnet Standard
- Identified features that are currently under development by the BACnet committee
- Identified features where there was consensus on a high-level design in principle and in the near future a proposal could be discussed in the BACnet committee
- Identified features that are expected to be considered by the BACnet committee in the future (such as applying Authorization to existing BACnet network and security management features)

Table 2.1

Feature	BACnet Standard (ASHRAE 2020) Update	Status
BACnet/SC	Defines BACnet Secure Connect (BACnet/SC) in Annex AB	Approved Nov. 2019 as addendum bj
BACnet/SC Cipher Suite	Update Annex AB to clarify minimum required TLS capabilities for BACnet/SC implementations	Approved Aug. 2021 as **addendum cd**
BACnet/SC Network Port Object	Update Clause 12.56, Network Port Object Type, for BACnet/SC and add to Clause 19 procedures for online replacement of certificates used in BACnet/SC	Approved Jan. 2022 as **addendum cc**
Authorization	Define device authentication and request authorization data options and required behavior	Approved Nov. 2024 as **addendum cp**
Authorization Configuration	Define object types or a file definition for interoperable configuration of device Authorization policy	
Onboarding	Define a standard file format for off-line certificate data interchange during BACnet/SC device onboarding	Approved June 2024 as **addendum cs**
Onboarding	Define new Clause 19 Procedure for Online Trust on First Use (e.g., /IP to /SC bootstrap)	
Onboarding	Define new Clause 19 Procedure for Secure Onboarding (BRSKI)	
Certificate Management	Update BACnet Network Port Object procedures to use Authorization	
Firmware Updates	Define new Clause 19 Procedure using Authorization	
Backup and Restore	Update Clause 19.1 Procedure to use Authorization	
Time Management	Update BACnet's UTCTimeSynchronization Service to use Authorization	
Network/Security Events	Define new Clause 19 Procedure using BACnet Alerts and Authorization	Consensus on design in principle.*
Audit Logs	Update Clause 19.6 Procedure to use Authorization	
Network Segmentation	Define new Clause 19 Procedure for BACnet Firewall/Router behavior	Consensus on design in principle.*
BIBBs and Profiles	Define new BIBBs and profiles for interoperable cybersecurity-related functionality	

* *Consensus was reached among the participants in the consensus-building activity described in the Acknowledgments of this document.

3 Implementing BACnet/SC

The availability of BACnet/SC (secure connect data link) is a catalyst for improving the cybersecurity of BACnet® systems. It is defined in Annex AB of the BACnet Standard, along with addendum cd of the BACnet Standard which specifies the Transport Layer Security (TLS) V1.3 Cipher Suite Application Profile for BACnet/SC.

BACnet/SC topology is that of a hub-and-spoke model consisting of a centralized hub with an optional failover hub and multiple BACnet/SC nodes. Optionally BACnet/SC nodes may support direct connections with other BACnet/SC nodes on the same BACnet/SC network.

BACnet/SC implementations are complex due to credential configuration and the use of third-party libraries for WebSocket, TLS, and the associated cipher suites. These complexities can impede interoperability and ease of configuration, thus the need for these guidelines for BACnet/SC implementation and configuration features.

3.1 Motivation

Secure Connection—BASs have traditionally been implemented using insecure protocols over data communication technologies such as IPv4, IPv6, Ethernet, MS/TP, and ARCNET. Insecure networks are no longer acceptable, and having a secure data link for BASs is a necessity.

Security has traditionally relied on physical security of the network, IT network isolation, and other IT practices. While it is quite possible to achieve a secure BACnet network using standard IT network security practices, BACnet/SC provides a leap forward in simplifying the security of BACnet systems. Additionally, BACnet/SC can contribute to system defense-in-depth by adding another layer of protection.

3.2 Important Aspects of BACnet/SC

3.2.1 Heartbeat Request

The heartbeat request is defined to send by initiating BACnet/SC node per Clause AB.6.3 of the BACnet Standard for the purpose of keeping established BACnet/SC connections alive. The accepting BACnet/SC node can also initiate a heartbeat request at any time. Thus, all devices must be capable of responding to a heartbeat request at any time.

3.2.2 Operational Certificate

A BACnet/SC device's operational certificate is defined to be validated against the directly signed certificate authority (CA) certificate. This could be a root CA or an intermediate CA depending on how the certificates are signed. This is unlike typical web browsers where any CA in the certificate chain may be used to validate a certificate.

Addendum cc of the BACnet Standard also restricts there to be at most two issuer certificate files for each BACnet/SC connection: one for the network's active certificate authority (CA and a second for transitioning to a new CA. Once the transition is completed the old CA should be removed. This means that all devices on a BACnet/SC network will use the same single CA for validating connections when not transitioning to a new CA.

For more information on certificate management, see Chapter 6.

3.2.3 DNS/mDNS Support

BACnet/SC device URIs may often be defined using host names instead of IPv4/IPv6 addresses. While not strictly required for BACnet/SC, devices should support DNS or mDNS as clients and declare such support on the BACnet PICS.

3.3 BACnet Profiles and BIBBs

Annex A of the BACnet Standard defines the BACnet Protocol Implementation Conformance Statement (PICS) that lists device capabilities and standard profiles supported.

> **BSC-1** Manufacturers **should** provide a BACnet PICS statement for all devices that support BACnet/SC. This **shall** include supported TLS versions, additional supported cipher suites, digital signatures, and key exchanges.
>
> **BSC-2** Devices supporting BACnet/SC hub functionality **shall** conform to profile B-SCHUB (including NM-SCH-B).
>
> **BSC-3** Devices initiating direct connections **shall** support NM-SCDC-A.
>
> **BSC-4** Devices accepting direct connections **shall** support NM-SCDC-B.

Devices managing BACnet/SC certificates using the process defined in addendum cc shall implement NM-SCCM-A. There is no explicit "B side" of this BIBB. The supporting behavior is required to be present to support the changes required for BACnet/SC in the Network Port Object per addendum cc.

3.4 Addendum cd and Supported Ciphers/Key Algorithms

Addendum cd of Standard 135 specifies the TLS V1.3 Cipher Suite Application Profile for BACnet/SC. Specifically it states the following:

> *BACnet/SC implementations shall support TLS version 1.3 as specified in RFC 8446. BAC net/SC implementations shall support the following TLS V1.3 cipher suite application profile. For the definition of the terms in quotes see RFC 8446:*
>
> *a. TLS cipher suite TLS_AES_128_GCM_SHA256,*
> *b. digital signature with ecdsa_secp256r1_sha256, and*
> *c. key exchange with secp256r1.*

These are the minimum requirements. It is recommended that all BACnet/SC devices support more than the minimum cipher suite profile since some IT departments and installations may not be prepared to support elliptic curve or may have policies that favor (or deprecate) the use of specific cipher suites.

There are five standard cipher suites in TLS V1.3: the one above plus four more. More common and should be supported are:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA25

Less common and may be supported are:

- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

The BACnet Standard permits devices to be configured to use TLS V1.2 as a local matter. This may be a customer requirement though it may create interoperability problems for devices that do not include support for TLS V1.2.

> **BSC-5** Devices capable of supporting TLS connections below version 1.3 **shall** provide a way to prevent the TLS connection from downgrading for a standard strict TLS 1.3 system.

3.5 Capacity

When providing a PICS for BACnet devices, the BACnet/SC device capabilities, and maximum capacities shall be listed in the respective sections of the standard PICS. This should include the following:

- If initiating direct connections is supported, the maximum number of simultaneous direct connections initiated
- If accepting direct connections is supported, the maximum number of simultaneous direct connections accepted
- If the hub function is supported, the maximum number of simultaneous node connections accepted
- Additional cipher suites supported beyond those required for TLS V1.3
- Additional TLS versions other than V1.3 supported

3.6 Optional BACnet/SC Behavior

3.6.1 Timeouts

The BACnet/SC data link was published as an addendum to the BACnet Standard that did not require a specific protocol revision. Addendum cc added support for BACnet/SC to the Network Port Object and made some minor changes to the BACnet/SC specification, but it cannot be implemented in devices until BACnet protocol revision 24 is supported.

The reconnect timeout in Annex AB of the BACnet Standard has been changed to be two separate timeouts in the Network Port Object in addendum cc. Specifically, it is split into SC_Minimum_Reconnect_Time and SC_Maximum_Reconnect_Time.

Addendum cc recommends the following default values:

- SC_Connect_Wait_Timeout of 10 seconds
- SC_Disconnect_Wait_Timeout of 10 seconds
- SC_Heartbeat_Timeout of 300 seconds

3.6.2 Support for (Accepting) Direct Connections

BACnet/SC direct connection is optional functionality for transmitting unicast BACnet messages. It allows two devices on the same BACnet/SC network to directly communicate and bypass the BACnet/SC hub for non-broadcast communication if the network fabric is configured in such a way as to allow direct communication. Note that BACnet/SC devices are required to maintain a connection to the BACnet/SC hub at all times.

This can be useful to provide network resiliency or when there is a large amount of traffic that must be transmitted between two devices and they do not wish to burden the hub with the additional traffic to reduce latency. Examples include daily/weekly trend data collection, firmware updates, and bulk configuration changes. It can also be useful when initially setting up and configuring a BACnet network.

> **BSC-6** Devices **may** support accepting BACnet/SC direct connection functionality to respond to high-traffic situations. Devices that support accepting direct connections **shall** support NM-SCDC-B.
> **BSC-7** Devices that initiate high-traffic operations **may** support initiating BACnet/SC direct connection functionality. Devices that support initiating direct connections **shall** support NM-SCDC-A.

The use of direct connections may vary by manufacturer due to device capability and implementation. Its use may also vary based on the actual system installation, network topology, network performance, and cybersecurity policy.

3.6.3 Discovery of Device's Own Direct Connect URI

Addendum cc of the BACnet Standard introduced the SC_Direct_Connect_Accept_URIs' property, which is an array of URI strings. It shall be configurable. Its value may be automatically initialized based on the device's assigned IP address if no other value has been configured.

3.7 BACnet/SC Configuration

As noted above, Annex AB of the BACnet Standard specifies the BACnet/SC data link but was not precise about the configuration of its parameters. Proprietary configuration mechanisms should align with the Network Port Object changes in addendum cc of the BACnet Standard. The initial configuration features shall be compatible with the recommendations in Chapter 5.

Future:

Many BACnet/SC parameters are defined as Network Port Object properties in addendum cc and are required to be ***configurable*** (using a vendor-defined mechanism). It is likely that a future addendum will define standard Authorization requirements for writing to those properties using standard BACnet services, and it may require some properties to be ***writable*** (using a standard BACnet service).

4

IT Network Access

It is increasingly the case that BAS networks share some network infrastructure with systems that support other applications, but BAS/OT Ethernet networks may also be implemented, in their entirety or in part, via cabling and switches that are not part of an IT-managed network. Many variations are possible, such as the following:

- The BAS/OT network could be isolated (completely or via a firewall) from the IT network.
- The BAS/OT network could be implemented using managed switches.
- The BAS/OT network could be virtually isolated using VLANs and/or VPNs.
- The BAS/OT network could include daisy chains of unmanaged switches (built into BAS controllers) connected to the managed switch fabric.
- The BAS/OT network could be implemented using industrial-grade switches in a ring topology using rapid-spanning tree or Media Redundancy Protocol (MRP) for redundancy.

Building automation devices that are designed to be able to connect to actively managed network fabric are expected to support common IT protocols and meet certain product security requirements. Support for the core TCP/IP network protocols is assumed, and some are required for BACnet/IP and BACnet/SC, but there are several other useful protocols that are relevant to granting and managing devices' access to a network. This chapter provides an overview of network access, from product documentation to protocols and services.

4.1 Motivation

Restricting Network Access to Authorized Devices—To improve the security of network-connected systems and devices, only authorized devices should be permitted to connect to the BAS network.

Device Configuration Options—Devices should be able to be configured to comply with the customer's network policies, such as the use of IPv4 vs. IPv6 and static vs. dynamic address assignment.

Device Management—The use of certain network protocols allows network management personnel to monitor and manage network-connected devices more effectively. Protocols in this category include DHCP, DNS, and NTP.

Restricted Network Protocols—Some network protocols might not be permitted to be used due to cybersecurity concerns. Protocols in this category include Telnet, FTP, HTTP, SSL (and older versions of TLS), and WEP.

Ensuring that Software is Up-to-Date—By policy, certain types of devices may be required to have approved software patches installed before they are allowed to connect to the network. Ensuring that automation systems have up-to-date software is typically divided between the IT personnel (server and workstation operating systems) and the BAS vendor (BAS-specific applications and controllers).

Changes in Network Policies—Over the expected life of BAS devices, network policies are likely to change. For example, the management of BAS networks deployed during building construction may be turned over to IT groups that have different policies.

4.2 SECURITY CONSIDERATIONS

When BAS devices are connected to managed network fabric, the BAS devices are potentially exposed to attacks from or through misconfiguration of non-BAS devices. Likewise, non-BAS devices are potentially exposed to attacks from or misconfiguration of BAS devices. IT personnel are increasingly interested in ensuring that connected devices, including BAS devices, meet minimum security requirements.

The connection of unauthorized BAS devices to a BAS network presents a potential risk to the operation of the BAS and to other connected systems.

Devices that have software with known, exploitable vulnerabilities are a security risk to all other devices connected to the same network fabric.

BAS devices' use of ports and protocols should be known by network management personnel so that firewalls and network monitoring tools can be configured appropriately.

The current time is needed for several BAS and IT functions, including scheduled equipment operation, logging, and certificate validation. This requires reliable time synchronization from trusted sources. BACnet®'s time synchronization services do not have authorization and may not be derived from verified time sources, but for many BACnet devices (e.g., those that communicate using MS/TP) there is currently no realistic alternative.

Potential mitigations include the following:

1. BAS devices can be connected to dedicated, physically isolated network infrastructure.
2. Shared network fabric may be configured to provide virtual isolation of the BAS devices from other network-connected devices.
3. Managed network switches often have the capability to disable unused ports or to prevent unauthorized devices from joining the network. RADIUS servers can be used, in conjunction with compatible managed switches or access points, to control access to network resources at the point of connection to the network fabric. (Note: RADIUS is a networking protocol that enables centralized authentication and authorization of users who want to access a remote network.)
4. Automated methods for detecting devices that contain software with known, exploitable vulnerabilities can be applied.
5. BAS software should support patch management processes.

4.3 Product and Project Documentation

Product network and security documentation is needed for the specification/bid process, security reviews of proposals, and inclusion in submittals. Product network and security documentation should also be made available to end customers upon request.

NAC-1 Product suppliers **should** be able to provide the following documentation during the specification/bid process:

- Product cut sheet
- BACnet PICS for each model of BACnet device
- BTL certification documentation if applicable

NAC-2 Product suppliers **should** be able to provide product security documentation, which may include the following:

- Product hardening recommendations (documentation to configure a device to meet certain security requirements).
- Data encryption capabilities (hash strength, use of hardware modules such as a TPM).
- FIPS 140/ IEC 62443 compliance status.
- Local user account password management policy (complexity, multifactor authentication, expiration, etc.).
- Local display/UI: describe the user authentication mechanism (e.g., PIN, simple password, or integrated with user account).
- Local physical management ports (Ethernet, serial) and access methods (HTTPS, SSH, TTY).
- Types of reset operations that are supported, including a description of the data that is retained for each type. See Chapter 7 for additional information.
- How conformance to the principle of least privilege is achieved.

NAC-3 Product suppliers **should** be able to provide documentation of standard network port usage:

- **Should** include a list of network ports and protocols used by each type of product:
  - Open server ports.
  - Destination ports of client protocols.
  - Whether the ports are used to access services outside of the BAS or to provide services to devices that are outside of the BAS.
- **May** include protocol versions supported (including references to RFCs or other standards), protocol options supported, and whether the use of specific protocol versions can be disabled.
- **Should** enumerate cipher suites that are supported.
  - Note that products that support BACnet/SC **shall** enumerate the TLS versions and cipher suites supported for BACnet/SC in the product's BACnet PICS, in accordance with the requirements in Annex A and addendum cd of the BACnet Standard.
- **May** include a machine-readable declaration, such as a manufacturer usage description (MUD) document.

Project documentation should be submitted to the building owner as a project deliverable. This ordinarily includes project-specific information such as system design, product usage, and product

configuration options. Manufacturers may provide resources to allow channel partners to generate project documentation upon request.

NAC-4 BAS installers/integrators will be expected to provide building owners with project-related documentation of BASs, networks, and security. BAS vendors' systems and tools **should** facilitate the creation of the following types of documentation:

- **May** include message flow diagrams:
  - Sequence diagrams for common flows.
  - Typical messages between devices.
- **Should** include Network Topology diagrams.
  - Specifically indicate the intersection of BAS and IT networks.
  - Indicate remote access requirements (if permitted).
- **May** include estimates of Network Utilization, if available.
- **Should** include descriptions of wireless communication usage:
  - Wi-Fi, Bluetooth, NFC, LoRa—and security options.
- **Should** include a BAS device inventory.
  - BACnet PICS (profiles), or similar submittal for other protocols.
  - Spreadsheet listing device identity and network attributes.
    - MAC, IP address, BACnet network number, device instance, device name.
    - For example, BIG-EU's B-PAT (project address table) or EDE (engineering data exchange).
- **May** include machine-readable as-configured network usage declarations, such as a MUD document.

Online documentation can be provided for IT/cybersecurity organizations to reference in an ongoing fashion.

NAC-5 Devices **may** provide a MUD URL/repository pointer as part of their boot process (via IEEE 802.1X or DHCP options). Repositories can be global, hosted by the manufacturer, or on site.

4.4 Network Access Control

BACnet/SC (and BACnet/IP and BACnet/IPv6) devices are typically connected to Ethernet networks. In some environments the Ethernet network is implemented via managed switches that are maintained and monitored by an IT group. Managed switches may implement security functionality such as VLANs, destination/port filtering, and device authentication.

NAC-6 Devices **should** implement Ethernet port polarity/speed autodetection.

NAC-7 Devices **may** support IEEE 802.1X device authentication. IEEE 802.1X is a link layer protocol (encapsulating EAP) that allows a switch to challenge a device to provide authentication credentials which may be validated by an authentication server (such as RADIUS).

- This capability is needed for all markets.
- Even in systems which use IEEE 802.1X device authentication, it is common to permit MAC address registration (in the switches or RADIUS server) of OT devices.
- The same underlying protocols are used by WPA2 and WPA3 Enterprise authentication for Wi-Fi access.

NAC-8 Devices **may** support IEEE 802.1X-2004 or -2010.

- Devices supporting IEEE 802.1X **should** support both the username/password (EAP-PEAP) and the certificate-based (EAP-TLS) authentication mechanisms.
  - Devices **should** implement a secure configuration mechanism for IEEE 802.1X authentication parameters (username/password and certificate).
- Devices **should** provide a stable MAC address for registration for Ethernet switch access. The MAC address should be easily readable by field personnel.

4.5 Network Address Assignment and Name Resolution

BACnet/SC (and BACnet/IP, BACnet/IPv6) devices need to configure their IP network settings and IT server addresses before they can fully participate in a BACnet system (e.g., connect to a BACnet broadcast management device [BBMD] as a foreign device or connect to a BACnet/SC Hub). At one time, it was possible to rely on static configuration of these settings, and this is still the norm during construction and for dedicated BAS networks, but it is increasingly common for site IT policy to require dynamic discovery of these settings upon restart. Note that devices may also use TCP/IP or UDP/IP in conjunction with other application protocols.

NAC-9 Devices that support BACnet/IP (defined in Annex J of the BACnet Standard):

- **Shall** support IPv4, as required by the BACnet Standard.
- **Shall** permit IPv4 to be disabled if it is not being used.
- The UDP Port **shall** be configurable in the range 47808–47832 and 49152–65535 (see Clause J.1.2 of the BACnet Standard).
- BBMDs **shall** support DNS, since Broadcast Distribution Tables in Network Port Objects may contain DNS names starting with protocol revision 17 (see the definition of BACnetHostAddress in Clause 21 of the BACnet Standard).

NAC-10 Devices that support BACnet/IPv6 (defined in Annex U of the BACnet Standard):

- **Shall** support IPv6, as required by the BACnet Standard.
- **Shall** permit IPv6 to be disabled if it is not being used.
- BBMDs **shall** support DNS, since Broadcast Distribution Tables may contain DNS names (see the definition of BACnetHostAddress in Clause 21 of the BACnet Standard).
- The UDP Port **shall** be configurable in the range 47808–47832 and 49152–65535 (see Clause U.1.1.2 of the BACnet Standard).

NAC-11 Devices that support BACnet/SC (defined in Annex AB of the BACnet Standard):

- **Should** support both IPv4 and IPv6 and should be configurable to disable either one when not being used.
- **Should** support DNS.
- BACnet/SC hubs as well as nodes accepting direct connections **should** document the TCP ports on which they are listening. The TCP ports used for BACnet/SC **may** be configurable.

NAC-12 IP Address configuration:

- Devices supporting IPv4 **shall** be able to manually configure their IP address, subnet, and default gateway (if applicable).

- Devices supporting IPv4 **shall** support DHCP for dynamic address allocation.
- Devices supporting IPv6 **shall** support SLAAC—but not all sites may use it.

NAC-13 Configuring devices to know the address of the DNS server and other servers:

- Devices supporting IPv4 **shall** support DHCP to obtain DNS server configuration.
- Devices supporting IPv4 **shall** support manual configuration of DNS server.
- Devices supporting IPv6 **shall** support DHCPv6.
- Devices supporting IPv6 **shall** support SLAAC DNS option (2010).
- Devices supporting IPv6 **shall** be configurable to obtain DNS server configuration via DHCPv6 or via SLAAC.

NAC-14 Devices **should** be configurable to disable unused physical network interfaces.

NAC-15 Devices **shall** be configurable to disable/block unused TCP and UDP ports and associated services.

For new construction, the BAS integrator may be expected to provide the initial BAS network infrastructure and, if necessary, a DHCP server, a DNS server, and a certificate authority (CA). Later, the BAS network may be transitioned to IT control, with new DNS names, IP settings, and/or an owner-managed CA, any of which could require partial recommissioning of the BAS devices. In other cases, the IT department may be responsible for the network infrastructure and associated supporting services in support of construction.

A challenge to the design of future BAS products and systems will be the need to adapt to changes in the network infrastructure and the network policies. For example, newly installed systems may need to be partially recommissioned when the management of the BAS network infrastructure is transferred from the BAS integrator to a designated customer organization. Likewise, the integration of a newly commissioned BAS subsystem with an existing system may require changes to the security configuration. Ladder-free recommissioning implies that devices can be reconfigured over the network to meet new requirements resulting from recommissioning for migration of control by qualified personnel using vendor-approved tools. Note that addendum cc of the BACnet Standard defines interoperable methods for BACnet/SC network port configuration.

NAC-16 Devices **should** support scalable, secure, network-based reconfiguration of network settings to support migration of control.

4.6 Time Services

BASs use knowledge of the current time for scheduling the operation of equipment and predicting the occupancy of spaces. Furthermore, systems that use certificates for authentication need the current time to check the period of validity of a certificate. Unauthorized changes to device clocks could result in improper system operation or denial of service (DoS).

ISA 62443-4-2, *Technical Security Requirements for IACS Components*, requirement CR 2.11 on Timestamps, mandates the following:

1. SL-C 1—Create timestamps (date and time) for use in audit records.
2. SL-C 2, 3—Timestamps are synchronized with a system-wide time source.

Time synchronization within a BACnet-based system is typically done using one of BACnet's two standard time synchronization services, TimeSynchronization (Clause 16.7 of the BACnet Standard) and UTCTimeSynchronization (Clause 16.8 of the BACnet Standard). Time-related proper-

ties in the BACnet Device Object (Clause 12.11 of the BACnet Standard) are Local_Time, Local_Date, UTC_Offset, and Daylight_Savings_Status. Currently there is no standard service authorization mechanism in BACnet, so it may not be possible to distinguish between legitimate and illegitimate attempts to modify a BACnet device's clock.

NAC-17 Time service requirements for BACnet devices:

- BACnet devices using BACnet/SC **shall** maintain a clock with the current time and date during operation (see AB.7.4 of the BACnet Standard).
- BACnet devices **may** use IT time protocols (such as SNTP or NTP) upon restart before validating or otherwise using BACnet/SC certificates.
- BACnet devices that require knowledge of the current time for proper operation **should** have real time clocks that maintain time across restarts.
- BACnet devices **should** support time synchronization techniques to reduce clock drift.

Most devices in a BACnet network will be BACnet time recipients, meaning that they will learn the current time from another device in the system using a BACnet service. Such devices will typically support the DM-TS-B BIBB (Clause K.5.12 of the BACnet Standard) or the DM-UTC-B BIBB (Clause K.5.14 of the BACnet Standard).

NAC-18 Additional requirements for BACnet time recipients:

- Devices **should** support DM-UTC-B (UTCTimeSynchronization recipient).
  - Devices supporting DM-UTC-B **shall** support the BACnet Daylight_Savings_Status and UTC_Offset properties.
- Devices **may** support DM-TS-B (TimeSynchronization recipient).
  - If this capability is supported, it **should** be configurable—and disabled by default if DM-UTC-B is supported.

In the future, after an interoperable authorization method has been added to the BACnet Standard, BACnet time recipients should require appropriate authorization credentials before honoring BACnet TimeSynchronization or UTCTimeSynchronization requests, as well as WriteProperty requests that would modify any time-related properties in the Device Object.

One or more devices in a BACnet network will be BACnet time senders, meaning that they will actively provide the current time to the devices in the system using BACnet services. Typically, this function is performed by a single server or supervisory controller. Such devices will typically support the DM-TS-A BIBB (Clause K.5.11 of the BACnet Standard), the DM-UTC-A BIBB (Clause K.5.13 of the BACnet Standard), and either the DM-ATS-A BIBB (Clause K.5.29 of the BACnet Standard) or the DM-MTS-A BIBB (Clause K.5.30 of the BACnet Standard). Additional time-related properties in the BACnet Device Object of BACnet time senders are Time_Synchronization_Recipients, UTC_Time_Synchronization_Recipients, Time_Synchronization_Interval, Align_Intervals, and Interval_Offset.

NAC-19 Additional requirements for BACnet time senders:

- A BACnet time sender **should** support the DM-TS-A and DM-UTC-A BIBBs (UTCTimeSynchronization and TimeSynchronization sender).
  - It **should** be configurable to enable one or both services.
- A BACnet time sender **may** support the DM-ATS-A and DM-MTS-A BIBBs.
- The Time_Synchronization_Interval property **shall** be configurable to be 0 (to disable DM-ATS-A).

- A BACnet time sender **may** use NTP or SNTP or another mechanism to obtain accurate time.

IT systems use timestamps for data logging and for security and audit logging. IT security processes may require tightly synchronized clocks in a system to facilitate analysis of traffic and logs from multiple sources. In IT-managed systems, NTP or a similar protocol is typically used for time synchronization.

NAC-20 IT departments **may** require that some devices use NTP or a related protocol to increase the accuracy of timestamps.

- Site NTP servers **may** use cellular devices or GPS-based devices to obtain accurate time.
- Microsoft Windows-based servers/workstations **may** use Windows Time Service (based on NTP).
- Devices **may** support NTP or SNTP (port 123).
  - Devices which support NTP or SNTP **should** support the DHCP NTP option to obtain server names or addresses.
  - Devices **should** be configurable to disable BACnet DM-UTC-B and DM-TS-B functionality while NTP or SNTP is being used by the device.
  - Devices which support NTP or SNTP **should** be configurable to disable those protocols and to use BACnet's UTCTimeSynchronization or TimeSynchronization services.

4.7 References and Related Resources

- ANSI/ASHRAE Standard 135-2020, particularly the following sections:
  - Annex A: Protocol Implementation Conformance Statement
  - Annex AB: BACnet Secure Connect (BACnet/SC)
  - Addendum cc regarding functionality to support the management of BACnet/SC network ports
  - Addendum cd regarding TLS V1.3 Cipher Suite Application Profile for BACnet/SC
  - Addendum cp regarding Authentication and Authorization
- Google Application Security Requirements for IoT Devices
- IEC 62439-2, *Media Redundancy Protocol (MRP)* (IEC 2021)
- IEEE 802.1Q, *Bridges and Bridged Networks* (IEEE 2018b)
- IEEE 802.1X, *Port-Based Network Access Control* (IEEE 2004, IEEE 2010, IEEE 2020)
- IEEE 802.1AR, *Secure Device Identity* (2018b)
- IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)* (Rigney et al. 2000)
- IETF RFC 3410, *Introduction and Applicability Statements for Internet-Standard Management Framework* (Case et al. 2002)
- IETF RFC 5247, *Extensible Authentication Protocol (EAP) Key Management Framework* (Aboba et al. 2008)
- IETF RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification* (Mills et al. 2010)
- IETF RFC 6272, *Internet Protocols for the Smart Grid* (Baker and Meyer 2011)
- IETF RFC 8520, *Manufacturer Usage Description (MUD)* (Lear et al. 2019)
- IETF RFC 8633, *Network Time Protocol Best Current Practices* (Reilly et al. 2019)
- ISA/IEC 62443-3-3, *System Security Requirements and Security Levels* (ISA/IEC 2013)

    - SR 2.11, *Timestamps*
- NIST FIPS 140-2 and 140-3 Security Requirements for Cryptographic Modules (NIST 2001, NIST 2019)
- NIST SP 800-97 *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* (Frankel et al. 2007)
- NIST SP 500-267B, *USGv6 Profile* (Montgomery et al. 2020)
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
    - ID.AM-1: Physical devices and systems within the organization are inventoried
    - ID.AM-2: Software platforms and applications within the organization are inventoried
    - PR.AC-1: Identities and credentials are managed
    - PR.AC-3: Remote access is managed

5

BACnet/SC Device Onboarding

Device Onboarding is the initial network and security configuration of a device to allow it to participate in a BAS network. Some network and security configuration may need to come from IT systems, and IT may be involved in issuing credentials. Additional application configuration of the device may then occur over the network. Onboarding has traditionally been performed by vendor-specific configuration tools, but onboarding of BACnet/SC devices in multivendor systems requires the exchange of interoperable credentials.

Aspects of the onboarding process include the following:

Factory Credentials—Secure devices come configured with factory credentials to identify themselves and to provide a factory root of trust. Famous exploits have created botnets of IoT devices with default passwords. Jurisdictions (including the state of California) have introduced regulations banning the sale of products with weak credentials. There are restrictions on the strength and uniqueness of device factory credentials.

Scalable Onboarding—Devices need to be provided with a great deal of information to join an /SC network. The certificate authority (CA) for the /SC network needs information about the devices (including their public key, in the form of a certificate signing request [CSR]) to prepare the signed operational certificate that the device uses to join the /SC network. Vendors need a scalable workflow to onboard groups of devices, which are identified by their factory device credentials.

Trust—A common model for configuring OT and consumer IoT devices is Trust on First Use (TOFU), where the device is trusted by the user when it is removed from its packaging. The device's configuration interface trusts the user or local configuration tools implicitly until they set up local credentials. In high-security applications, there may be a need to establish bidirectional trust between device and configuration tool before onboarding proceeds. The device proves its identity and the configuration tool proves it has authorization from the manufacturer, using factory device credentials. When a device is onboarded, it will be configured with site-specific credentials.

BACnet/SC specifies the site-specific credentials and configuration settings that are needed for a device to access the network. In the future, BACnet® device Authentication and Authorization mechanisms will specify additional security credentials.

5.1 MOTIVATION

Multivendor Projects—Network and security configuration (including BACnet/SC certificates) are typically managed by one BAS vendor and need to be shared with vendors responsible for installing subsystems.

Device Preconfiguration—Some equipment may be able to be preconfigured before actual installation on-site. The supplier needs to be able to obtain the network and security configuration in an off-line manner.

Recovery from Device Reset—If devices are reset due to disconnection from the network or a security incident, the vendor will need to repeat the onboarding process.

Network Reconfiguration—During large-scale changes to network configuration, such as the introduction of network segmentation to implement security zones or as systems migrate from BACnet/IP to BACnet/SC, vendors may wish to perform bulk reconfiguration of devices using the onboarding process.

Support Other BACnet Parameters—During system commissioning, it may be useful to share other BACnet parameters (beyond BACnet/SC network and security configuration) between vendors. Such parameters may include device instance, device name, location, MS/TP or IP parameters, and BACnet network numbers. Current practice includes exchanging spreadsheets with this information (such as the EDE and B-PAT formats that are used in Europe), so onboarding tools may support the import/export of CSV files.

5.2 SECURITY CONSIDERATIONS

BAS onboarding mechanisms cannot assume the availability of Internet access from a device to vendor cloud services (unlike consumer-oriented IoT devices).

Onboarding mechanisms that do not require authorization (such as a TOFU configuration interface) could permit a device to be captured by something other than the intended system.

Onboarding mechanisms that do not require device authentication could be susceptible to device spoofing or establishing a man-in-the-middle channel.

Onboarding mechanisms without device authentication may allow unauthorized (or unexpected) devices onto the system.

Onboarding mechanisms without communication security may result in the exposure of credentials during the onboarding process.

Reuse of the onboarding process after device reset could be used as an exploit.

Mitigations for security concerns for onboarding mechanisms include the following:

- Provide physical security during onboarding for devices that use a TOFU configuration model.
- Vendor-specific onboarding tools must use secure communication and secure credential storage.
- Require user authorization for onboarding (except at the initial stages for the TOFU configuration model).
- Do not use global factory credentials (i.e., no default passwords).
- Use the CSR/certificate workflow between vendor tools and CA so private keys are not exposed.

- Onboarding mechanisms should be supervised by authorized users and time limited (during system commissioning and maintenance).
- Verify signing requests and other relevant initial trust establishment steps by out-of-band mechanisms before acknowledging them.

5.3 BACnet/SC Onboarding Guidelines

Vendor-specific tools are expected to provide a secure proprietary mechanism for onboarding devices. Devices can support BACnet/SC at a lower BACnet protocol revision than would require the Network Port Object extensions for BACnet/SC defined in addendum cc of the BACnet Standard (protocol revision 24) or even the mandatory support of the NPO object itself (protocol revision 17). Support for the Network Port Object permits online interoperable configuration after onboarding (see Chapter 6**)**. However, even for devices which do not support addendum cc, but support at least revision 17 already, vendor tools should provide configurability consistent with addendum cc during the onboarding process.

DO-1 During onboarding, devices **should** be able to configure IT settings such as DHCP vs. static configuration, DNS server, IPv4 and IPv6 addresses, and network access credentials.

DO-2 During onboarding, devices **should** be able to configure configurable and writable Network Port Object properties such as BACnet network numbers (for BACnet routers).

DO-3 During onboarding, devices supporting BACnet/SC **should** be able to configure internal parameters corresponding to the Network Port Object configurable properties for BACnet/SC as specified in addendum cc of the BACnet Standard (see Chapter 3 of this docment), including the following:

- SC_Primary_Hub_URI, SC_Failover_Hub_URI
- SC_Hub_Function_Enable (if applicable)
- SC_Direct_Connect_Initiate_Enable, SC_Direct_Connect_Accept_Enable, and SC_Direct_Connect_URIs (if applicable)

DO-4 During onboarding, configuration tools supporting BACnet/SC devices **should** be able to generate a CSR and load operational certificates and signing certificates using standard file formats as specified in Annex AB and addendum cc of the BACnet Standard (see Chapter 6 of this document). Those credential files will need to be securely exchanged with a site-specific certificate signing authority. Configuration tools should support the required validation logic for certificates defined in addendum cc. File format requirements include the following:

- **Clause AB.7.4.1.2** The signing CAs **shall** support processing of certificate signing requests in Privacy Enhanced Mail (PEM) format (per RFC 7468) conveying a certificate signing request and return the signed certificates in PEM formatted PKCS7 structure.
- **Clause AB 7.4.1.3** The configuration tool **shall** support the exchange of certificate signing requests and signed certificates in PEM format per RFC 7468.
- **Addendum CC 12.56.Y24 Operational_Certificate_Files** The operational certificate file **shall** be an X.509 certificate in PEM format. For details on a BACnet/SC network see Clause AB.7.4.1.

- **Addendum CC 12.56.Y25 Issuer_Certificate_Files** Each issuer certificate file **shall** contain an X.509 certificate in PEM format. For details on a BACnet/SC network see Clause AB.7.4.1.1.
- **Addendum CC 12.56.Y26 Certificate_Signing_Request_File** This read-only property, of type BACnetObjectIdentifier, specifies the File object that contains the PKCS #10 certificate signing request as defined by RFC 5967 in PEM format that can be used by the signing CA to create an operational certificate, matching the internal private key for the port. For details on a BACnet/SC network see Clause AB.7.4.1.2.

DO-5 During onboarding, certificate signing tools representing the site-specific CA **shall** be able to receive CSRs and generate operational certificates as required by Clause AB.7.4.1. Certificate signing tools **shall** also be able to export their issuer certificate.

5.4 Interoperable Onboarding Guidelines

There is a need for a data interchange standard between vendors for off-line onboarding workflows. Floppy net configuration is the lowest common denominator for situations such as configuration of devices before arrival on site, configuration of multivendor systems before networks are fully connected, and recovering from broken network configurations.

Addendum cs of the BACnet Standard specifies an interoperable file format that allows CSR files from several BACnet devices to be packaged into a single file. This file is processed by a CA and, if successful, the CA inserts each device's Issuer and Operational certificate files into the received file. The method of transmission of the files is not defined.

Future:

A potential future addendum would define an onboarding procedure using interoperable online TOFU techniques for environments where the commissioning network is physically protected. One idea under consideration is bootstrapping from BACnet/IP to configure a device via Network Port objects and File objects, followed by a device restart to join a BACnet/SC network. Another idea is for a BACnet/SC device to accept direct connections with relaxed certificate validation.

Additional work may be done to evaluate standards for online interoperable secure onboarding of BACnet devices such as Bootstrapping Remote Secure Key Infrastructure (BRSKI) or Secure Zero Trust Provisioning (SZTP).

5.5 References and Related Resources

- ANSI/ASHRAE Standard 135-2020, Annex AB (BACnet/SC)
  - Addendum cc regarding Network Port Object extensions for BACnet/SC
  - Addendum cd regarding minimum required ciphers for BACnet/SC
  - Addendum cs regarding off-line certificate exchange file format for BACnet/SC
- IETF, RFC 8572, *Secure Zero Trust Provisioning (SZTP)* (Watsen et al. 2019)
- IETF, RFC 8995, *Bootstrapping Remote Secure Key Infrastructure (BRSKI)* (Pritikin et al. 2021)
- UK Code of Practice for Consumer IoT Security—"No default passwords" (DDCMS 2018)

6

BACnet/SC Certificate Management

Certificate management is the process of generating and distributing certificates associated with device private keys. BACnet/SC requires certificate management of all devices to establish a secure network. Many devices may also require a public key infrastructure (PKI) certificate for other protocols (e.g., HTTPS, Modbus TCP Security, and EAP-TLS).

6.1 Motivation

BACnet/SC requires a signing certificate (root of trust) and a device certificate for the TLS private key to be used for BACnet/SC. The certificate's Subject and Subject Alternative Name (SAN) fields are not used by BACnet/SC. The BACnet/SC certificate attests to a device's permission to join the network based on its private key, not its device identity (see addendum cp, Clause 17.3, and recommendation **CM-2** later in this chapter).

Other protocols may require certificates (e.g., IEEE 802.1X, HTTPS for a user interface, SNMP over TLS). Typically, a certificate will attest to the device's identity and be part of a signing chain to a site-managed IT root certificate or a global PKI root certificate. Some devices may use the same key and certificate for BACnet/SC and all other TLS-based protocols.

Other protocols may require the Subject or SAN fields of a certificate to attest to the network identity of the device—its IP address or DNS name. There could be distinct certificates (and corresponding private keys) or common certificates used by each TLS-based protocol. This means that certificate issuing must be coordinated with network management for the assigned addresses and names.

Addendum cc of the BACnet Standard specifies interoperable mechanisms for updating a device's BACnet/SC certificates using the following workflow, from the device's perspective:

1. Retrieve a CSR from the device.
2. Send updated operational and signing certificates to the device.
3. Request the device to validate the new configuration.
4. Restart the device to enable the new configuration.

Onboarding—Every BACnet/SC device needs to be issued certificates (appropriate to their network segment) to be able to connect to the BACnet/SC network. Devices may also require certificates for other protocols, such as HTTPS. Offline data interchange (files) may be used between a certificate authority and vendor installation tools.

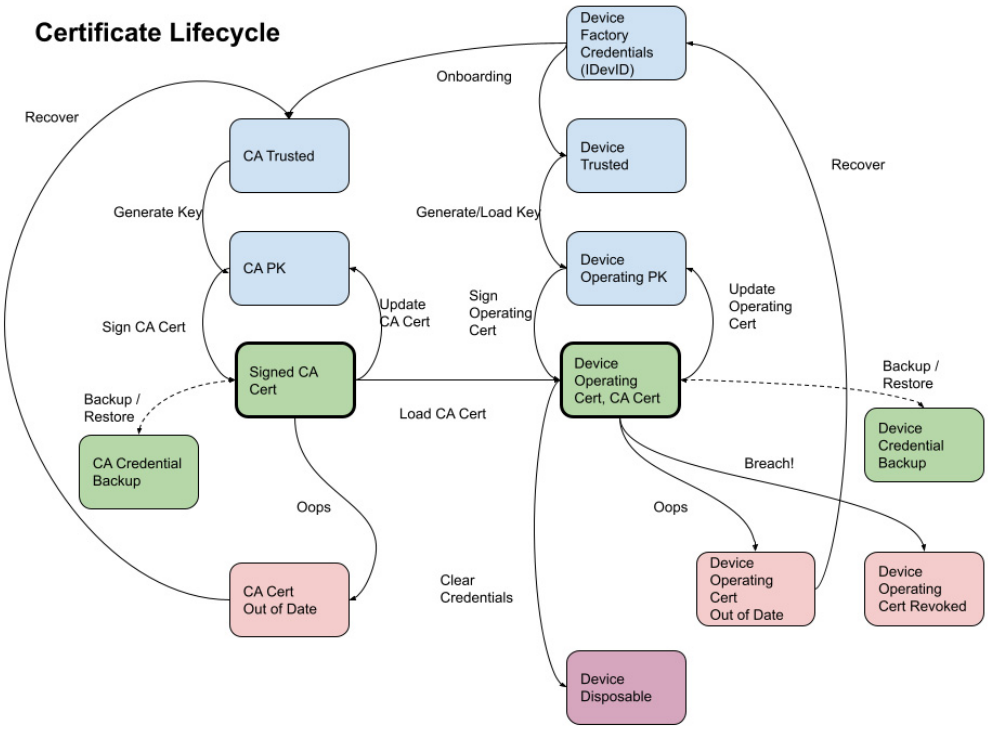

Figure 6.1 The life cycle of a digital certificate.

Network Segmentation—A BACnet/SC system may be divided into network segments for performance or security reasons. When it is necessary to prevent devices from connecting to the wrong network segment, distinct signing keys (and hence signing certificates) should be used for each network segment.

Scheduled Updates—Certificates have limited lifespans, which may be mandated by site IT policy. The BACnet/SC operational certificates should be updated before they expire.

Compromised Keys—PKI certificates have a revocation mechanism for invalidating certificates if the associated private key has been compromised. BACnet/SC does not define an interoperable revocation mechanism (but leaves that as a local matter), so if a compromised device needs to be disconnected from the BACnet/SC network, a new issuer certificate should be created and distributed to the uncompromised devices as well as new operational certificates. See addendum cc of the BACnet Standard for details on how to accomplish this.

Change of Administration—During the life of a building, the organization responsible for network management and certificate management may change. Such transitions may occur during commissioning of a new system, during a transition from a BAS-managed to IT-managed network, or during a change in operating management. The new administration will most likely want to assign a new certificate authority and reissue all certificates to devices. This authority should remain under control of the building owner and is consistent with the principles of right-to-sign and right-to-migrate.

6.2 Security Considerations

Certificates are designed to be public information, so privacy during certificate management is not as important as authorization and trust of the certificate issuer.

Addendum cc of the BACnet Standard does not specify an authentication or authorization mechanism, so unauthorized access to the BACnet/SC credentials could result in a denial of service by disconnecting devices from the network.

Sites may require the use of certain cryptographic algorithms (within the set supported by TLS 1.3), so tools and devices must be able to use the required algorithm. A certificate signature type may be different than the signature type that a device uses for its CSR.

Devices sharing a private key increase the risk of compromise. A vendor should not reuse private keys/certificates for multiple devices. BACnet® authorization features, such as those defined in addendum cp of the BACnet Standard, are likely to rely on unique private keys and operational certificates for each device as an authentication mechanism.

BACnet/SC operating and signing certificates should have limited lifetimes. Ideally a device generates a new operating private key when certificates need updating. A new signing certificate must be generated when issuing new operational certificates, to invalidate stale operational certificates. If certificates are not replaced before they expire, devices will not be able to connect to the BACnet/SC network, necessitating a recovery procedure that may require the use of vendor-proprietary tools and procedures.

Removing a BACnet/SC device from a network requires updating the operating and signing certificates for the rest of the network. A change in site policy about cipher suites may require updating the operating and signing keys and the certificates of the network.

Malformed or misconfigured certificates could lead to accidental denial of service (DoS) for one or more protocols.

Setting a device's clock to a time outside the lifetime of its operating or signing certificate (or outside the lifetime of the hub's operational certificate) could prevent the device from connecting to the BACnet/SC network. Unauthorized and/or incorrect use of the BACnet Time Synchronization services could lead to such a situation.

Mitigations

- Use secure offline mechanisms for exchanging data during certificate management.
- Support all cipher suites required by TLS 1.3.
- Configuration tools or devices should validate certificates before using them.
- Block addendum cc of the BACnet Staandard and Time Synchronization operations at the boundaries of a BAC net/SC network (using a BACnet-aware firewall/router).
- Monitor BACnet/SC device certificates to warn of impending expiry. Devices and management tools should notify users.
- Monitor BACnet/SC device certificates (required to be readable by addendum cc) for unexpected changes.
- Monitor BACnet/SC devices to detect unexpected disconnections from the network.

6.3 DEVICE GUIDELINES

Certificates are the basis for authentication and authorization for many protocols in building networks. BASs should support the current best practices, including the following:

NIST Cybersecurity Framework (version 1.1) recommended activities:

- PR.AC-4 Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
- PR.AC-7 Users, devices, and assets are authenticated commensurate with the risk of the transaction
- PR.AC-1 Identities and credentials are used for authorized devices, users and processes
- PR.AC-4 Access permissions and authorizations
- PR.AC-5 Network integrity is protected
- PR.AC-6 Identities are use during interactions
- PR.AC-7 Users, devices, and assets authenticated commensurate with the risk of the transaction
- PR.DS-2 Date in-transit is protected

ISA 62443-3-3 System Security requirements and Security Levels requirements:

- SR 1.2, *Software Process and Device Identification and Authentication*
- SR 1.8, *Public Key Infrastructure (PKI) Certificates*
- SR 1.9, *Strength of Public Key Authentication*
- SR 7.6, *Network and Security Configuration Settings*

ISA 62443-4-2 Device requirements:

- NDR/EDR 3.13, *Provisioning Asset Owner Roots of Trust*

Additional requirements for BACnet devices that support BACnet/SC are as follows:

CM-1 Devices **shall** support the cipher suites listed in addendum cd of the BACnet Standard, at a minimum:

BACnet/SC implementations shall support TLS version 1.3 as specified in RFC 8446. BACnet/SC implementations shall support the following TLS V1.3 cipher suite application profile. For the definition of the terms in quotes see RFC 8446:

a. TLS cipher suite TLS_AES_128_GCM_SHA256,
b. digital signature with ecdsa_secp256r1_sha256, and
c. key exchange with secp256r1.

CM-2 Devices/configuration tools **shall** support the file formats for CSR (IETF RFC 7468 PEM) and Certificates (PEM format PKS7) as specified in Clause Annex AB 7.4 of the BACnet Standard. A CSR for a device's BACnet/SC operational certificate **should** contain the device's BACnet device instance number in a SAN entry as per the BACnet URI scheme defined in Clause Q.8 of the BACnet Standard. Other device identity information (vendor, model, serial number, UUID) may also be included.

CM-3 Devices/configuration tools **should** validate new operating and signing certificates before using them.

CM-4 Devices **should** locally log connection failures associated with validation failures of peer certificates.

CM-5 Devices **shall** support a reset to factory defaults as defined by Annex AB of the BACnet Standard, Clause 7.4.2. Factory reset may be required for safe disposal of devices. See ISA/IEC 62443 4-1 of SG-4, Secure disposal guidelines.

CM-6 Devices **may** support online certificate updates via the mechanisms described in *Addendum CC*. Devices **shall** support a secure offline (or non-BACnet) mechanism for onboarding and updating BACnet/SC certificates. Devices and management tools **may** use standard protocols to interact directly with an IT-maintained CA (such as IETF RFC 7030, Enrollment Over Secure Transport).

CM-7 Devices and management tools **may** use standard protocols for detecting certificate revocation, such as Online Certificate Status Protocol (X.509 OCSP) or Certificate Revocation List (IETF RFC 5280).

CM-8 Devices **may** notify users and management tools of imminent certificate expiration.

6.4 Certificate Signing Guidelines

CM-9 CA-issued BACnet/SC operational certificates **should** make the minimum necessary claims (i.e., no wildcards in SAN, limited key usage claims). BACnet/SC does not currently use the Subject or SAN certificate fields for validating the identity or network address/name of a device, but these fields are important for device approval and should be carried over from the CSR if possible. These fields **may** need to be set for devices using a single TLS operational certificate for multiple protocols, particularly HTTPS Web UI.

CM-10 Certificate signing tools **shall** support the file formats for CSR (PEM format PKCS10) and Certificates (PEM format PKCS7) as specified in Annex AB 7.4 of the BACnet Standard.

CM-11 Operational certificate lifetime **should** be within the signing certificate's lifetime.

BACnet/SC makes no assumptions about the trust model above the CA certificate. All devices are configured with the CA certificate, and that is their root of trust for BACnet/SC operational certificates.

However, the trust model matters for audit, organization policy, revocation, and uses of an operational certificate other than BACnet/SC.

CM-12 Certificate signing tools **shall** support trust models:

- Self-Signed Root: Local and informal with one or two levels above CA
- Self-Signed Root: Local Customer IT CA or IT delegated CA
- PKI: Customer IT CA linked to the public root of trust

6.5 References and Related Resources

- ASHRAE Standard 135-2020
  - Addendum cc
  - Addendum cd
- ISA/IEC 62442-3-3 System Security Requirements and Security Levels (ISA/IEC 2013)
  - SR 1.2, *Software Process and Device Identification and Authentication*

  - SR 1.8, *Public Key Infrastructure (PKI) Certificates*
  - SR 4.3, *Use of Cryptography*
  - NDR/EDR 3.13, *Provisioning Asset Owner Roots of Trust*
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
  - Top-down framework defining scope and best practices for cybersecurity standards and end-user policies and processes. Provides cross-references to many existing cybersecurity standards, including the ISA/IEC 62443 family.
  - PR.AC-1 Identities and credentials are used for authorized devices, users and processes.
  - PR.AC-7 Users, devices and assets authenticated commensurate with the risk of the transaction.
- NIST 800-82r2 Guide to Industrial Control Systems (ICS) Security (Stouffer et al. 2015)
- NIST 800-53r5 Security and Privacy Controls for Information Systems and Organizations (NIST 2020)
- IETF RFC 2315, PKCS 7 (Kaliski 1998)
- IETF RFC 2986, PKCS 10 (Nystrom and Kaliski 2000)
- IETF RFC 5208, PKCS 8 (Kaliski 2008)
- IETF RFC 5280, X.509 Certificates (Cooper et al. 2008)
- IETF RFC 7468, Textual encoding format for PKCS 7, 8, and 10 (Josefsson and Leonard 2015)
- IETF RFC 8446, TLS V1.3 (Rescorla 2018)

7

Device Reset

Devices may need the capability to reset parts of their configuration to comply with security and privacy policies and to allow for recovery from problems. This capability may be referred to as *factory reset* or *reset to factory mode*. Since the details of the mechanism and extent of such resets are proprietary, these guidelines define specific capabilities which may be part of the reset features of a device.

Database reset*:* the erasure of user information and site-specific applications and application configuration.

Network/security reset*:* the erasure of site credentials (keys, passwords, certificates), site root of trust (certificates). Network/security reset places the device in a mode that requires a repeat of its onboarding process, and maintains factory credentials and root of trust.

Firmware reset: reverts a device to using a previously installed stable version or factory-supplied version of firmware. Devices that support online firmware updates may alternate between multiple firmware volumes for each update, allowing for use of the previously installed version. Older designs may include read-only factory firmware that can be restored to an active volume. Devices that do not support stand-alone firmware reset may include a trusted loader for updating firmware, even in scenarios where the current firmware is corrupted. Larger devices may use standard operating system mechanisms for firmware (as opposed to application software) management.

Safe mode: the ability to restart a device with limited firmware functionality for diagnostics. Safe mode may include a trusted loader for updating firmware.

7.1 Motivation

Recovery from Configuration Error/Expiration/Loss of Credentials—Modern network protocols (including IEEE 802.1X, BACnet/SC) may require devices to have current credentials to access the network, and devices may need to have current server (and site root-of-trust) certificates to trust access to the system. Many of those credentials are typically provisioned during a secure onboarding process for the device. Changes to the network configuration of a device or to its network environment can break its ability to access the network. A device may be able to be recovered via a local configuration interface, or it may need a local reset mechanism that permits it to be recovered by repeating the secure onboarding process.

Downgrade/Recovery from Corrupt Software/Firmware Installation—Failures in the firmware update process or hardware failures might impair a device's operation. A reset mechanism

might be able to restore firmware to a working state. A safe mode might enable restoring a device's firmware to a working state.

Recovery from Cybersecurity Exploit/Infection—When a device is compromised (or merely suspected to be compromised) by malware, part of the recovery process may include resetting the device to a clean state. A local reset mechanism may be required if the device is quarantined from the network or if the malware prevents network-based configuration. Secure onboarding with new credentials may be required. Care must be taken when recovering a device's onfiguration from backup, since it may be compromised. Site policy may require compromised devices to be replaced rather than reset.

Removal of Data for Disposal/Sale of Device—Security policies and regulations may require that all site-specific information be securely erased from a device before it is removed from a system for disposal.

7.2 Security Considerations

Reset mechanisms cannot be a channel for a denial-of-service attack.

Recovery scenarios may not permit network access to a device and may require a local reset mechanism. A local reset mechanism might be physical (a button), a local UI, a local configuration port (serial, network), or via a short-distance wireless protocol.

Devices in BASs may be difficult to access physically (in the ceilings, or on a roof or in remote equipment rooms), so network mechanisms are preferred for configuration and management, which may include network reset mechanisms. Network reset mechanisms should require authorization.

Forensic analysis of a device's state may be required before invoking a reset mechanism.

Mitigations for security concerns for reset mechanisms include the following:

- Provide physical security for devices to limit access to local reset mechanisms.
- Require authorization for reset mechanisms.
- Monitor the network for loss of communication to devices.
- Monitor device database and firmware state to detect unexpected changes.

7.3 Device Guidelines

Manufacturers may choose to implement firmware reset or safe mode in their devices. Various reset capabilities may be combined into a single mechanism.

> **DR-1** A device **should** require authorization for a local reset mechanism (if possible). A device **shall** require authorization for a network-based reset mechanism.
>
> **DR-2** A device **should** provide the user with feedback about the success/failure of an attempted reset.

Network/security reset provides a recovery mechanism for common network problems, BACnet/SC configuration problems, and certificate expiry problems. Network/security reset is required for BACnet/SC credentials by Clause AB.7.4.2.1 or the BACnet Standard for device disposal.

> **DR-3** A device **shall** provide a capability to perform a local network/security reset.

DR-4 A successful network/security reset **shall** place a device in a mode that permits repeating its onboarding process (see for example Chapter 5).

Database reset may be required by regulations or site security policy for device disposal. Database reset may also be useful in recovery scenarios (where applications or application configuration is suspected to be corrupted).

DR-5 A device **should** provide the capability to perform a database reset.

DR-6 A database reset mechanism **may** be combined with the network/security reset mechanism for the device disposal use case.

7.4 References and Related Resources

- ANSI/ASHRAE Standard 135-2020
  - Clause AB.7.4.2.1, Reset to Factory Defaults
- ISA/IEC 62443 *Security for Industrial Automation and Control Systems*, a family of standards for OT cybersecurity.
  - ISA/IEC 62443-3-3, *System Security Requirements and Security Levels* (ISA/IEC 2013)
    - Requirements for system design (SR1.2, SR1.5, SR 7.6) which authenticator management and configurability of network/security settings.
  - ISA/IEC 62443-4-2, *Technical Security Requirements for IACS Components* (ISA/IEC 2018b)
    - Requirements for devices (CR 7.4) control system recovery.
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
  - Top-down framework defining scope and best practices for cybersecurity standards and end-user policies and processes. Provides cross-references to many existing cybersecurity standards, including the ISA/IEC 62443 family.
- UK Code of Practice for IoT Devices (2018)—Recommendation #11 (DDCMS 2018)

8

Identity Authentication

Authentication is the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system (NIST 2020). Authorization is a result (TRUE/FALSE) of comparing a user/device/process request to perform an action against the security policy that governs that action. Authorization is used for access control. However, the terms *authentication* and *authorization* are often used interchangeably although they are two distinct functions. Authentication usually comes before authorization, but not always. Some systems allow anonymous access, and then IT assigns rights to the anonymous users; FTP sites and public websites are notable examples of this. Authorization is addressed in Chapter 9.

In general, authentication requires a claim of identity (usually a username, but not always) and then proof that you possess some unique information that confirms that claim of identity. Proof is something you have, something you know, or something you are (i.e., three factors). Something you have could be a key, rotating code application, key card, certificate, etc. Something you know is usually a password or passphrase, while something you are is typically a biometric proof. Multifactor authentication just requires multiple distinct types of proof of identity.

BACnet/SC is defined in Annex AB of the BACnet Standard. The BACnet/SC specification defines a set of site-specific credentials and configuration settings that are necessary for a device to access a BACnet/SC network. Mutual device authentication is performed using the built-in client/server authentication mechanisms defined in the TLS 1.3 protocol using public key certificates that identify each device involved in the TLS connection. This means that BACnet/SC does not uniquely identify human users of a system, only the devices which are participating in the communication.

BACnet/SC only uses certificates for authentication. That is, a BACnet/SC device is either allowed to communicate anything to any other /SC device in its /SC network (if it is successfully authenticated) or to not communicate using /SC at all (if authentication failed). In other words, in the current /SC implementation, a successfully authenticated device is also authorized to issue any BACnet® action in the absence of any authorization mechanism. Addendum cp of the BACnet Standard defines additional authentication mechanisms and standard authorization mechanisms to expand the capabilities of BACnet devices to authenticate and authorize individual service requests.

8.1 Motivation

Situations that benefit from authentication include the following:

Multivendor BAS Systems Projects—There may be per-system authentication for the many types of users. Support for standard IT authentication servers reduces the management complexity in large projects.

Site Audit Policy—Sites may require audit trails/logs which indicate who did what, when, and why. Also, date and time stamps will be included with each BAS audit or system activity log entry. However, mission-critical applications (e.g., pharmaceuticals or life-sciences jobs) may also require the "why" for regulatory compliance in the BAS logs.

Device-Level Protection—If the BAS controllers' features are misconfigured then users can do things that they are not supposed to do. Local maintenance and "recovery" accounts should require user authentication.

Network Access—In many sites, devices must be authenticated to be granted network access (IEEE 802.1X, HTTPS certificates, BACnet/SC certificates).

Centralized Management and Scalable Authentication Management—Have role-based centralization system for managing BAS user accounts and allow for immediate changes for the user's account to be locked or removed if the user is leaving the company, on an extended vacation, or being promoted and no longer accessing the BAS.

Authorization—User and device authentication is a prerequisite for assigning authorization rights.

IEC 62443-3-3 Compliance—The following requirements govern user and device authentication in OT systems:

- SR 1.1, *Human User Identification and Authentication*
- SR 1.2, *Software Process and Device Identification and Authentication*
- SR 1.3, *Account Management*
- SR 1.4, *Identifier Management*
- SR 1.7, *Strength of Password-Based Authentication*
- SR 1.9, *Strength of Public Key Authentication*
- SR 1.10, *Authenticator Feedback*
- SR 1.11, *Unsuccessful Login Attempts*
- SR 2.1, *Authorization Enforcement*
- SR 2.8, *Auditable Events*

Authentication is a prerequisite for authorization of users, devices, and processes: without strong authentication, authorization techniques may be limited to possession of secret credentials which can be shared or copied. For example, an admin account with a well-known password could easily be used by unauthorized users.

8.2 Security Considerations

Authentication mechanisms for users could be bypassed by credential sharing. BAS users (e.g., operators) have been known to hide credentials on a sticky note under the keyboard (or more spectacularly, spray painting the password on a block wall at the site).

Authentication mechanisms could be compromised if users can use weak or repeated passwords. This is a particular threat for interfaces with remote access.

Authentication mechanisms could be compromised if credentials are exposed at rest and in transit. Exposure could be due to weak (or nonexistent) encryption or to poor access controls for storage

and backups. One serious threat is the escalation of a credential compromise from access to a BAS device to IT assets.

Authentication mechanisms could be bypassed if an unauthorized party could reuse an authenticated session. Parties with network access may attempt session hijacking to gain access to BAS or IT resources.

8.3 BAS User Guidelines

BAS owner/operators must put in place policies and procedures to protect user credentials. BASs should include features that support those procedures (e.g., supporting MFA to prevent account reuse). Although these procedures cannot be enforced by manufacturers, they may be included in documentation provided to the customer's operations staff.

- BAS users (e.g., operators) should be forbidden from leaving printed credentials on or near workstations.
- BAS user account management policies for user authentication must use strong or complex credentials to defend against brute force attacks.
- BAS user accounts shall not be shared among other facilities employees or the HVAC&R service employees.

8.4 BAS System User Authentication Guidelines

Vendors are expected to provide a secure proprietary mechanism for authenticating users and devices.

> **IA-1** During configuration of the BAS, the system integrator **should** create named user accounts (rather than having a default user account) on the BACnet device, and select the appropriate authentication factors with the supplemental authentication item if applicable.
>
> **IA-2** During configuration of the BAS, there **may** be other authentication related items that one may need to configure, such as session timeouts, password length, password aging, number of unsuccessful login attempts, password history, time-of-day constraints, etc. Note: these items **should** be logged in the BAS system or audit logs with who, what, and when information.
>
> **IA-3** During configuration, each user **should** have a unique user account name. The initial password **should** be assigned by the BAS facility manager or the BAS administrator if the passwords are locally managed.
>
> **IA-4** During the life of the BAS, it **should** be possible to purge or wipe all customer-specific sensitive information, including user account information, emails, phone numbers, etc. (see Chapter 7).

If a centralized authentication management system is used with the BAS, then consider the system that does not require use of a list of users on the BAS. For example, the BAS would use role-based authorization and use the user identity for UI and audit purposes.

> **IA-5** The BAS **may** support the use of the customer's central authentication management system.
>
> **IA-6** Small embedded devices **may** only support local user accounts. They **should** follow IoT regulations around credential management and be equipped with reasonable security,

such as California Senate Bill 327, passed in 2020, and UK Code of Practice for Consumer IoT Security (2018).

IA-7 BAS vendor **should** have authentication functionality comply with the many Access Control controls from NIST SP 800-53 rev5.

IA-8 The BAS vendor developing BAS applications on smartphones **shall** follow best practices below.:

- Password-protect your technology.
- Note that user credentials could be cached on the device. Such credentials should be stored securely.

IA-9 The BAS authentication system **shall** store user or device credentials in a secured/ protected location and manner.

IA-10 The BAS **shall** protect against authentication exploits and vulnerabilities.

BAS authentication over insecure communications is when a client or server communicates over a non-secure (unencrypted) channel, leaving it possible for an attacker to intercept, change, or recover sensitive communications and information (i.e., passwords, session IDs, and other credentials).

IA-11 The BAS **should** support authentication over a secure communication channel.

IA-12 BAS user authentication **shall** protect and not expose session IDs or identity tokens.

IA-13 BAS Central User Account Management Systems **shall** be compliant with regional data privacy requirements (GDPR, California privacy laws, etc.).

Future:

The recently approved addendum cp of the BACnet Standard adds per-request device authentication and authorization. The credentials are carried in data options within BACnet/SC network segments of a BACnet system. The trusted network infrastructure (BACnet/SC hubs and routers) attest to the source of requests from devices that used strong authentication during their initial connection to the network. BACnet/SC devices designed to comply with BACnet protocol revision 29 or later may implement addendum cp.

8.5 References and Related Resources

- ANSI/ASHRAE Standard 135-2020
  - References to authentication at the device level in specification
- ISA/IEC 62442, Series of Standards, Industrial communication networks—Network and system security
  - 62442-3-3, *System Security Requirements and Security Levels* (ISA/IEC 2013)
    - SR 1.1, *Human User Identification and Authentication*
    - SR 1.2, *Software Process and Device Identification and Authentication*
  - 62442-4-2, *Technical Security Requirements for IACS Components* (ISA/IEC 2018b)
    - SR 1.1,

        - SR 1.2,
- IETF RFC 6749, *The OAuth 2.0 Authorization Framework* (Hardt 2012)
    - Core OAuth 2.0 framework; describes the roles (resource owner, client, authorization server, etc.)
- Security and Privacy Controls for Information Systems and Organizations
- IETF RFC 9200, *Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth)* (Seitz et al. 2022)
- NIST SP 800-53 rev5, *Security and Privacy Controls for Information Systems and Organizations* (NIST 2020)
    - See Identification and Authentication (IA), family of IA Controls.
- NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management* (Grassi et al. 2017)
- NIST SP 800-82 rev3, *Guide to Operational Technology (OT) Security* (Stouffer et al. 2023)
- NIST SP 800-162, *Guide to Attribute Based Access Control (ABCS) Definition and Considerations* (Hu et al. 2014)

9

Authorization

Authorization is a system feature for granting users, processes, and devices access to system data and operations.

BAS systems may contain data which is subject to privacy or security policies and hence may only be accessed by authenticated and authorized users. User privileges may vary depending on the situation (i.e., system in normal operation or in scheduled maintenance) or time of day. Distributed control applications may require granting privileges to devices to access and control other devices.

BAS systems may support a range of operations of various sensitivity and risk, such as changing set points, overriding control sequences, acknowledging alarms, enforcing physical access control, updating system configuration, performing maintenance, auditing events, and performing network and security management. Authorization for some operations may be limited to users with appropriate training and responsibility. Automated operations may need to be restricted to only be performed by authorized devices.

User authentication and authorization is typically managed by the primary front end (workstation or server) in a BAS. Device authentication and authorization may be managed by the network infrastructure and peer devices, often using authentication and authorization servers.

Devices in BASs require simple and persistent configuration, so role-based authorization can be used so devices do not need to be configured with information about users and detailed authorization policy. A device's policy defines the role required for it to permit an operation. Authorization credentials must be accompanied by proof of authentication (device, user) of the requester to be valid and to support audit logging use cases.

A BAS should incorporate the principle of least privilege: users and devices are granted authorization for only those roles/operations they need to perform. The system may require re-authentication for a user to escalate privileges for sensitive operations.

IT organizations may require that a BAS incorporates the principle of zero trust. End devices are responsible for verifying the authentication and authorization of the sources of all network or local requests.

9.1 Motivation

Multiple Organizations—Personnel from different organizations may have distinct responsibilities for the BAS. Such organizations may include site facilities staff, IT, equipment vendors, and

controls contractors. Users would then have distinct authorization corresponding to the responsibilities (such as network management or equipment maintenance).

Multiple Systems—Multiple systems (HVAC, physical access, lighting, vertical transport) may exist within a BAS network and be interconnected. The systems may have distinct operators and service personnel. Users would then have distinct authorization on different systems (HVAC operators could see occupancy information from a physical access system but could not configure that system).

Security Levels of Device Operations—Operations on a device may require distinct security levels (e.g., controlling normal operation vs. configuration of applications vs. configuration of network and security settings).

Perimeter vs. Zero Trust—Granting access to a workstation/server does not automatically grant access to all applications running on that user interface. Likewise, granting access to a secure BAS network does not automatically grant access to all operations on all devices on that network. This means that authorization enforcement needs to occur within the user interface software and within the devices on a network. Secure BAS networks may be connected to insecure BAS network segments (BACnet/IP, Zigbee, MODBUS) and IT networks that do not enforce device authentication for network access. Network segmentation techniques (see Chapter 14) may enforce coarse authorization policy at the boundary of a secure BAS network, but in general, secure BAS devices cannot assume perimeter protection will prevent them from receiving unauthorized requests.

Unintentional Access—Requiring authorization for sensitive operations prevents unintended access. Without authorization enforcement, protection of the sensitive operations relies on the restraint of users (who may just be poking around the system) or security through obscurity and assumes correct configuration of automation.

Protection of Sensitive Information—Information maintained by systems may be governed by privacy regulations (e.g., HIPAA, GPDR, CCPA) or security policy (credentials). BASs typically do not maintain personally identifying information (physical access control data being one exception). Security configuration and credentials or system operating state (e.g., occupancy) may be considered sensitive information. The system owner may need to be able to prove that the information cannot be disclosed to unauthorized parties.

Configuration Cost/Complexity—BASs typically have lower installation and operating costs than other types of engineered control systems (e.g., industrial controls). A BAS may use role-based authorization to minimize the configuration burden on devices. An authorization mechanism with central management of users, devices, and policies can help minimize maintenance costs.

9.2 Security Considerations

Strong user/device authentication is a prerequisite to authorization, otherwise authorization policy can be bypassed through impersonation. Similarly, user interfaces need strong session control features to prevent unauthorized users from performing operations on the system within the session of an authorized user.

Authorization mechanisms should be designed to prevent the forging of credentials. For example, credentials which are signed by a trusted authority are more difficult to forge than unsigned credentials.

Authorization credentials must not be reused by unauthorized actors (i.e., the authorization mechanism must prevent replay or man-in-the middle attacks). System design may protect against expo-

sure of credentials, but designs may also prevent credential reuse if the credentials are linked to an actor's identity and are required to be accompanied by authentication.

Interoperable device-level authorization may require a trusted network infrastructure (to provide confidentiality and authentication of requests from peers) and trusted workstation/server software (to provide user authentication and authorization policy). This is a consequence of division of responsibility within the system to minimize the configuration complexity of devices.

If authorization mechanisms are too complicated or optional, then the mechanisms are likely to be disabled by users.

Authorization mechanisms may need to minimize network/computational overhead for embedded devices so the mechanisms are not disabled to maintain acceptable system performance.

In building systems, availability is more important than confidentiality and integrity (the CIA triad is inverted compared to IT systems). Designs which require an authorization server to be available all the time may not be sufficiently reliable. BASs are designed to be resilient against a single point of failure (including IT servers which may be required for authentication or authorization).

Building systems may be on isolated networks or may be required to operate solely using local resources—so authorization mechanisms cannot require access to outside servers (via the Internet) for configuration or operation.

If local device interfaces do not enforce authorization, they could be used to bypass network-level policy.

Mitigations for security concerns for authorization mechanisms include the following:

- Limit physical access to the system and network fabric.
- Implement network segmentation with some authorization policy in a BAS network.
- Require authentication of users and devices as a prerequisite for authorization.
- Provide failover servers for centralized authentication and authorization functions.
- Implement off-site backup and disaster recovery processes (for both natural disasters and ransomware) for authentication and authorization servers.
- Audit system configuration and usage for compliance with site authorization policy.
- Monitor the network and device logs for authorization failures.
- Maintain audit logs of changes to authorization configuration.

9.3 Device Guidelines

System authorization capabilities are distributed among features in user interfaces (workstations/servers), authentication/authorization servers, and end devices. Systems should support best practices including the following:

NIST Cybersecurity Framework (version 1.1) recommended activities:

- PR.AC-4, *Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties*
- PR.AC-7, *Users, devices, and other assets are authenticated commensurate with the risk of the transaction*

ISA 62443 3-3 System Security Requirements and Security Levels requirements:

- SR 2.1 SL-C 2, Authorize software processes and devices.
- SR 3.9 SL-C 2, Protect audit information and tools from unauthorized access, modification and deletion.

- SR 4.1 SL-C 1, Protect confidential of information where explicit read authorization is required.
- SR 6.1 SL-C 1, Provide capability for authorized users to read audit logs.

9.3.1 Workstation/Server Capabilities

BAS workstations/servers are often the primary user interface to the system and play a unique role in authenticating and authorizing users.

AZ-1 Workstations/servers **should** use strong authentication for users (see Chapter 8) as the basis for authorization policy.

AZ-2 Workstations/servers **should** implement role-based authorization for users.

AZ-3 Workstations/servers **should** require re-authentication of users for privilege escalation for sensitive operations.

AZ-4 Workstations/servers **should** support device-level authorization when available for remote operations initiated by users and processes, using the principle of least privilege.

9.3.2 Device Capabilities

Physical security, network access control, and workstation/server features can protect network-attached devices from unauthorized access. However, the principle of zero trust requires that devices validate authentication and authorization credentials for sensitive network-initiated operations.

AZ-5 Devices **should** require device authentication and authorization for network requests for sensitive operations.

- Devices **may** directly enforce user authentication and authorization for network requests for sensitive operations. More commonly, devices may trust workstation/servers to authenticate and authorize individual users.
- In general, providing a device with authentication and authorization for BAS network access (i.e., BACnet/SC operational certificate) is not sufficient for authorizing sensitive operations on peer devices.
- BACnet device management operations (Firmware Updates, Backup and Restore, Certificate Management) are sensitive and require authorization.

AZ-6 Devices **should** support consistent authentication and authorization features for all supported network protocols so authorization cannot be bypassed.

AZ-7 Devices **should** require user authentication and authorization for local access to sensitive operations.

- If accounts are maintained locally, devices **should** support different user accounts for different authorization roles in accordance with the principle of least privilege.

AZ-8 Devices **should** require credentials from trusted authentication and authorization servers when possible (rather than use device-managed credentials).

AZ-9 Devices **should** log auditable events associated with authorization mechanisms (configuration of credentials, authorization failure). Access to read and manage audit data should require distinct authorization roles.

AZ-10 Devices **should** log diagnostic events associated with authorization mechanisms, including authorization failure.

9.3.3 Online BACnet Authorization

Before protocol revision 29, BACnet® did not define an interoperable mechanism for authorizing requests. Devices may return an authorization error for a request, but the reasons for doing so are a local matter. Vendors may implement proprietary authorization mechanisms for sensitive operations (based on the source BACnet address [and vendor-identifier] or using the Confirmed-Private-Transfer service).

Future:

Addendum cp of the BACnet Standard, approved in November 2024, defines a mechanism for adding strong authentication and authorization to client devices so that target devices can allow or deny certain BACnet network operations based on the identity of the client device and the requested operation. The credentials are carried in BACnet/SC BVLC data options. The trusted network infrastructure (BACnet/SC hubs and routers) attest to source of requests from devices which used strong authentication during their initial connection to the network (see addendum cp, Clause 17.3). The feature uses role-based authorization based on the OAuth 2.0 model, with some modifications borrowed from the IETF Authentication and Authorization for Constrained Environments (ACE) initiative. The roles are known as *scopes* in OAuth.

Devices will need to meet interoperability requirements (likely to be defined in future BIBBs) such as:

- Devices should support standard scopes for common interoperable operations, including the following:
  - Use of priority for command prioritization of writable present-value properties
  - Network Port Object operations
  - Addendum cc certificate management operations
  - Procedures in Clause 19 of the BACnet Standard—including Backup/Restore and Restart
  - Configuration and control of specific vertical systems
- Devices should support site-configurable scopes for custom applications.
- Devices may support manufacturer-specific scopes for common proprietary applications.

Devices should log diagnostic information (see section 13.5 of this document).

9.4 References and Related Resources

- ASHRAE Standard 135-2020
  - Addendum cp
  - Support Device Identity and Authorization at network request level
  - Uses OAuth 2.0 model
- ISA/IEC 62442 3-3, *System Security Requirements and Security Levels* (ISA/IEC 2013)
  - SR 1.2, *Software Process and Device Identification and Authentication*
  - SR 2.1, *Authorization Enforcement*
  - SR 2.8, *Auditable Events*

    - SR 3.9, *Protection of Audit Information*
    - SR 4.1, *Information Confidentiality*
    - SR 6.1, *Audit Log Accessibility*
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
    - Top-down framework defining scope and best practices for cybersecurity standards and end-user policies and processes. Provides cross-references to many existing cybersecurity standards, including the ISA/IEC 62443 family.
    - PR.AC-1, *Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes*
    - PR.AC-2, *Physical access to assets is managed and protected*
    - PR.AC-6, *Identities are proofed and bound to credentials and asserted in interactions*
    - PR.PT-1,*Audit/log records are determined, documented, implemented, and reviewed in accordance with policy*
- NIST 800-82 rev2, *Guide to Industrial Control Systems (ICS) Security* (Stouffer et al. 2015)
- NIST 800-53 rev5, *Security and Privacy Controls for Information Systems and Organizations* (NIST 2020)

10

Secure Product Development and Vulnerability Management

Cybersecurity of BAS products and systems is achieved not only by the inclusion of product and system features but also by the methods used to develop thr products and systems. Although this document focuses on product functionality that is related to cybersecurity, the product development process used by manufacturers will have an impact on the quantity and severity of vulnerabilities in their products.

10.1 Product Vulnerability Management Guidelines

VUL-1 Manufacturers **should** implement a secure product development process that will reduce the number and severity of vulnerabilities over the lifetime of each product.

VUL-2 Manufacturers **should** have means for tracking vulnerabilities in their products and for informing their customers about important vulnerabilities and their possible remediations or mitigations.

10.2 References and Related Resources

For more information about secure product development processes and product vulnerability management, consult the following references:

- ISA/IEC 62443-4-1, *Secure product development lifecycle requirements* (ISA/IEC 2018a)
- Microsoft Security Development Lifecycle (SDL)
- NIST SP 800-218, *Secure Software Development Framework V1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* (Souppayaet al. 2018)

11

Firmware Updates

Traditionally, building automation and industrial control equipment and devices left the factory with firmware on a ROM or EEPROM chip. The firmware was a monolithic binary image, which might be constant over the installed lifetime of the device. Firmware updates might be possible via a proprietary field service process.

Modern controllers may use nonvolatile storage for configuration and a variety of software such as boot loader, operating system, applications, or control programs. Manufacturers may provide mechanisms for end users or field service personnel to update this software. BACnet® defines Device Object properties (Protocol_Revision, Firmware_Revision, Application_Software_Version, Database_Revision) that can describe the state of a device's software.

BAS controls and equipment may have long installed lifetimes. Markets expect product updates (particularly security updates) to be available for a corresponding product support life cycle.

11.1 Motivation

Bug Fixes—Device software may be updated periodically to fix software defects andimprove stability and interoperability. Vendors may wish to update devices due to updates to operating systems or open-source/third-party libraries.

Vulnerability Patches—Device software may be updated to fix known vulnerabilities in device software that can be used by cybersecurity exploits. Vendors may wish to track and patch known vulnerabilities in operating systems or open-source/third-party libraries used by devices. Customers may have policies or contractual requirements around the timeliness of patching vulnerabilities. There is an expectation that vendors will adhere to standards for tracking, disclosing, and rating vulnerabilities (e.g., CVSS score).

Protocol Updates—During the installed lifetime of a device, standard network protocols (including BACnet) may be updated to change the required behavior and message syntax. Sites may deprecate the use of old or insecure protocol options or require the use of updated cipher suites.

Root Credential Updates—Updated root certificates (for PKI or manufacturer) may be provided to devices as part of secure firmware updates.

Feature Updates—Manufacturers may use firmware updates to add or extend product features. For example, devices shipped with support for BACnet/IP may be field-upgradable to support BACnet/SC. Devices with support for BACnet/SC using proprietary configuration mechanisms

may be field-upgradeable to support Network Port Object configuration as defined in addendum cc of the BACnet Standard.

11.2 Security Considerations

Insecure update processes could provide a mechanism to load malicious code onto devices, either by compromising the supply chain to spoof a legitimate update or by a malicious actor using the update mechanism directly.

Remote (over-the-air) updates could be interfered with mid-transaction, either to interrupt the update or to corrupt the update content.

An update might not be applied to the correct device, unintentionally or due to a malicious actor spoofing devices to prevent intended updates.

A firmware update mechanism may be used legitimately to downgrade a device to a previous version. However, owners may wish to forbid the downgrade of a device to a version with known vulnerabilities.

A firmware update mechanism needs to be robust so that a failed update cannot be used to disable a device as a denial-of-service attack.

Mitigations for security concerns for firmware update mechanisms include the following:

- Provide physical security for devices to limit access to firmware update mechanisms.
- Require authentication and integrity checking of firmware updates.
- Require authentication of devices receiving updates.
- Require authorization for firmware update mechanisms.
- Firmware update processes should be supervised and verified.
- Monitor the network for loss of communication to devices.
- Support device reset to recover from failed firmware updates.
- Monitor device database and firmware states to detect unexpected changes.
- Secure development life-cycle best practices, such as vulnerability tracking and disclosure.

11.3 Device Guidelines

IT devices and consumer-oriented IoT devices are expected to have firmware update mechanisms that can be initiated by end users. OT and BAS devices may require firmware update mechanisms to be used by authorized service personnel. The timing of updates may need to be managed carefully, and the process may include verification of correct resumption of system operation. BACnet/SC devices might be expected to be updated over their working life to track changes to the underlying IT protocols including TLS support, cipher suites, and library vulnerability patches.

> **FWU-1** A device **should** have the ability to receive firmware updates, particularly to address security issues. An update could be an entire firmware image or an incremental patch.
>
> **FWU-2** Firmware update processes **should** validate the authenticity and integrity of updates.

This guideline is consistent with ISA/IEC 62443-4-2 NDR/EDR 3.10 at the SL-C 2 level. Devices may be configured with a manufacturer root of trust to validate signed update files. Proprietary

update mechanisms may validate updates in the tool chain rather than the end device. A device is still expected to do credential checking at interfaces used by maintenance tools.

FWU-3 Firmware update processes **shall** be able to apply updates without a connection to the Internet.

FWU-4 It **should** be possible to apply updates across the local network (without physical access to the device).

- BAS devices are often in locations that are difficult to physically access.
- BAS devices are often installed in large quantities, so physical access to all devices for periodic maintenance is cost prohibitive.

OT systems and BASs do not want system outages during updates and need control over the timing of updates. Life safety or physical access control systems may require additional oversight and validation during the application of updates. Service contracts may require verification of correct system operation after the application of updates. Many sites (pharmaceutical, industrial) require that periodic maintenance be performed only during scheduled production downtime.

FWU-5 Firmware update processes **shall** include the ability to manually initiate updates. They may provide the ability to schedule updates. They may provide the ability for automatic updates (if system availability will not be affected by the update; for example, an update for a workstation or data collection device or in a noncritical environment).

FWU-6 After a firmware update a device **should** maintain its configuration or provide a mechanism for restoring its configuration.

- If network and security configuration are not able to be maintained across a firmware update, the device **shall** repeat a trusted onboarding process to provide the initial network and security configuration.

FWU-7 A successful firmware update **shall** result in the Device Object Firmware_Revision property reflecting the revision in the update.

FWU-8 A device **should** log attempts and results of firmware updates.

- See section 13.4.2 of this document (Network/Security Alerts), Clause 19.6 of the BACnet Standard, and ISA/IEC 62443 Part 3-3 SR 2.8.
- A device **may** provide device restart notifications (Clause 19.3 of the BACnet Standard).

FWU-9 If a firmware update fails, the device **shall** be able to recover or continue with the previous firmware image.

Future:

There is no consensus currently to standardize a BACnet mechanism for interoperable firmware updates. Standard IT mechanisms may emerge, such as IETF RFC 9019, *A Firmware Update Architecture for Internet of Things*.

A future BACnet addendum would define standard authorization requirements if updates were deployed using BACnet Files, and possibly testable features to confirm the integrity and authenticity of update files.

11.4 References and Related Resources

- Google Application Security Requirements for IoT Devices
  - Verified firmware updates
  - Scalable process for firmware updates
  - Commitment to security updates
- ISA/IEC 62443 Security for Industrial Automation and Control Systems
  - Family of standards for OT cybersecurity
- ISA/IEC 62442-4-1, *Secure Product Development Lifecycle Requirements* (ISA/IEC 2018a)
  - DM-5, *Disclosing Security-Related Issues*
  - SUM-4, *Security Update Delivery*
- ISA/IEC 62443-4-2, *Technical Security Requirements for IACS Components* (ISA/IEC 2018b)
  - Requirements for devices (NDR/EDR 3.10 SL-C 2 control system recovery)
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
  - Top-down framework defining scope and best practices for cybersecurity standards and end-user policies and processes. Provides cross-references to many existing cybersecurity standards, including the ISA/IEC 62443 family.
  - PR.DS-6 Integrity checking of software/firmware
- Common Vulnerability Scoring System (CVSS) v3.1—US National Vulnerability Database maintained by NIST (NIST 2019)
- Common Vulnerability Reporting Framework (CVRF) v1.1—MITRE CVE (NIST 2018)
- Commercial Product Support Lifecycle policies—Defining availability of service, support, repair parts in terms of end-of-sale and end-of-life milestones
- UK Code of Practice for IoT Devices (DDCMS 2018)
  - Guideline #2—Implement a vulnerability disclosure policy
  - Guideline #3—Keep software updates

12

Backup and Restore

Building automation controls and equipment are often configured with site-specific credentials, settings, and control sequences. The goal of backup and restore capabilities is to enable the timely resumption of correct system operation after a failure or cybersecurity incident. In general, the full dynamic state of devices (notification subscriptions, trend logs, recent history) may not be captured by a backup process. Building automation workstations and servers are typically backed up using standard IT tools.

The appropriate backup strategy for devices may depend on their mechanisms for configuration:

- Local configuration interface (device maintains the configuration)
- Interoperable online configuration (for example, the Network Port Object or writable configuration objects such as Notification Class)
- Proprietary online configuration where the device maintains the configuration
- Proprietary online configuration from a central database

In the last case, backing up the central database may be sufficient for allowing system recovery for that vendor's equipment. However, addendum cc of the BACnet Standard requires interoperable online configuration for certain network settings, including credentials (particularly BACnet/SC operating and signing certificates). Many devices permit dynamic creation/modification/deletion of objects via interoperable BACnet® messages. A device may update its database-revision property when these changes occur, but it is not required for all such changes. A proprietary configuration tool would need to monitor devices for changes to those settings and perform a targeted backup to complement the configuration maintained in the central database. A proprietary configuration tool would need to check for untracked changes in devices before performing a restore.

Backup and restore capabilities are required for some BACnet devices. The content and format of the backup file set is not defined. BACnet Standardized Device Profiles require support for clause 19.1 of the BACnet Standard Procedures for Advanced Workstations (as clients, BIBB DM-BR-A) and Building Controllers (as servers, BIBB DM-BR-B). The procedure uses the ReinitializeDevice service and BACnet File Objects. The only authorization is a plaintext password in the ReinitializeDevice service (possibly one per transaction type). As a result, the interoperable BACnet restore mechanism is not widely trusted.

12.1 Motivation

Compliance with Site Policy—A site may require systems to support a backup policy, perhaps motivated by NIST Cybersecurity framework subsection PR.IP-4, *Backups of information are conducted, maintained, and tested*.

Device Replacement—A replacement device will likely require unique settings and credentials, but its onboarding process could merge other settings from a backup of its predecessor.

Restore after Device Reset—A device (or even workstation/server) needs to be reset and restored to recover from a failure or ransomware attack.

Restore after Firmware Update—A device may not have all of its configuration maintained across a firmware update. It may need a direct restore from a backup or may need to have a backup converted to a recent version to be compatible with upgraded features.

Restore after Misconfiguration—If configuration changes are applied to the wrong device, or if incorrect configuration changes are made, restore a device to a last known good configuration.

Restore after Intrusion—If a device has been compromised, it may require a reset or firmware update. Its configuration may also be compromised and require arestore to a last known good configuration. The intrusion may have occurred many months before being detected.

Interoperable vs. Proprietary Configuration—Network/security settings may be managed at a site by one vendor and the application configuration may be managed by the device manufacturer (or their channel). Different backup and restore capabilities may be needed in a device to support each management channel.

Server Failure/Disaster Recovery—To protect against scenarios where local backups would be lost or corrupted, backup file sets may be archived off site.

Off-line or Onboarding Restore—If the configuration information that needs to be restored includes network settings and credentials, then that information may need to be extracted from a backup file set by a proprietary tool for use in a device onboarding process, or the device may need to be restored via a local configuration interface.

12.2 Security Considerations

If a device pauses normal operations during a backup or restore, then unauthorized initiation of backup mode could be used as a denial-of-service attack.

A site may wish to prevent unauthorized disclosure of system information in a backup file set.

Unencrypted credentials should not be disclosed in a backup file set.

Restoring a device from an invalid backup file set (intentionally or accidentally) could leave a device in an invalid configuration and result in denial of service.

Backup and restore operations may be considered auditable events by a site.

Mitigations for security concerns for backup and restore mechanisms include the following:

- Provide physical security for devices to limit access to backup and restore mechanisms.
- Require authentication and integrity checking backup file sets during a restore.
- Require authorization for backup and restore mechanisms. Backup processes should be supervised and verified.
- Audit backup and restore operations.

- Require inactivity timeouts in backup and restore mechanisms.
- Monitor the network for loss of communication to devices.
- Support device reset to recover from failed restores.
- Monitor device database and firmware state to detect unexpected changes.

12.3 Device Guidelines

12.3.1 General Capabilities

High-security markets (such as military, hospital, government) may require system backup and restore capabilities meeting the requirements of ISA/IEC62443-3-3 SL2. The site may require a disaster recovery plan, and a system may need to support testing of the recovery plan. IT may be involved in the backup and restore of system elements which are computers with standard operating systems.

> **BR-1** Workstations/servers **should** be able to be backed up by a standard IT mechanism. Current conditions are motivating sites to be prepared to recover from ransomware attacks.

Interoperable online management of network and security configuration (via a mechanism specified in addendum cc of the BACnet Standard, for example) means that not all configuration changes are guaranteed to flow through a vendor's tool chain.

> **BR-2** Vendors **should** provide the capability to back up a device's configuration. The capability could be through a local configuration interface, interoperable online mechanism, or proprietary online mechanism. The restore operation may require a proprietary toolset.

> **BR-3** Network, security, and application configuration that can be updated via an interoperable online mechanism **should** be included in backup file sets.

Vendors may provide backup for proprietary application configuration, executables, and firmware.

> **BR-4** Backup file sets **may** need to exclude or encrypt sensitive information (e.g., personal information covered by HIPAA or GDPR or credentials).

> **BR-5** Devices **should** be able to verify the authenticity and integrity of backup files during a restore operation, ideally by signing the backup files with vendor tool or device credentials.

> **BR-6** Backup files **may** be encrypted.

> **BR-7** A device **should** log attempts and results of backup and restore operations.

- See section 13.5 of this document, Clause 9.6 of the BACnet Standard, and ISA/IEC 62443 3-3 SR 2.8.

A device **may** provide device restart notifications (Clause 19.3 of the BACnet Standard) if a device restart is part of restore operation. A device **should** update the Last-Restart-Reason and Last-Restore-Time properties.

> **BR-8** Backup and restore mechanisms **should** have inactivity timeouts.

12.3.2 Online BACnet Backup and Restore

The procedure for interoperable online backup and restore is defined in Clause 19.1 of the BACnet Standard. The current procedure relies on physical security of the network, since the only authorization mechanism is a clear text password included in the ReinitializeDevice operation. Other clients are locked out of operations on the backup files while a device is in backup or restore mode, but the BACnet address (SADR/SNET) of the initiating client is the only means for a device to enforce this. The BACnet procedures include an inactivity timeout.

The B (or server) side of the backup and restore BIBB (DM-BR-B) is required for the building controller profile. However, all devices supporting online management of their network/security configuration (addendum cc of the BACnet Standard) will need to support some form of backup of that information.

> **BR-9** Devices **may** support DM-BR-B. It is strongly recommended that devices support the sensitive information protection (BR-4), authenticity, and integrity (BR-5) requirements above.

Future:

When the BACnet authorization proposal (currently in public review) is approved, it is expected that the interoperable online backup and restore procedures will be updated in a follow-on proposal to improve security. Updated procedures may include the following:

- Deprecate the use of the cleartext password in BACnet's ReinitializeDevice service.
- Use BACnet authentication and authorization data options during backup and restore transactions.
- Require authenticity and integrity validation of backup file sets upon restore.

12.4 References and Related Resources

- ANSI/ASHRAE Standard 135-2020
  - BACnet Procedures 19.1, *Backup and Restore*
  - Annex K: BACnet Interoperability Building Blocks: DM-BR-A, DM-BR-B
  - Annex L: Descriptions and Profiles of Standardized BACnet Devices: B-AWS, B-BC
- ISA/IEC 62442-3-3, *System Security Requirements and Security Levels* (ISA/IEC 2013)
  - SR 7.3, *Control system backup*
  - SR 7.4, *Control system recovery and reconstitution*
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
  - Top-down framework defining scope and best practices for cybersecurity standards and end-user policies and processes. Provides cross-references to many existing cybersecurity standards, including the ISA/IEC 62443 family.
  - PR.IP-4, *Backups of information are conducted, maintained, and tested*
  - RC.RP-1, *Recovery plan is executed during or after a cybersecurity incident*

13

System Diagnostics

Service personnel need tools and device features to enable network diagnostics and security monitoring. Abnormal or unexpected system behavior may be a symptom of an error or an intrusion. Diagnostic capabilities may be used temporarily in response to an event or may be ongoing to detect symptoms leading up to an event and provide forensic data during response to an event.

These capabilities reduce the effort of troubleshooting, identify communications and configuration problems, and detect unexpected and noncompliant behavior. These capabilities are useful for all BACnet® network types (BACnet/IP, MSTP, BACnet/SC). Diagnostic capabilities are especially needed to facilitate the diagnosis of complex features inherent to BACnet/SC networks, particularly certificate management. Solving interoperability problems may require sharing diagnostic data with the off-site support groups of multiple vendors. However, in a secure network environment, diagnostic capabilities must not introduce vulnerabilities (back doors).

The diagnostic process includes steps such as the following:

- Data collection of settings, events, network messages.
- Analysis of data for anomalies: comparison against baseline, as well as validation rules.
- Forwarding data to off-site support.
- Diagnosis of possible root causes.
- Application of a solution and verification of correct system operation.

13.1 Motivation

Initial Onboarding—Multiple settings in IT equipment and a BACnet/SC node must all be configured correctly to permit the BACnet/SC node to connect to the system. If a node is unable to connect, service personnel will need diagnostic data about failed attempts with error codes recorded at the BACnet/SC hub and the node. Devices need off-line diagnostic support capabilities.

Network Disconnection—The reachability of a device or network may change due to an unintended change in configuration of BACnet or IT equipment. Online monitoring may detect disconnections, but devices may need off-line diagnostic support capabilities.

Sporadic Connection—Devices or networks may experience reduced performance due to the poor quality of a connection. System operation may continue, but with an increase in timeouts and retries. Diagnostic data may include traffic and error counters.

Duplicate Settings—Correct system operation requires uniqueness of certain device network parameters, such as IP address (ARP cache poisoning), BACnet/SC VMAC (via direct connect), Device-Instance, Device-Name, Network Number (in BACnet routers), and device certificates. Diagnostic mechanisms can detect duplicate parameters.

Unexpected Traffic—The participants in a BAS network do not change often; network changes typically coincide with updates to the physical building systems. So, it is an unusual event for new BACnet routers or new BACnet devices to appear on the network. It is also unusual to observe BACnet client requests originating from an address not associated with a known device.

Broken BACnet Transactions—In a multivendor system, there may be times when an interoperable BACnet transaction is not working. The source of the problem could be a faulty BACnet implementation, configuration errors, firewall interference, or the lack of correct authorization. Capturing the network messages permits on-the-wire forensics, which can be correlated with configuration information or error logs at each end of the transaction. Diagnostic data may need to be forwarded to both vendors' support groups for resolution of the problem.

Broken Security Policy—A system may be operating correctly but not be abiding by the intended security policy. There could be lapses in certificate management (violating requirements about certificate uniqueness, or certificate lifetimes), or devices could be operating with a downgraded security configuration. IT organizations may request diagnostic information on the network and security settings of devices to audit compliance with security policy.

13.2 Security Considerations

Diagnostic mechanisms may impose a performance burden on devices and the network. A device should prevent unauthorized parties from enabling diagnostic mechanisms as a form of denial-of-service attack.

Diagnostic mechanisms may need to temporarily disable security features (encryption, authentication, authorization, and/or auditing). If the root cause of a problem is not discovered and corrected, devices should not permit the owner/operator to accidentally or intentionally leave security features disabled. Devices should prevent unauthorized parties from enabling diagnostic mechanisms that disable security features.

Diagnostic mechanisms may expose sensitive system data. BACnet/SC protects data in transit with TLS encryption, and BACnet networks may also be physically protected. Diagnostic mechanisms may bypass these protections, so the data collected by diagnostic mechanisms should only be accessible to authorized users—including in communications with remote support groups.

Diagnostic mechanisms may be useful for cybersecurity oversight for intrusion detection and forensics. Devices should prevent unauthorized users from disabling diagnostic mechanisms and deleting diagnostic data.

Secure sites may have policies to disallow (not just disabled by device configuration) the presence of diagnostic capabilities in devices during normal operation. Such policies provide defense in depth against changes of configuration or compromise of the device and mitigate the intrusion tactic of "living off the land" using tools present in a compromised system. Devices designed for such an environment may need to be able to install and assert/verify a clean firmware version. Such a site may permit a diagnostic firmware version or temporary diagnostic monitoring equipment during commissioning or troubleshooting.

Mitigations for security concerns for diagnostic mechanisms include the following:

- Provide physical security for devices to limit access to diagnostic mechanisms.
- Require authorization for enabling/disabling diagnostic mechanisms.
- Enforce a temporary lifetime for diagnostic modes that disable security features.
- Require authorization to access and delete diagnostic data.
- Encrypt diagnostic data at rest and in transit.

13.3 Device Monitoring Guidelines

Device monitoring tools periodically query the current state of a device across the network. BACnet defines a number of diagnostic and status properties in various objects, which can be used to detect and diagnose problems.

13.3.1 BACnet Device Object

BACnet defines many required properties in the BACnet Device Object which can be monitored to track the current state of the device, including System_Status, Local_Time, Local_Date, Model_Name, Firmware_Revision, Application_Software_Version, Database_Revision, Device_Address_Binding.

SD-1 A device **should** support the following recommended optional properties in the BACnet Device Object:

- Location
- Serial_Number
- Last_Restore_Time
- Last_Restart_Reason
- Time_Of_Device_Restart

13.3.2 Network Port Object

The Network Port Object exposes configuration and status information, which can be monitored for diagnostic purposes.

A Network Port Object is required for data links other than BACnet/SC since BACnet protocol revision 17. Support for the Network Port Object for the BACnet/SC data link is defined in addendum cc of the BACnet Standard, approved in 2021. It is mandatory for devices supporting BACnet/SC data link and BACnet protocol revision 24 or higher. Network Port Objects for BACnet/SC have Network_Type SECURE_CONNECT and include many required diagnostic properties, including the tracking of connection states. Addendum cc of the BACnet Standard requires that the BACnet/SC certificate signing request, operational certificate, and signing certificate are exposed as BACnet File objects.

SD-2 SECURE_CONNECT Network Port Objects **may** use the Reference_Port mechanism to expose the IPv4 or IPv6 (PROTOCOL) and Ethernet (PHYSICAL) properties.

SD-3 SECURE_CONNECT Network Port Objects **should** support the optional Current_Health property. If a SECURE_CONNECT Network Port Object supports the VALIDATE_CHANGES command of the Command property, then it is required to support the Command_Validation_Result property.

SD-4 SECURE_CONNECT Network Port Objects representing BACnet/SC nodes **should** support the optional SC_Primary_Hub_Connection_Status and SC_Failover_Hub_Connection_Status properties.

13.3.3 IT Device Monitoring

IT systems may monitor devices to detect uptime/reliability, configuration changes, and unusual behavior. IT may also monitor traffic at switches or IP routers, looking for traffic from unexpected devices or ports. Vendors may choose to support IT monitoring protocols (for example, ICMP PING and SNMP v3) in their devices.

SD-5 A device **should** have IT monitoring protocols disabled by default.

SD-6 A device that can enable IT monitoring protocols **should** have a secure mechanism to do so. IT monitoring protocols should only be enabled with the permission of IT.

SD-7 A device's documentation **should** include a description of its required and optional network ports used for IT monitoring. See section 4.4 of this document.

13.4 Network/Security Event Logging

Network/security event logging can provide a historic data source to extend the view provided by instantaneous diagnostic property values. External network events and internal device events can be logged to support diagnostics and forensic analysis.

Changes to the security configuration or actions by users may be considered by some sites to beauditable events. Systems may implement audit logs at the server/workstation level. Some devices may also support the BACnet Audit Log procedure defined in Clause 19.6. or the BACnet Standard

- ISA 62443-3-3 SR 2.8, *Auditable Events*
    - Regarding record: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity, and audit log events
    - Regarding the inclusion of timestamp, source (device, software, user), etc.

BACnet network/security events may need to be forwarded to IT network/security tools for intrusion detection analytics.

SD-8 Devices **should** assign a severity level to a network/security event. One scheme would be the syslog standard severity levels.

SD-9 Devices **should** support configurable system logging levels—log events at a given severity level or higher.

SD-10 Network/security events **should** only be delivered to authenticated and authorized users/processes.

SD-11 The system **should** maintain the integrity of network/security events.

Network/Security events that may be logged by some device mechanism include the following:

- Restarts (and boot actions)
    - Initial network parameters
    - Certificate expiry times

- BACnet/SC connections, failed connection attempts, disconnections
- Other BACnet/SC connection state machine transitions
- TLS peer certificate validation information
- Dynamic changes to network parameters
- BACnet Error/Abort/Reject messages initiated or received
- BACnet Confirmed Request Timeouts

13.4.1 Local Logging

A device may log events locally and make them accessible via a local interface or vendor-specific tool. Devices may log application events and diagnostics in addition to network/security events. Local logs are particularly valuable for diagnosing problems during onboarding or network disconnection.

> **SD-12** Devices **may** maintain a local log which includes network/security events. Logging should include standard BACnet network/security events and include attributes corresponding to source BACnet address (SNET, SADR) where appropriate.

13.4.2 BACnet Alerts

A device may represent network/security events using the BACnet alert mechanism described in the AlertEnrollment Object definition (Clause 12.52 of the BACnet Standard). Such alerts may be sent as Confirmed-Event-Notifications and/or stored locally in an EventLog Object. At the time of this writing, the contents of such alerts are vendor specific.

> **SD-13** Devices **may** support the BACnet alert mechanism for logging and notifying network/security events. Alerts **should** include descriptive messages and include attributes corresponding to the source BACnet address (SNET, SADR) where appropriate.

Future:

We propose that a procedure be added to the BACnet Standard for using the alert mechanism for interoperable network/security event logging, including recommended network/security event types and event attributes.

The procedure would also define standard authorization requirements for viewing/modifying event logs containing network/security events and modifying the configuration of network/security event generation and notification.

An additional addendum is expected to define standard authorization requirements for the procedures for use of Audit Notifications and Audit Log objects.

13.4.3 IT Protocols

A device, particularly a larger device like a workstation or server that uses a common operating system, may have its event logs monitored. Customers may want those system events and user audit logs to be captured into a security information and event management (SIEM) tool. Such tools are used to provide real-time monitoring and analysis of system events and user actions to detect potential cybersecurity-related anomalies, unauthorized user behaviors, and other potential system threats.

SD-14 Devices **may** support IT logging (via syslog or Windows Events). Logging **should** include standard BACnet network/security events and include attributes corresponding to source BACnet address (SNET, SADR) where appropriate.

Additional recommendations for syslog usage include the following:

- Configurable to support syslog over TCP or UDP
- Configurable destination port (default 514)
- Configurable facility code level (typically Local Use 0-7)
- Configurable syslog server by domain name or IP address
    - Implies device should be able to use DNS—DNS server address must then be configurable or set via DHCP
- Configurable Severity Level (may depend on logging level of event)—local authorities may restrict usage of some codes
- Consider support for standard event formats within syslog messages: CEF (ArcSight—Common Event Format), LEEF (IBM—Log Event Extended Format)

For integration of IT/OT/BAS events, various event sources need to have a common time standard of timestamps.

13.5 Network Message Capture

A traditional technique for troubleshooting BACnet/IP networks has been network message capture (packet capture). Packet capture files can be shared with off-site support teams to diagnose complex problems. However, many secure environments prohibit raw packet capture of network traffic.

For BACnet/SC networks, where the traffic is carried by encrypted TLS sessions, traditional packet capture can record the establishment of BACnet/SC connections, but it cannot display the BACnet messages themselves without additional assistance.

SD-15 Devices **may** be required to be installed with firmware which does not contain message capture capabilities. Temporary diagnostic devices or firmware versions **may** be used during commissioning and removed from the system for normal operation.

SD-16 When the capability does exist, a device **shall** permit only authorized users to enable/disable/configure message capture. Changes to configuration are auditable events.

SD-17 Message capture data **should** be encrypted at rest and in transit. Only authorized users and processes should have access to message capture data.

SD-18 Message capture mechanisms which reduce security **should** be temporary and revert automatically to normal operation after a defined time.

13.5.1 BACnet Hub/Device Above WebSocket Message Capture

One alternative is capturing BACnet/SC BVLC messages (at a BACnet/SC hub, node, or router) above the WebSocket layer (and hence above TLS encryption). In this alternative, non-BACnet traffic and TLS handshakes are not captured.

BACnet/SC BVLC messages can be used to diagnose problems once a successful BACnet/SC connection has been established. Comprehensive error logging may be a substitute diagnostic technique.

SD-19 Devices **may** implement secure message capture of BACnet BVLC messages.

13.5.2 Full Network Message Capture

Another alternative is to capture all network traffic in a standard format using a tool such as PCAP or Wireshark. This enables diagnostics that require correlation with non-BACnet traffic or TLS handshakes.

Diagnostic and security tools may be built into IT network infrastructure (switches). Standard tools may not have an existing key escrow mechanism. Standard tools may not be "BACnet aware" and instead use traffic analysis to detect unexpected situations.

Work-arounds to permit diagnostics of BACnet/SC traffic with general network message capture might include disabling encryption in TLS in a pair of communicating devices or having one end of a TLS session export pre-master secrets to share with a packet analysis tool. Both of the work-arounds could introduce security holes into products.

SD-20 Devices **should not** provide a mechanism for disabling TLS authentication for BACnet/SC. Devices **shall** always validate peer BACnet/SC operational certificates as specified in Annex AB of the BACnet Standard. Onboarding/configuration tools **should** relax certificate lifetime validation when directly connecting to devices with expired certificates.

SD-21 Devices **may** provide a mechanism to escrow the pre-master secret (session key) for a TLS session. Session key escrow is preferable to disabling TLS encryption for the following reasons:

- Disabling encryption exposes traffic on the network in real time, potentially to all network participants. Escrowed session keys expose historic traffic, but only to recipients of the keys.
- Escrowed session keys should be encrypted at rest and in transit—possibly with the public key of the intended recipient.
- Both ends of the TLS session need to be configured to permit disabling of TLS encryption (which weakens the security of other connections to the hub), but escrowed session keys can be implemented at one end of the connection without reconfiguring the other device.
- An escrowed session key is only valid for the single session.

Recommendation **SD-19** would require the device to start a new TLS session after a reasonable period of time, and the new TLS session would have a different session key.

- Packet decoding tools need the network message log for the complete TLS session in addition to the escrowed session key to decode the TLS contents.

Site policy might restrict the session key escrow capability to diagnostic hubs/routers that are removed from the system during normal operation.

13.6 References and Related Resources

- RFC 5424, *The Syslog Protocol* (Gerhards 2009)

- ISA 62443-3-3, *System Security Requirements and Security Levels* (ISA/IEC 2013)
  - SR 2.8, *Auditable events*
  - SR 3.9, *Protection of audit information*
  - SR 4.1, *Information confidentiality*
  - SR 6.1, *Audit log accessibility*
  - SR 6.2, *Continuous monitoring*
  - SR 7.6, *Network and security configuration settings*
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
  - PR.PT-1 Audit Logs
  - DE.AE-3 Event data collected and correlated from multiple sources
  - DE.CM-1 Network monitoring

14

Network Segmentation

Network segmentation is the intentional partitioning of a system into multiple physical or logical network segments.

BASs are typically divided into multiple network segments to improve performance, cost, availability, and security. A network segment could use wired connections with a ring, daisy chain, bus, or star topology or use a wireless data link layer. Supervisory, building, and campus networks may use standard IT switched network technology (typically Ethernet, possibly on VLANs). Remote access may also be provided using standard IT technology such as VPNs and firewalls.

BACnet® provides a mechanism for communicating across multiple network segments using BACnet routing. A large controller on a BACnet/IP network segment may function as a BACnet router to a directly connected MS/TP field network segment. A BACnet router may join a BACnet/IP network segment on a BAS-only, isolated, Ethernet network to a BACnet/SC network segment on the building IT Ethernet network.

14.1 Motivation

Physical—BASs may require physical network technologies for low-cost field devices other than IT network technologies (switched Ethernet, Wi-Fi). Those field networks may be lower speed and may use inexpensive wiring or wireless technology. Those field networks can be connected to the larger BAS using BACnet routers or via gateways or application-level integration. An example of physically motivated network segmentation is using BACnet routers to connect BACnet/SC and BACnet MS/TP (low-speed, low-cost twisted-pair wiring) network segments.

Secure System Migration—With the introduction of BACnet/SC, devices in BACnet-based BASs can migrate to a modern, secure network technology. Network segmentation provides a mechanism to connect newer BACnet/SC devices to an existing, insecure BACnet/IP or MS/TP network. Existing BACnet/IP network segments may be protected in a VLAN implemented by IT switches, and existing network segments may be secured physically but require a connection point to external networks. Monitoring and firewall policy can be implemented at connection points between the network segments to add security to the system.

Security—A best practice for secure networks is to segment the network into zones of differing security levels. Monitoring and firewall policy can be implemented at connection points between all network segments. Some network segments may require physical isolation on distinct infrastructure (switches and wiring). Network segments may be logically isolated in a VLAN on shared network infrastructure. A large BAS may be partitioned into security zones by geography or pri-

mary vendor or function (for example, building networks vs. campus backbone, access control vs. HVAC, or central plant network vs. zone network). The security policy at a site may require that BAS network segments have restrictions on inbound and outbound access to the Internet.

Reliability and Fault Tolerance—BASs are typically designed to provide reliability via local control when network connectivity is impaired. Critical systems may have a dedicated network segment with industrial-grade network equipment or redundant wiring or backup power. Network segmentation provides controlled access to the local network segment.

Availability and Performance—Network segmentation is often used to shield BAS devices from interference from IT traffic, and IT networks may need to be shielded from BAS network traffic (such as UDP broadcasts from BACnet/IP devices). BAS networks require allocation of many IP addresses for devices. Network segmentation can isolate BAS address allocation from the IT network. BASs typically have a control hierarchy, where supervisory controllers need to interact with nearby devices. The BAS network hierarchy can be aligned with the control hierarchy to limit network traffic needed for local control to a local network segment.

14.2 Security Considerations

Although network segmentation can be used to improve the security of a BAS, unauthorized (re)configuration of BACnet routers and firewalls could result in a denial of desired services or ineffective message filtering.

Possible mitigations for security concerns around unauthorized network configuration include the following:

- Provide physical security for routers and firewalls.
- Require authorization for (re)configuration.
- Monitor the network for communication through routers and firewalls.
- Log router and firewall (re)configuration attempts.

Unauthorized wireless (e.g., cellular) or tunneling protocol (e.g., VPN) connections can be used to bypass network segmentation and firewalls. Systems may include such capabilities for commissioning or maintenance. Site policy should forbid unauthorized remote network access capabilities during normal system operation. Possible mitigations for security concerns around unauthorized remote network access include:

- Provide a monitored mechanism for authorized remote access.
- Document device capabilities for remote network access and provide the end user a means to disable and monitor the capabilities.
- Monitor the network for communication through routers and firewalls.

14.3 Network Environment Guidelines

14.3.1 Network Isolation

BASs are often installed and operating in buildings before IT infrastructure and Internet connectivity is in place. BASs may also be physically or logically isolated (behind firewalls) and lack Internet access.

NSEG-1 Devices **shall** be able to be onboarded and operated without Internet access.

When BASs are using IT infrastructure, device network settings need to meet IT requirements. For example, there could be situations where there is no DHCP or only DHCPv6. See guidelines in section 4.6.

NSEG-2 (This recommendation has been removed.)

In a BAS system that uses BACnet with network segmentation, there may be constraints on the use of protocols other than BACnet. For example, a server/workstation outside an isolated BACnet network may be able to reach a controller via BACnet, but not SSH or TELNET or HTTPS. A site may permit interim protocol usage (e.g., wireless communication) during construction. A device vendor may need to report ports necessary for device operation (e.g., via MUD) that need to be forwarded by routers to isolated networks. See guidelines in section 4.4.

14.3.2 IT Firewall Compatibility

A BAS may be protected by IT firewalls between the Internet and the IT network, between the IT network and BAS, and between BAS network segments.

BAS devices can help detect when ports or destinations are blocked by IT firewalls unexpectedly. Ports or destinations may be blocked due to configuration errors or IT firewall rule changes.

NSEG-3 Devices **may** use BACnet Network/Security Alert logging (see section 13.5.2 of this document) to report failed attempts to use other protocols as well as BACnet.

BASs may expect IT firewalls to filter malformed packets (to prevent buffer overflow exploits), but this is not expected to impact BACnet/SC (since all traffic is inside TLS).

BASs may be forbidden from providing remote network access, except via authorized channels through IT firewalls.

NSEG-4 Devices **should not** include remote network access capabilities that bypass IT firewalls.

14.4 BACnet Firewall/Router Guidelines

14.4.1 Monitoring/Filtering

BACnet firewall/routers monitor and filter BACnet messages routed between network segments according to a site's security policy. The filtering rules can be BAS-aware, based on BACnet message type, which may be difficult to implement in commonly used IT firewalls/switches. BACnet/SC messages travel within encrypted TLS connections and are only visible and filterable at the connection endpoints.

BACnet/SC messages are not expected to be filtered by end devices, as BACnet authorization is expected to be used for controlling device behavior in the future. Devices may use port-level firewall features on BACnet data links other than BACnet/SC and to filter other protocols.

In general, BACnet messages should not be filtered by the BACnet/SC hub. This would not provide strong security since devices can bypass the hub with direct connections. However, there could be utility in filtering some BACnet broadcasts (for example, Time Synchronization) that are normally relayed by the BACnet/SC hub.

An example filter/monitor scenario is shown in Figure 14.1. A BACnet/SC network segment (Network 1) provides the secure backbone of the BAS. All devices on that network segment have been

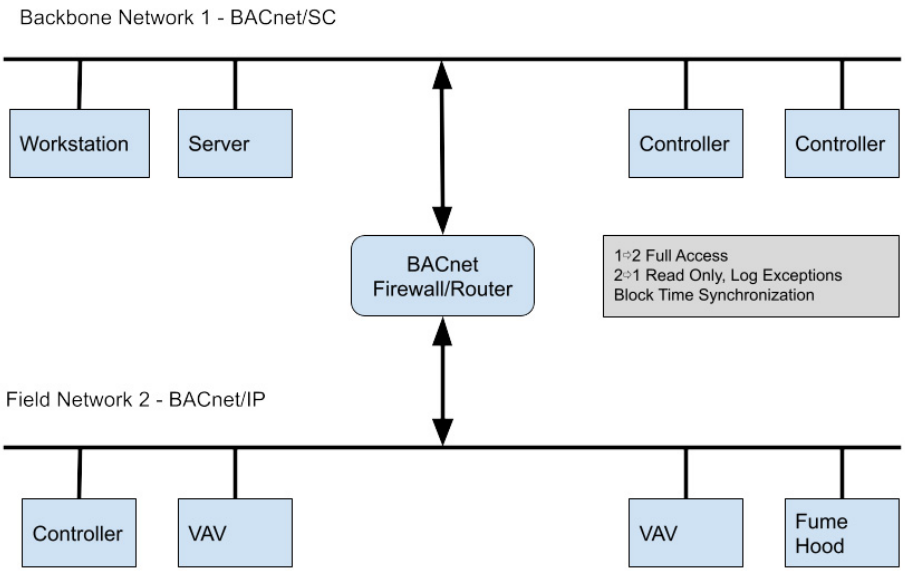

Figure 14.1 Example BACnet internetwork with a BACnet firewall/router.

granted permission to participate in the network via a BACnet/SC signed TLS certificate. Workstation and server nodes on that network segment enforce authorization policy for users. A BACnet/IP network segment (Network 2) is a field network for a floor in the building. The controller on Network 2 manages devices on its own network segment but does not need access devices on the backbone. Devices on the backbone (particularly the workstation and server) are expected to need management access to devices on the field network. The devices, cabling, and switches for Network 2 are physically secured to an extent (being located in mechanical rooms or ceiling plenums), but if someone obtained physical access to the field network, they would have full access to all BACnet network segments in the absence of filtering at the BACnet router.

To provide defense in depth, the BACnet router connecting Networks 1 and 2 could be configured to allow full access from the trusted backbone (Network 1) to the field network (Network 2) but limit traffic to read-only access in the other direction. In addition, the site could implement a policy to block the BACnet time synchronization services from crossing network segments.

The focus of BACnet firewall/router monitoring and filtering policy is to detect/prevent unauthorized transmission of well-formed BACnet requests to devices across a network segment boundary, particularly when BACnet Authorization is not available on one or both network segments.

> **NSEG-5** BACnet firewall/routers **should** be able to monitor/filter BACnet-Confirmed-Request-PDUs (with segmented-message=FALSE or sequence-number=0) and BACnet-Unconfirmed-Request-PDUs.
>
> - Unexpected BACnet PDUs of other types will be ignored by target devices.

- Unexpected BACnet-Confirmed-Request-PDUs after the first segment will be ignored by target devices.

NSEG-6 BACnet firewall/router message handling **should** be determined by configurable rules, each of which supports one of the following actions:

- Allow—Allow message
- Block-Drop—Silently drop the message
    - Required for unconfirmed requests. An option for confirmed requests.
    - May be required by a site to prevent probing.
    - Will result in retries and a timeout for confirmed requests.
- Block-Abort—Drop the message and send a BACnet-Abort-PDU to the initiating device (as if it came from the target device) containing the message's invokeID and AbortReason=security-error (5).
    - An option for confirmed requests.
    - Immediately cancels the transaction.
    - Provides feedback to the initiating device that it is not authorized.
    - May be disallowed by a site to prevent probing.

NSEG-7 BACnet firewall/router message handling rules **should** each support enabling/disabling monitoring features:

- Log and/or send an Alert when the rule is triggered (see section 13.5, Network/Security Alert Logging).
- Collect per-rule statistics when the rule is triggered (message count, byte count).

NSEG-8 A BACnet firewall/router's rule data model **should** support common use cases including the followng:

- Blocking Time Synchronization messages
- Blocking Global broadcasts
- Enforcing a Read-Only policy for initiating devices on a specified network segment
- Permit Control/Configuration for known initiating devices
- Enforcing network hierarchy to limiting access between secondary network segments while allowing access from the backbone network segment

A BACnet firewall/router's rule data model should provide minimum capabilities for matching messages.

NSEG-9 Rules **should** be able to match on source and/or destination information including the following:

- BACnet network number
- Router BACnet port (or data link type)
- BACnet MAC address

NSEG-10 Rules **may** be able to match on source and/or destination BACnet Device Instance.

NSEG-11 Rules **should** be able to match on BACnetConfirmedServiceChoice or BACnetUnconfirmedServiceChoice.

NSEG-12 Rule data model **should** require Explicit Enable Rules (supports ISA/IEC 62443 3-3 requirement SR 5.2 at SL-2).

- This implies that if rule matching is enabled, and if no rules are matched for a message, then the default action of the firewall/router is to Block-Drop.

NSEG-13 Rules **should** only refer to service parameters guaranteed to be in the first segment of a confirmed service request.

NSEG-14 Rules **should** be matched in priority order, and the action and monitoring for a message is specified by the first rule matched.

NSEG-15 It **may** be possible to enable temporary rules for a limited time to assist maintenance or diagnostics.

A BACnet firewall/router may provide additional monitoring and statistics capabilities for all messages passing through it.

Future:

In the future, it expected that an annex will be added to the BACnet Standard defining the behavior described in this section.

An additional addendum could define object types or a file definition for interoperable configuration of BACnet firewall/router monitoring/filtering rules.

14.4.2 Island Mode

Island mode is the capability to isolate a network segment, particularly during the response to a cybersecurity incident. This capability supports ISA/IEC 62443 3-3 requirement SR5.2 at SL-3.

NSEG-16 A BACnet firewall/router **may** have the capability to disable (i.e., place OUT_OF_SERVICE) a BACnet port used by the BACnet routing function in order to isolate a network segment. There **should** be a similar capability to re-enable the port.

NSEG-17 The port-disable mechanism **should** require authorization.

NSEG-18 If the port-disable mechanism is accessible via a network, it **should** be accessed from an upstream or management port to disable/enable a downstream port.

Network segment isolation may be implemented in the IT switch/router fabric, in addition to isolation provided by BACnet routers. The IT switch/router fabric would be able to block all protocols from crossing between network segments. The IT switch/router fabric could disable a port used by a BACnet router.

14.5 References and Related Resources

- Google Application Security Requirements for IoT Devices
  - Requirement 15—No external network connectivity (i.e., don't bypass firewalls)
  - Guideline 3—Manufacturer Usage Descriptions (used to request external access through firewalls)
- IETF RFC 8519, *YANG Data Model for Network Access Control Lists (ACLs)* (Jethanandani 2019)

- IETF RFC 8520, *Manufacturer Usage Description Specification* (Lear et al. 2019)
- ISA/IEC 62443, *Security for Industrial Automation and Control Systems*
  - Family of standards for OT cybersecurity
- ISA/IEC 62443-1-1, *Terminology, Concepts, and Models* (IEC 2009b)
  - Defines concept of Security Zones and Conduits (which use network segmentation) for analysis and implementation of systems
- ISA/IEC 62443-3-3, *System Security Requirements and Security Levels* (ISA/IEC 2013)
  - Requirements for system design (SR 5.1, SR 5.2, SR 5.4) which specify network segmentation
- NIST Cybersecurity Framework version 1.1 (NIST 2018)
  - Top-down framework defining scope and best practices for cybersecurity standards and end-user policies and processes. Provides cross-references to many existing cybersecurity standards, including the ISA/IEC 62443 family.
  - In the Protect function, identifies subcategories (PR.AC-3, Remote access is managed, and PR.AC-5, Network integrity is protected) that specify network segmentation.

15

Mapping Recommendations to the BACnet Standard

Table 15.1 shows how the **shall** recommendations in this document correspond to the BACnet Standard (2020).

Table 15.1

Recommendation Identifier	BACnet Requires	BACnet Option	BACnet Silent	Notes
Network Access				
NAC-3	X			Note that products that support BACnet/SC **shall** enumerate the TLS versions and cipher suites supported for BACnet/SC in the product's BACnet PICS, in accordance with the requirements in Annex A and addendum cd of the BACnet Standard.
NAC-9				Devices that support BACnet/IP **(**Annex J of the BACnet Standard):
	X			◦ **Shall** support IPv4.
			X	◦ **Shall** permit IPv4 to be disabled if it is not being used.
	X			◦ The UDP Port **shall** be configurable in the range 47808–47832 and 49152–65535 (see Clause J.1.2 of the BACnet Standard).
	X			◦ BBMDs **shall** support DNS, since Broadcast Distribution Tables in Network Port Objects may contain DNS names starting with protocol revision 17 (see the definition of BACnetHostAddress in Clause 21 of the BACnet Standard).
NAC-10				Devices that support BACnet/IPv6 (Annex U of the BACnet Standard):
	X			◦ **Shall** support IPv6.
			X	◦ **Shall** permit IPv6 to be disabled if it is not being used.
	X			◦ BBMDs **shall** support DNS, since Broadcast Distribution Tables may contain DNS names (see definition of BACnetHostAddress in Clause 21 of the BACnet Standard).
	X			◦ The UDP Port **shall** be configurable in the ranges 47808–47832 and 49152–65535 (see Clause U.1.1.2 of the BACnet Standard).
NAC-12				IP Address configuration:
		X		◦ Devices supporting IPv4 **shall** be able to manually configure their IP address, subnet, and default gateway (if applicable).
		X		◦ Devices supporting IPv4 **shall** support DHCP for dynamic address allocation.
		X		◦ Devices supporting IPv6 **shall** support SLAAC—but not all sites may use it.

Table 15.1

Recommendation Identifier	BACnet Requires	BACnet Option	BACnet Silent	Notes
NAC-13				Configuring devices to know the address of the DNS server and other servers"
		X		◦ Devices supporting IPv4 **shall** support DHCP to obtain DNS server configuration.
		X		◦ Devices supporting IPv4 **shall** support manual configuration of DNS server.
		X		◦ Devices supporting IPv6 **shall** support DHCPv6.
		X		◦ Devices supporting IPv6 **shall** support SLAAC DNS option (2010).
		X		◦ Devices supporting IPv6 **shall** be configurable to obtain DNS server configuration via DHCPv6 or via SLAAC.
NAC-15			X	Devices **shall** be configurable to disable/block unused TCP and UDP ports and associated services.
NAC-17				Time service requirements for BACnet devices:
	X			BACnet devices using BACnet/SC **shall** maintain a clock with the current time and date during operation
NAC-18				Additional requirements for BACnet time recipients:
	X			Devices supporting DM-UTC-B **shall** support the BACnet Daylight_Savings_Status and UTC_Offset properties.
NAC-19				Additional requirements for BACnet time senders.
	X			The Time_Synchronization_Interval property **shall** be configurable to be 0 (to disable DM-ATS-A).
BACnet/SC Profiles and BIBBs				
BSC-1	X[a]			Manufacturers should provide a BACnet PICS for devices. This **shall** include supported TLS versions, additional supported cipher suites, digital signatures, and key exchanges.
BSC-2	X			Devices supporting BACnet/SC hub functionality **shall** conform to profile B-SCHUB (including NM-SCH-B).
BSC-3	X[b]			Devices initiating direct connections **shall** support NM-SCDC-A.
BSC-4	X[c]			Devices accepting direct connections **shall** support NM-SCDC-B.

a. The content is required if the PICS is provided.
b. Implied requirement.
c. Implied requirement.

Table 15.1

Recommendation Identifier	BACnet Requires	BACnet Option	BACnet Silent	Notes
Addendum CD and Supported Ciphers/Key Algorithms				
BSC-5			X	Devices capable of supporting TLS connections below version 1.3 **shall** provide a way to prevent the TLS connection from downgrading for a standard strict TLS 1.3 system.
BSC-6	X (implied)			Devices **may** support accepting BACnet/SC direct connection functionality to respond to high-traffic situations. Devices that support accepting direct connections **shall** support NM-SCDC-B.
BSC-7	X (implied)			Devices that initiate high-traffic operations **may** support initiating BACnet/SC direct connection functionality. Devices that support initiating direct connections **shall** support NM-SCDC-A.
Guidelines for devices that support BACnet/SC				
CM-1	X[d]			Devices **shall** support the cipher suites listed in addendum cd of the BACnet Standard, at a minimum:
CM-2	X			Devices/configuration tools **shall** support the file formats for CSR (RFC 7468 PEM) and Certificates (PEM format PKS7) as specified in Annex AB 7.4 of the BACnet Standard.
CM-5	X			Devices **shall** support a reset to factory defaults as defined by Clause AB 7.4.2 of the BACnet Standard.
CM-6			X	Devices **may** support online certificate updates via the mechanisms described in addendum cc of the BACnet Standard. Devices **shall** support a secure off-line (or non-BACnet) mechanism for onboarding and updating BACnet/SC certificates.
BACnet/SC Certificate Signing				
CM-10	X			Certificate signing tools **shall** support the file formats for CSR (RFC 7468 PEM) and Certificates (PEM format PKS7) as specified in Annex AB 7.4 of the BACnet Standard.
CM-12	X			Certificate signing tools **shall** support trust models: ◦ Self-Signed Root: Local and informal with one or two levels above CA ◦ Self-Signed Root: Local Customer IT CA or IT delegated CA ◦ PKI (public key infrastructure): Customer IT CA linked to the public root of trust

d. The requirement in the BACnet Standard is for devices that support protocol revision 23 or later.

Table 15.1

Recommendation Identifier	BACnet Requires	BACnet Option	BACnet Silent	Notes
Device Reset				
DR-1			X	A device **should** require authorization for a local reset mechanism (if possible). A device shall require authorization for a network-based reset mechanism.
DR-3			X	A device **shall** provide a capability to perform a local network/security reset.
DR-4			X	A successful network/security reset **shall** place a device in a mode that permits repeating its onboarding process.
Identity Authentication				
IA-8			X	BAS vendor developing BAS applications on smartphones **shall** follow best practices below: ◦ Password-protect your technology. ◦ Note that user credentials could be cached on the device. Such credentials should be stored securely.
IA-9			X	The BAS authentication system **shall** store user or device credentials in a secured/protected location and manner.
IA-10			X	The BAS **shall** protect against authentication exploits and vulnerabilities.
IA-12			X	BAS user authentication **shall** protect and not expose Session IDs or Identity Tokens.
IA-13			X	BAS Central User Account Management Systems **shall** be compliant with regional data privacy requirements (GDPR, California privacy laws, etc.).
Firmware Updates				
FWU-3			X	Firmware update processes **shall** be able to apply updates without a connection to the Internet.
FWU-5			X	Firmware update processes **shall** include the ability to manually initiate updates.
FWU-7			X	A successful firmware update **shall** result in the Device Object firmware revision property reflecting the revision in the update.
FWU-9			X	If a firmware update fails, the device **shall** be able to recover or continue with the previous firmware image.

Table 15.1

Recommendation Identifier	BACnet Requires	BACnet Option	BACnet Silent	Notes
System Diagnostics				
SD-16			X	When the capability does exist, a device **shall** permit only authorized users to enable/disable/configure message capture. Changes to configuration are auditable events.
SD-20	X			Devices **shall** always validate peer BACnet/SC operational certificates as specified in Annex AB of the BACnet Standard.
Network Segmentation				
NSEG-1			X	Devices **shall** be able to be onboarded and operate without Internet access

A

A Brief History of BACnet Cybersecurity

An ASHRAE project committee that developed the BACnet® protocol was formed in 1987 and the official BACnet Standard, ANSI/ASHRAE Standard 135, *BACnet—A Data Communication Protocol for Building Automation and Control Networks,* was first published in 1995. During the initial commercial deployments of BACnet-based systems, BASs were physically separate from IT systems in almost all cases. Cybersecurity was not a significant concern—at that time it was generally believed that an HVAC system was not likely to be targeted. Furthermore, network-based attacks on physically isolated BACnet-based HVAC systems required direct access to the BAS network.

This began to change in 1999 when the BACnet committee (Standing Standard Project Committee [SSPC] 135) defined a standard method for BACnet devices to communicate on TCP/IP networks, commonly referred to as BACnet/IP. Some facilities and campuses with existing TCP/IP networks began to connect a few BACnet/IP devices to those networks to make it easier to remotely monitor and manage those devices, and as a result, some of these devices inadvertently became Internet connected. However, the vast majority of BACnet devices continued to use low-cost communication methods, principally BACnet MS/TP.

Once BACnet devices were connected to shared networks, they became vulnerable to new avenues of attack. Not all attacks were malicious; for example, curious students searching for networked devices might accidentally interfere with BACnet communication in their university's BAS network. Cybersecurity-conscious building owners began to use network virtualization methods (VLANs and VPNs) to better control access to BASs that were connected to shared networks.

The BACnet committee took note of the increasing concern about the potential vulnerability of BACnet networks to cyberattacks amongst an influential minority of building owners, and a project was launched to define a new BACnet-specific method for securing all forms of BACnet communication, from BACnet MS/TP to BACnet/IP. This project resulted in a new addendum to the BACnet Standard, published in 2010. However, few manufacturers implemented this addendum, and it was removed from the 2020 edition of the BACnet Standard.

Manufacturers have taken advantage of the decreasing cost of computing hardware to build more sophisticated controllers, and an increasing number of the devices have been designed for BACnet/IP communication on Ethernet networks. As BACnet/IP devices became more common and were more likely to be connected to IT-managed networks, IT personnel paid increasing attention to the communication functionality and manageability of those devices.

The desire among some members of the BACnet committee to make BACnet become more IT friendly led to the establishment of the IT working group in 2009. The first concrete result of that group's efforts was BACnet Secure Connect (BACnet/SC), published in late 2019—a new communication method for BACnet that incorporates some modern cybersecurity features.

BACnet/SC leverages TLS (one of the Internet's most important protocols for secure communication) and ITU X.509 digital certificates. Note that BACnet/SC can only be applied on TCP/IP networks. BACnet/SC was incorporated into the BACnet Standard as Annex AB.

Addendum cc of the BACnet Standard, approved by ASHRAE in early 2022, defines an interoperable method for viewing and modifying the state of a device's BACnet/SC network port including the port's associated digital certificates. This enables improvements in the management of multivendor BACnet/SC networks.

Addendum cp of the BACnet Standard, published in November 2024, defines a mechanism for adding strong authentication and authorization to client devices so that target devices can allow or deny certain BACnet network operations based on the identity of the client device and the requested operation.

The BACnet committee is continuing to develop new BACnet-specific network security technologies. For an overview of some current and potential future work, see section 2.9 of this document.

References and Bibliography

References

ASHRAE. 2020. ANSI/ASHRAE Standard 135-2020, *BACnet®—A Data Communication Protocol for Building Automation and Control Networks*. Peachtree Corners, GA: ASHRAE.

ASHRAE. 2020. ANSI/ASHRAE Standard 135-2020, *BACnet®—A Data Communication Protocol for Building Automation and Control Networks*. Addendum cc 2022. Peachtree Corners, GA: ASHRAE.

ASHRAE. 2020. ANSI/ASHRAE Standard 135-2020, *BACnet®—A Data Communication Protocol for Building Automation and Control Networks*. Addendum cd 2021. Peachtree Corners, GA: ASHRAE.

ASHRAE. 2020. ANSI/ASHRAE Standard 135-2020, *BACnet®—A Data Communication Protocol for Building Automation and Control Networks*. Addendum cp 2024a. Peachtree Corners, GA: ASHRAE.

ASHRAE. 2020. ANSI/ASHRAE Standard 135-2020, *BACnet®—A Data Communication Protocol for Building Automation and Control Networks*. Addendum cs 2024b. Peachtree Corners, GA: ASHRAE.

ASHRAE. 2024. ANSI/ASHRAE Standard 135-2024, *BACnet®—A Data Communication Protocol for Building Automation and Control Networks*. Peachtree Corners, GA: ASHRAE.

ATA. 1999. ANSI/ATA 878.1-1999, *Local Area Network: Token Bus*. Darien, IL: ARCNET Trade Association. https://www.arcnet.cc/resources/ata8781.pdf

California State Legislature. 2018. *Information Privacy: Connected Devices*. Senate Bill No. 327. Sacramento, CA: California State Legislature. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

Cooper, D., S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC5280.

DDCMS. 2018. *Code of Practice for Consumer IoT Security*. London, UK: Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.

Fette, I. and A. Melnikov. 2011. *The WebSocket Protocol*. RFC 6455. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC6455.

IEC. 2009a. IEC TR 62443-3-1:2009, *Industrial communication networks—Network and system security—Part 3-1: Security technologies for industrial automation and control systems*. Technical Report. Geneva, Switzerland: International Electrotechnical Commission.

IEC. 2009b. IEC TS 62443-1-1:2009, *Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models*. Technical Specification. Geneva, Switzerland: International Electrotechnical Commission.

IEC. 2021. IEC 62439-2:2021, *Industrial communication networks—High availability automation networks—Part 2: Media Redundancy Protocol (MRP)*. Geneva, Switzerland: International Electrotechnical Commission.

IEEE. 2004. IEEE 802.1X-2004, *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. New York, NY: Institute of Electrical and Electronics Engineers.

IEEE. 2010. IEEE 802.1X-2010, *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. New York, NY: Institute of Electrical and Electronics Engineers.

IEEE. 2020. IEEE 802.1X-2020, *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. New York, NY: Institute of Electrical and Electronics Engineers.

ISA/IEC. 2013. ISA/IEC 62443-3-3-2013, *Security for Industrial Automation and Control Systems—Part 3-3: System Security Requirements and Security Levels*. Research Triangle Park, NC: International Society of Automation.

ISA/IEC. 2018a. ISA/IEC 62443-4-1-2018, *Security for Industrial Automation and Control Systems—Part 4-1: Secure Product Development Lifecycle Requirements*. Research Triangle Park, NC: International Society of Automation.

ISA/IEC. 2018b. ISA/IEC 62443-4-2-2018, *Security for Industrial Automation and Control Systems—Part 4-2: Technical Security Requirements for IACS Components*. Research Triangle Park, NC: International Society of Automation

ISA/IEC. 2020. ISA/IEC 62443-3-2-2020, *Security for Industrial Automation and Control Systems—Part 3-2: Security Risk Assessment for System Design*. Research Triangle Park, NC: International Society of Automation.

Josefsson, S., and S. Leonard. 2015. *Textual Encodings of PKIX, PKCS, and CMS Structures*. RFC 7468. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC7468.

Rescorla, E. 2018. *The Transport Layer Security Protocol Version 1.3*. RFC 8446. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC8446.

Moran, B., H. Tschofenig, D. Brown, and M. Meriac. 2021. *A Firmware Update Architecture for Internet of Things*. RFC 9019. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC9019.

NIST. 2001. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.* Federal Information Processing Standards Publication. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.140-2.

NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018.

NIST. 2019. FIPS PUB 140-3, *Security Requirements for Cryptographic Modules.* Federal Information Processing Standards Publication. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.140-3.

NIST. 2020. NIST Special Publication 800-53 (Revision 5), *Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5.

BIBLIOGRAPHY

Aboba, B., D. Simon, and P. Eronen. 2008. *Extensible Authentication Protocol (EAP) Key Management Framework*. RFC 5247. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC5247.

Baker, F., and D. Meyer. 2011. *Internet Protocols for the Smart Grid*. RFC 6272. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC6272.

Case, J., R. Mundy, D. Partain, and B. Stewart. 2002. *Introduction and Applicability Statements for Internet-Standard Management Framework*. RFC 3410. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC3410.

Frankel, S., B. Eydt, L. Owens, and K. Scarfone. 2007. NIST Special Publication 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-97.

Gerhards, R. 2009. *The Syslog Protocol*. RFC 5424. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC5424.

Google. n.d. Application Security Requirements for IoT Devices. Mountain View, CA: Google. https://partner-security.withgoogle.com/docs/iot_requirements.

Grassi, P.A., J.L. Fenton, E.M. Newton, R.A. Perlner, A.R. Regenscheid, W.E. Burr, J.P. Richer, N.B. Lefkovitz, J.M. Danker, Y.-Y. Choong, K.K. Greene, and M.F. Theofanos. 2017. NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b.

Hardt, D. 2012. *The OAuth 2.0 Authorization Framework*. RFC 6749. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC6749.

Hu,V., D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone. 2014. NIST Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162.

IEC. 2010. IEC 62443-2-1: 2010, *Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program*. Geneva, Switzerland: International Electrotechnical Commission.

ISA/IEC. 2015. ISA/IEC TR62443-2-3-2015, *Security for Industrial Automation and Control Systems—Part 2-3: Patch Management in the IACS Environment*. Research Triangle Park, NC: International Society of Automation.

IEC. 2023. IEC 62443-2-4: 2023, *Security for industrial automation and control systems—Part 2-4: Security program requirements for IACS service providers*. Geneva, Switzerland: International Electrotechnical Commission.

IEEE. 2018a. IEEE 802.1AR-2018, *IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity*. New York, NY: Institute of Electrical and Electronics Engineers.

IEEE. 2018b. IEEE 802.1Q-2018, *IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks*. New York, NY: Institute of Electrical and Electronics Engineers.

IEEE. 2022. IEEE 802.3-2022, *IEEE Standard for Ethernet*. New York, NY: Institute of Electrical and Electronics Engineers.

Jethanandani, M., S. Agarwal, L. Huang, and D. Blair. 2019. *YANG Data Model for Network Access Control Lists (ACLs)*. RFC 8519. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC8519.

Kaliski, B. 1998. *PKCS #7: Cryptographic Message Syntax Version 1.5*. RFC 2315. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC2315.

Kaliski, B. 2008. *Public-key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2*. RFC 5208. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC5208.

Lear, E., R. Droms, and D. Romascanu. 2019. *Manufacturer Usage Description Specification*. RFC 8520. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC8520.

Microsoft Security Development Lifecycle (SDL)

Mills, D., J. Martin, Ed., J. Burbank, and W. Kasch. 2010. *Network Time Protocol Version 4: Protocol and Algorithms Specification*. RFC 5905. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC5905.

Montgomery, D., M. Carson, T. Winters, M. Newcombe, and T. Carlin. 2020. NIST Special Publication 500-267B, *USGv6 Profile*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.500-267Br1.

NIST. 2019. Common Vulnerability Scoring System (CVSS) v3.1. Gaithersburg, MD: National Institute of Standards and Technology.

Nystrom, M., and B. Kaliski. 2000. *PKCS #10: Certification Request Syntax Specification Version 1.7*. RFC 2986. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC2986.

Pritikin, M., M. Richardson, T. Eckert, M. Behringer, and K. Watsen. 2021. *Bootstrapping Remote Secure Key Infrastructure (BRSKI)*. RFC 8995. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC8995.

Reilly, D., H. Stenn, and D. Sibold. 2019. *Network Time Protocol Best Current Practices*. RFC 8633. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC8633.

Rigney, C., S. Willens, A. Rubens, and W. Simpson. 2000. *Remote Authentication Dial In User Service (RADIUS)*. RFC 2865. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC2865.

Seitz, L., G. Selander, E. Wahlstroem, S. Erdtman, H. Tschofenig. 2022. *Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth)*. RFC 9200. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC9200

Souppaya, M., K. Scarfone, and D. Dodson. 2018. NIST Special Publication 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf.

Stouffer, K., S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn. 2015. Guide to industrial control systems (ICS) security. 800-82r2. NIST. https://doi.org/10.6028/NIST.SP.800-82r2.

Stouffer, K., M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson. 2023. NIST Special Publication 800-82 rev3, *Guide to Operational Technology (OT) Security*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3.

Watsen, K., I. Farrer, and M. Abrahamsson. 2019. *Secure Zero Touch Provisioning (SZTP)*. RFC 8572. Wilmington, DE: Internet Engineering Task Force. https://doi.org/10.17487/RFC8572.