SANS

Analyst Program

## Overview

# Next-Generation Cybersecurity for Buildings

Written by **Dr. Michael Chipley** and **Tim Conway**

October 2021

FORTINET

DRAGOS

# Introduction

Buildings are evolving at a pace that redefines what a building is or can be. Today's buildings do more than provide a comfortable place for people to live, work, or play; they now have become part of a new fabric that integrates people, technology, lifestyle, sustainability, and energy efficiency to enable the occupants and owner to enjoy a safe, secure, sustainable environment.

This paper explores how the rapidly changing "building" concept is being redefined by the following drivers:

- Building growth in square feet and CO2 emissions, constantly evolving building types and use, with new materials and new construction methods expanding the number of targets and the attack surface
- The need for building codes and standards to change to keep up with the technological advances
- The exponential growth of OT[1] and IoT devices used in buildings' control systems and mobile connections, and their evolution into enterprise building management systems (BMSs)[2]
- Tenant-experience software and use of mobile devices as digital keys and identification, exposing the building control systems to new vulnerabilities
- Grid-efficient buildings (GEBs)[3] that communicate in real time with the smart grid[4] and connect the building to other control systems, further expanding the interconnectivity and attack surface
- Energy-as-a-service (EaaS),[5] which enables buildings and electric vehicles to achieve net-zero consumption but rely on third parties to ensure the control systems are cybersecure
- The move to a zero trust architecture, where neither anybody nor anything is trusted

[1] "What is OT Security?" Operational Technology (OT) Security Reviews and Ratings, Gartner Peer Insights, www.gartner.com/reviews/market/operational-technology-security

[2] "Building Management System," Wikipedia, https://en.wikipedia.org/wiki/Building_management_system

[3] "Grid-interactive Efficient Buildings," Office of Energy Efficiency and Renewable Energy, www.energy.gov/eere/buildings/grid-interactive-efficient-buildings

[4] The Smart Grid, www.smartgrid.gov/the_smart_grid/smart_grid.html

[5] "Energy-as-a-Service: A Business Model for Expanding Deployment of Low-Carbon Technologies," Resources for the Future, www.rff.org/publications/issue-briefs/energy-service-business-model-expanding-deployment-low-carbon-technologies/

# Building Growth in Square Feet and CO2 Emissions

As the earth's population continues to grow, the demand for buildings of all types is projected to grow from 2.5 trillion square feet in 2018 to more than 5 trillion square feet by 2060, as shown in Figure 1. Building materials and operations currently account for almost 40% of the global CO2 emissions, as shown in Figure 2. Up until 2016, building control systems have not been designed or constructed to be cybersecure.

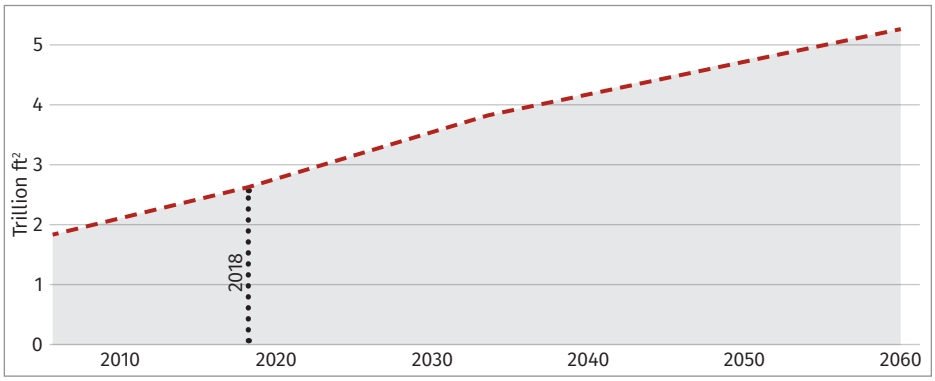


*Figure 1. Global Floor Area Growth*

Property owners, tenants, visitors, and other building users assume the availability of electricity and water at the flick of a switch or the turn of a faucet. The building control systems now connect to the internet, and malicious actors attack building control systems with regular frequency; the number and types of attacks will continue to grow and evolve.

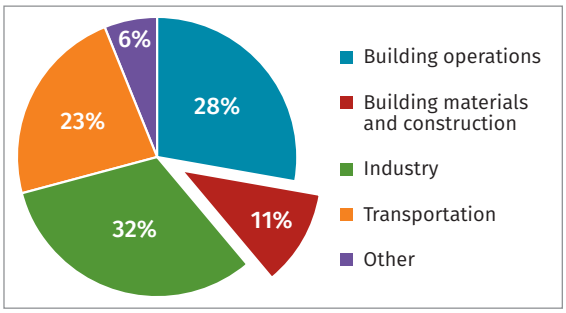


*Figure 2. Global CO2 Emissions by Sector*

The current building stock will undergo renovations to make them smart buildings, and new buildings will utilize technologies to make even smarter buildings, as shown in Figure 3. The buildings will incorporate new artificial intelligence, machine learning, and fault-detection diagnostics combined with IoT devices and components to achieve net-zero emissions[6] and net-zero energy[7] and to comply with water-consumption regulations. The buildings will become GEBs that integrate into the smart grid and can become distributed energy resources (DERs) that use renewables, battery energy storage (BES), electric vehicles (EVs), and wireless to provide sustainable energy to the building and its surrounding community.


*Figure 3. The Smart Building Ecosystem[8]*

[6] "What Does 'Net-Zero Emissions' Mean? 8 Common Questions, Answered," www.wri.org/insights/net-zero-ghg-emissions-questions-answered

[7] "Zero-energy building", https://en.wikipedia.org/wiki/Zero-energy_building

[8] "Securing Smart Buildings: Do You Know the Risks?" www.fortinet.com/securesmartbuildings

### Keeping Up With Urban Growth

**In 2018, the residential and commercial sectors accounted for about 40% (or about 40 quadrillion British thermal units) of total U.S. energy consumption.[9]**

**Embodied carbon is 25% of annual building sector emissions—and growing. Globally, embodied carbon accounts for 11% of annual greenhouse gas (GHG) emissions and 28% of building sector emissions. As operational energy efficiency increases, the impact of embodied carbon emissions in buildings becomes increasingly significant.[10]**

**The world is currently undergoing the largest wave of urban growth in human history. More than half the global population now lives in urban areas, and by 2060, two thirds of the expected population of 10 billion will live in cities.**

**To accommodate this tremendous growth, the global building stock will require an additional 2.48 trillion square feet (230 billion square meters) of new floor area, thus doubling it by 2060 (and the equivalent of adding an entire New York City every month for the next 40 years). This new building stock must meet zero-net-carbon standards.**

**More than half of the global population is now concentrated in urban areas, and by 2060 two thirds of the expected population of 10 billion will live in cities.**

## Building Types

We typically divide buildings into different categories depending on type of use, function, or processes they support.[11,12] See the "Building Types by Category" inset for a list of types. You can find a more extensive list at the Wikipedia link in footnote 12. The type of building, materials used in construction, and the functional use can vary over the life of the building. Most buildings will have a service life of 50 years or more and may undergo several modernizations/retrofits over their lifecycle. The convergence of the traditional IT infrastructure supporting the occupants' business needs (email, HR, professional services, R&D, among others) is being interconnected to the OT infrastructure (HVAC, lighting, physical access control [PACS], among others), and the number of OT/IoT devices will grow exponentially over the next decade. The building users will interact with the IT and OT/IoT systems with their mobile devices and will have expectations of new kinds of services a building will provide (intelligent wayfinding, wireless charging, digital keys, concierge services, to name a few).

The type of building will in turn determine what international, state, and local codes apply for the proper design, construction, and operation of the building. For example, a medical building must have additional life-safety equipment such as enhanced HVAC, infection control, nurse call stations, medical gases, and wayfinding signage, whereas an office building will provide common areas such as lobbies and elevators, dining, retail, security, and parking that interconnect with the tenant space as well as the tenant IT and OT systems such as picture archiving and communication system (PACS) and closed-circuit television (CCTV).

### Building Types by Category

- **Office buildings**
  - **Office towers**
  - **Walk-up**
- **Data centers**
- **Residential buildings**
- **Retail buildings**
  - **Shops/boutiques/services**
  - **Big box**
  - **Malls**
- **Hospitality buildings**
- **Multipurpose buildings**
  - **Multipurpose skyscraper**
  - **Mall/office space**
- **Institutional civic buildings**
- **Gathering buildings**
- **Religious buildings**
- **Educational buildings**
- **Industrial buildings**
- **Agricultural buildings**
- **Terminals (transportation buildings)**
- **Recreational buildings**

[9] www.bing.com/search?form=MOZLBR&pc=MOZD&q=building+power+consumption+us

[10] "Why the Building Sector?" Architecture 2030, https://architecture2030.org/buildings_problem_why/

[11] "13 Types of Buildings and Structure Classifications Used Throughout the World," Home Stratosphere, www.homestratosphere.com/types-of-buildings/

[12] "List of building types," Wikipedia, https://en.wikipedia.org/wiki/List_of_building_types

## Building Codes and Standards

The lifecycle of buildings is complex, governed by a variety of regulatory and organizational voluntary codes and standards. (See the appendix at the end of this paper for a more in-depth review of the codes.) The codes and standards vary dramatically across the globe and dictate many of the performance attributes of the building such as seismic, hurricane/tornado, energy and water consumption, sustainability, and impact on the environment. Codes are mandatory, and a building is designed, constructed, and operated under the regulatory compliance of those codes. Standards are voluntary, and building owners must decide which standards they want to adopt for security, environmental, energy, or risk performance of the building.

**Committees develop and update codes and standards, but typically they do not keep up with the rapid development and adoption of new building technologies. Use of new technologies such as tenant-experience apps, GEBs, and EaaS can create new attack surfaces and vulnerabilities and may also conflict with the codes.**

Many buildings are considered *critical infrastructure* as defined in the Department of Homeland Security National Infrastructure Protection Plan (DHS NIPP).[13] Historically, the buildings' OT systems would typically be isolated and not connected to the internet. As recent ransomware attacks have demonstrated, however, almost every building now has some vulnerability associated with either the IT or OT systems. Often, attacks target both at the same time.

## Building Management Systems Across Numerous Properties

Over the past decade, enterprise BMSs have become the norm. Building owners and facility engineers now have more control and insight into how their buildings are performing across a portfolio, campus, or complex. The days of the facility engineer with the BMS server under his or her desk for each building is rapidly changing. Today, cloud services integrate all the buildings onto one platform. Several things drive these changes:

- Cost-effective cloud services and vendors offering software-as-a-service (SaaS)
- Virtualization technologies
- IoT and mobile devices
- Tenant-experience software
- Artificial intelligence, machine learning, and fault-detection diagnostics

[13] "National Infrastructure Protection Plan," Department of Homeland Security, www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf

## Grid-Interactive Efficient Building Systems (GEBS)

The tremendous developments in smart grid technologies and distributed energy resources (DERs) are now being applied to the building stock. Photovoltaic panels on the roof and envelopes, large-scale BES, and wind and geothermal panels can transform a building that consumes a significant amount of resources (electric, water, natural gas) into a net-zero consumer and emissions emitter. Figure 4 illustrates the GEBS principles.

The *Roadmap* finds that over the next two decades, GEBs could deliver between $100 and $200 billion in savings to the U.S. power system and cut CO2 emissions by 80 million tons per year by 2030, or 6% of total power sector CO2 emissions.[15] That reduction equals more than the annual emissions of 50 medium-sized coal plants or 17 million cars.

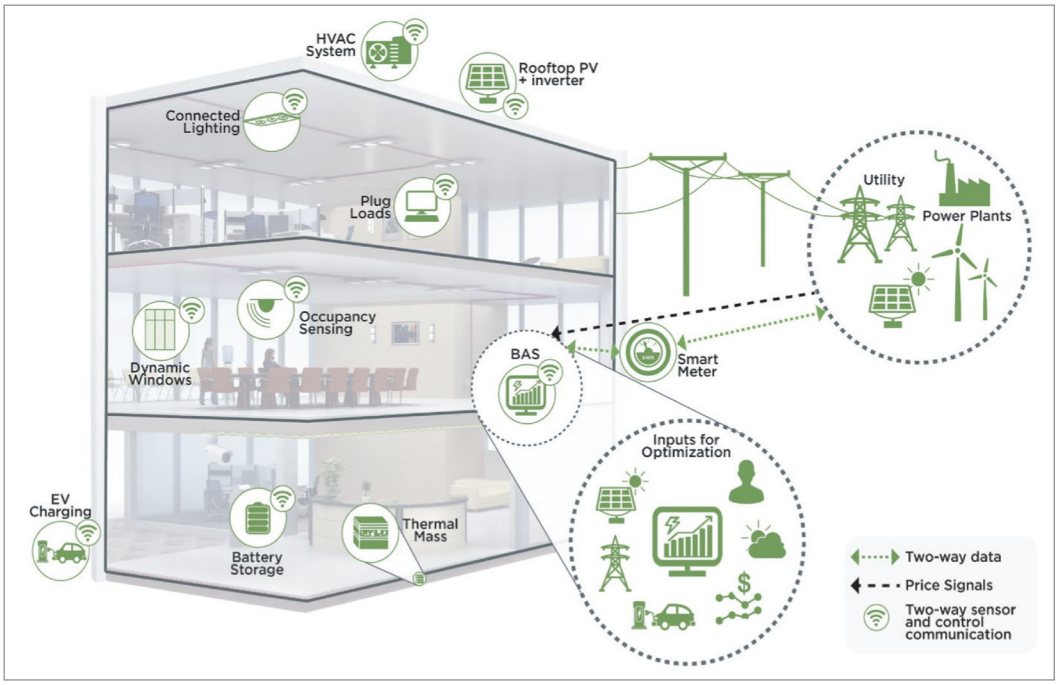


*Figure 4. Department of Energy Example of Grid-Interactive Efficient Commercial Building*[14]

## Energy-as-a-Service (EaaS)

Because the smart grid is now supplanting the traditional methodology of producing, distributing, and providing electrical power to the endpoint customer, a new business model is emerging: energy-as-a-service. In EaaS, the customer transfers ownership of the on-site equipment (power lines, transformers, switch gear, meters) to a third-party provider. Service providers are modifying prior financing models such as pay-for-performance contracts, power purchase agreements, energy-savings performance contracts, and utility energy-savings contracts to allow the service provider to retain ownership while the customer pays for the service. The Deloitte Energy-as-a-Service Report illustrates the changes in the existing grid into the smart grid and EaaS, as shown in Figures 5 and 6 (seen on the next page).[16]

[14] "Grid-interactive Efficient Buildings," U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, https://betterbuildingssolutioncenter.energy.gov/sites/default/files/attachments/bto-geb-factsheet-41119.pdf

[15] "DOE's National Roadmap for Grid-interactive Efficient Buildings," Office of Energy Efficiency and Renewable Energy, www.energy.gov/eere/articles/does-national-roadmap-grid-interactive-efficient-buildings

[16] "Energy-as-a-Service," Deloitte, www2.deloitte.com/uk/en/pages/energy-and-resources/articles/energy-as-a-service.html

As the EaaS business model expands, it is not clear who will provide the cybersecurity of the EaaS equipment and service. Traditional regional transmission offices (RTOs) and system owners that fell under the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) regulations will now need to have multiple interconnections across a distributed environment with billions of endpoint devices that expand the attack surface but are not under their control.

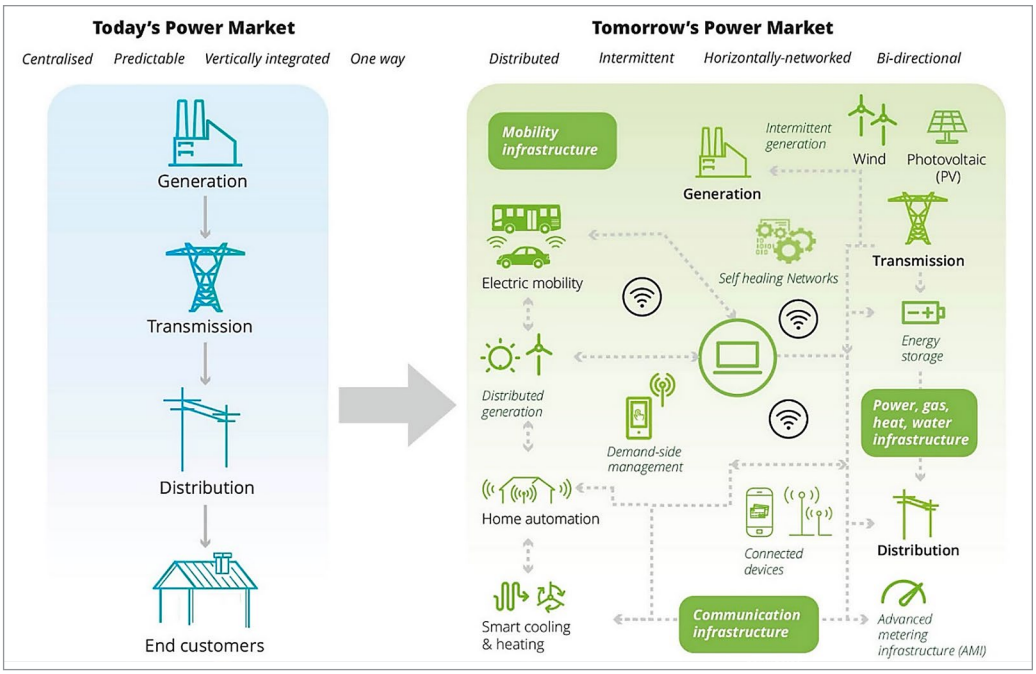


*Figure 5. Buildings Become the Center Point per Deloitte EaaS Report* Changes in the Power Market

## Building OT Control Systems

A building is a collection of many IT and OT systems that collectively perform specific functions for the occupants. Building OT[17] control systems are physical-equipment–oriented technologies and systems that control plants and equipment. They include devices that meet technical constraints and ensure physical system integrity, are event driven, and frequently utilize real-time software applications or devices with embedded software. These specialized systems are pervasive throughout buildings and are required to meet numerous safety, performance, security, reliability, and operational requirements.

Common OT control systems within buildings include:

- HVAC
- Lighting
- Fire and life safety
- Mass notification
- Vertical and horizontal transport
- Cranes and lifts
- Electronic security systems
- Parking
- Digital signage
- Weather
- Shade and daylighting
- Elevators
- Physical access control
- CCTVs and other IoT

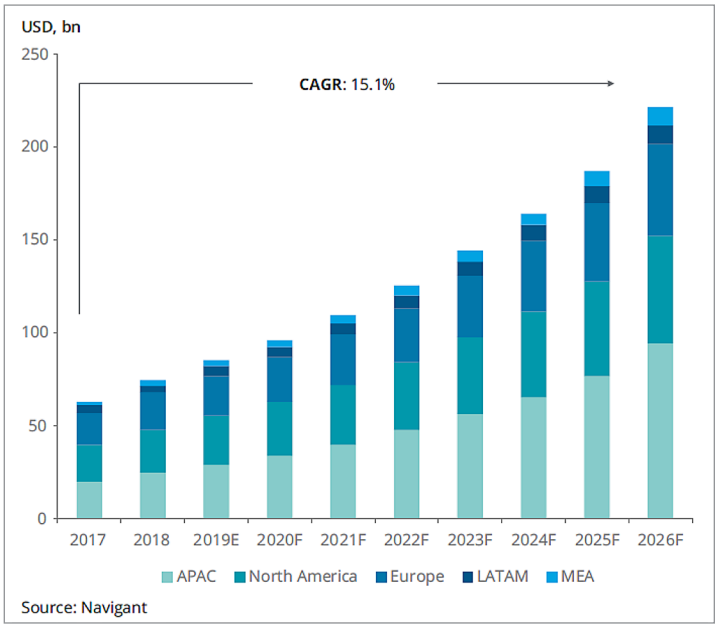


*Figure 6. Global, Commercial, and Industrial EaaS Market by Value per Deloitte EaaS Report*

[17] *Building OT* is capitalized throughout this paper for the sake of clarity in distinguishing it as a noun rather than a verb.

Figure 7 illustrates a Johnson Control System METASYS BMS that the facility engineer uses to manage the various OT control systems within the building. The IT front-end servers, workstations, firewalls, and switches perform IT functions but in a different manner.

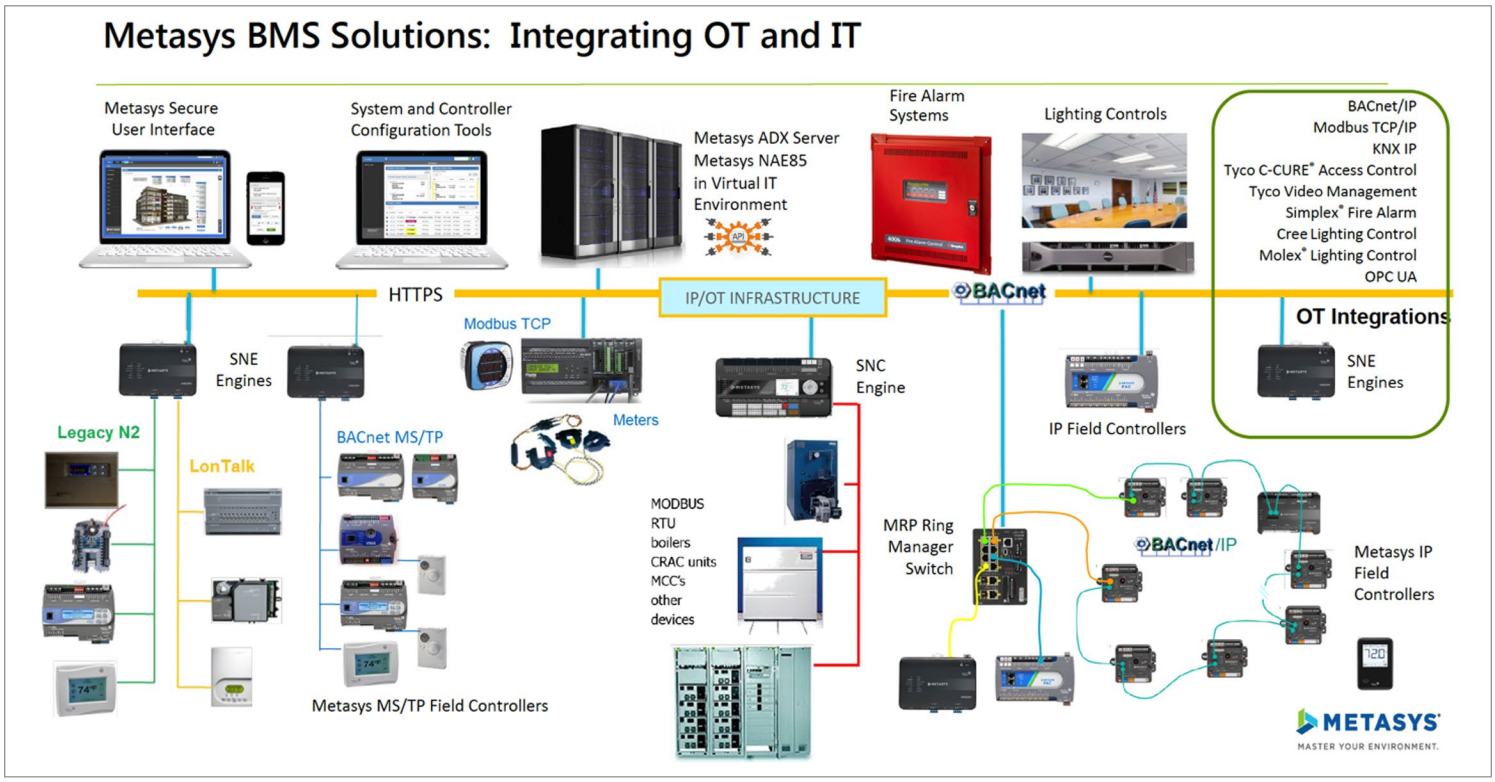


*Figure 7. Johnson Control Systems Metasys BMS*

Building OT control systems differ significantly from traditional information systems (administrative, mission support, and scientific data processing information systems) in that they use specialized software, hardware, and protocols. Building OT control systems are often integrated with mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities. The "front end" portions of Building OT control systems resemble traditional information systems in that they use the same commercially available hardware and software components. While most Building OT control systems do not resemble a traditional IS, the integration of their OT control systems' "front end" with IS introduces some of the same vulnerabilities that exist in current networked information systems.

**Developers should delay Building OT control systems updates until the completion of a thorough analysis of deployment impact.**

Building OT control systems typically use human machine interfaces (HMIs) to monitor processes as opposed to the GUIs used for IS. Many current Building OT control systems and subsystems are now a combination of OT and IT. In Figures 8 through 10 (seen on the next page), the pictures show the HVAC HMI/GUI at the building engineering operator's console, an advanced electric meter, and a building controller.

Building OT control systems typically have long life spans (in excess of 20 years), and installed systems that are no longer supported by the vendor are common. The combination of these factors introduces two issues. First, depending on the relative age and isolation of the system, there may not be a patch or upgrade path for components of the system. Second, attempts to patch the component or employ modern scanning methods might disrupt the system. Building OT control systems have experienced complete system shutdown when an intrusion detection system (IDS) or host-based scanning system (HBSS) scan is performed on an otherwise operational Building OT control system. Thus, developers should delay Building OT control systems updates until the completion of a thorough analysis of deployment impact. This added effort will require planning, notification of parties involved, probable extended security update timelines, and flexibility in security control compliance measurement and enforcement.

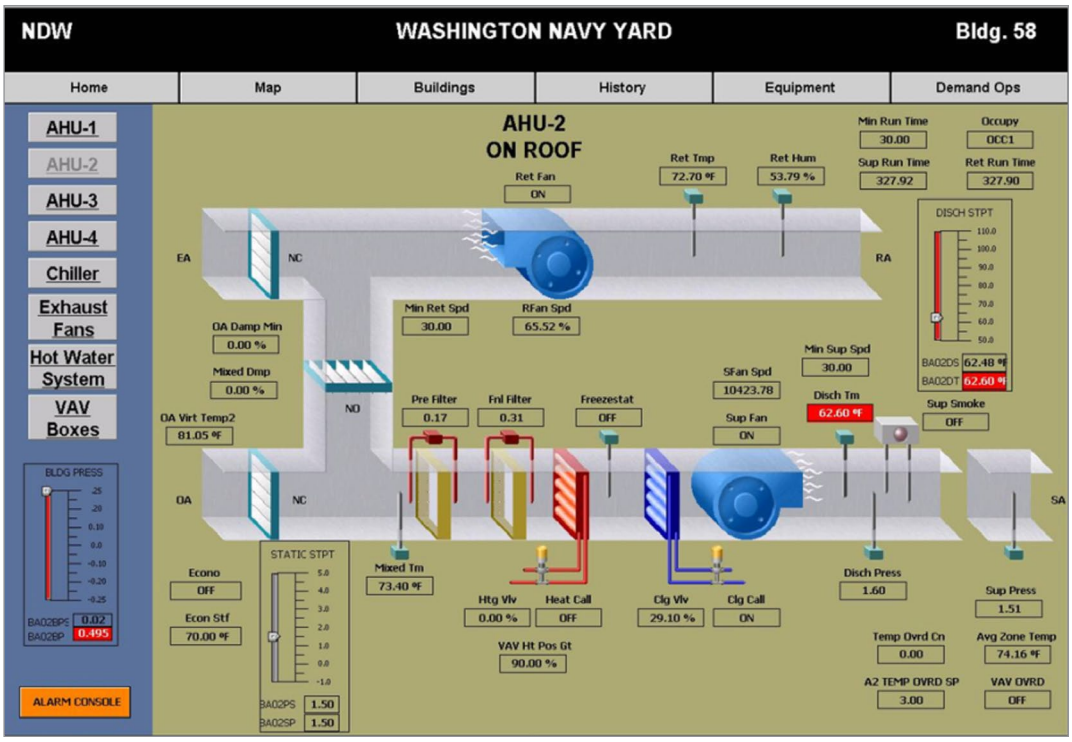


*Figure 8. Building HVAC Human Machine Interfaces*


*Figure 9. Advanced Smart Meter*


*Figure 10. Level 2 Controller*

### Building Control Systems NIST SP 800-53 Security Controls Implementation

**While we can apply many traditional IT baseline security controls such as NIST SP 800-53 to a Building OT control system, how and where to implement them varies, primarily because of technical and operational constraints. Interconnections between Building OT control systems and organizational networks and business systems expose Building OT control systems to exploits and vulnerabilities. Any attempts to address these exploits and vulnerabilities must consider the constraints and requirements of the Building OT control systems.**

## OT and IoT Devices and Components Growth

The exponential growth in OT and IoT devices and components is radically changing how we design, construct, operate, renovate, and decommission buildings. Buildings increasingly incorporate devices and components as part of the Building OT control systems, and the tenants and visitors interact with the Building OT via their mobile devices:

- IoT devices and sensors will grow from 7.6 billion to 24.1 billion.[18]
- Bluetooth device networks are projected to grow to 360 million annual shipments, while phone, tablet, and PC device shipments will grow to 2.1 billion annual shipments in 2023.[19]
- ZigBee home automation global market was valued at US$ 1,298.7 million in 2020 and is expected to surpass US$ 3,846.4 million by 2028, registering a CAGR (compound annual growth rate) of 15.2% during the forecast period (2021–2028).[20]

An IoT device is typically defined as internet-enabled and able to interact with other devices. The use of IoT enables the smart building to become an interactive experience with the tenant/visitor and dramatically reduces the energy and water consumption, enhances the environmental health (air and light), provides wireless location and electrical charging, and reduces the operating costs of the building.

Software Testing Help published the following list of the top 18 IoT devices examples In 2021.[21] It includes a remarkably wide variety of devices:

1. Google Home Voice Controller
2. Amazon Echo Plus Voice Controller
3. Amazon Dash Button
4. August Doorbell Cam
5. August Smart Lock
6. Kuri Mobile Robot
7. Belkin WeMo Smart Light Switch
8. Foobot Air Quality Monitor
9. Flow by Plume Labs Air Pollution Monitor
10. Nest Smoke Alarm
11. Nest T3021US Learning Thermostat Easy Temperature Control
12. Philips Hue Bulbs and Lighting System
13. Bitdefender BOX IoT Security Solution
14. Ring Doorbell
15. WeMo Insight Smart Plug
16. Logitech Harmony Universal Remote
17. Particle Photon Wi-Fi with Headers
18. NETGEAR Orbi Ultra-Performance Whole Home Mesh Wi-Fi System

The IoT devices and sensors interface and connect with physical security, fire, temperature, environmental, and network OT systems for residential buildings and are primarily for lifestyle and ease of use. Typically, these IoT devices and sensors have little to no instructions or best practices to cybersecure them; instead, the user is responsible for provisioning and implementing them in a secure manner.

---

[18] "Infographic: Real World Lessons in the Internet of Things," Transforma Insights, https://transformainsights.com/blog/real-world-iot

[19] "2019 Bluetooth Market Update," Bluetooth, www.bluetooth.com/bluetooth-resources/2019-bluetooth-market-update/

[20] "ZigBee Home Automation Market to Reach US$ 3846.4 Million by 2028," Coherent Market Insights, www.coherentmarketinsights.com/press-release/zigbee-home-automation-market-3723

[21] "18 Most Popular IoT Devices in 2021 (Only Noteworthy IoT Products)," Software Testing Help, www.softwaretestinghelp.com/iot-devices/

The Continental Automated Buildings Association lists the following top IoT devices and sensors for building owners:[22]

1. Occupancy management for the workplace
2. Environmental monitoring
3. Energy management

Note the IoT devices and sensors for commercial buildings focus on the health of the building, with a major emphasis on energy. Typically a control systems vendor provisions these IoT devices and sensors, and qualified facility engineers and technicians manage/monitor them. The cybersecurity of the HVAC, lighting, fire, and other systems is becoming much more secure as the systems become part of the larger enterprise BMS and are monitored by a facility security operations center (FSOC).

The Navy smart grid and the facility energy operations centers (FEOCs) are an example of how a portfolio of campus buildings connected to multiple other campuses in the region and the local community lifelines (utilities, road, rail, pipeline, telecom, police, fire, and emergency services) can now provide the next generation of cybersecurity insights and protection, as shown in Figure 11.

### The Future of FSOCs

**Currently, very few buildings connect to an FSOC to provide continuous monitoring or threat intelligence, or to react to a cyber intrusion/incident. Whether private sector or government, FSOCs will begin to emerge that can manage and protect a portfolio of assets to include the buildings, DERs, EVs, and tenant systems.**

**The next-generation smart building will also become the next-generation cybersecure building. By using the internet to achieve the integration needed to provide the tenant/visitor services, the current operations, maintenance, and cyber protection will need to evolve to an automated capability to react to cyber threats and attacks.**

**The next-generation cybersecure building will include technology, such as the Dragos Platform, to provide broad visibility of the assets and protocols, automated asset inventory synchronization, and threat detection using behavior analytics. Behavior analytics are based on characterizations of adversary tactics, techniques, and procedures (TTPs) that rapidly pinpoint malicious behavior, provide context-rich alerts and notifications, and are tied with investigation playbooks to help analysts respond to threats efficiently. Solutions that rely solely on anomaly-based threat detection methods are troubled with too many false positives, and the notifications often lack the context needed for a swift response.**

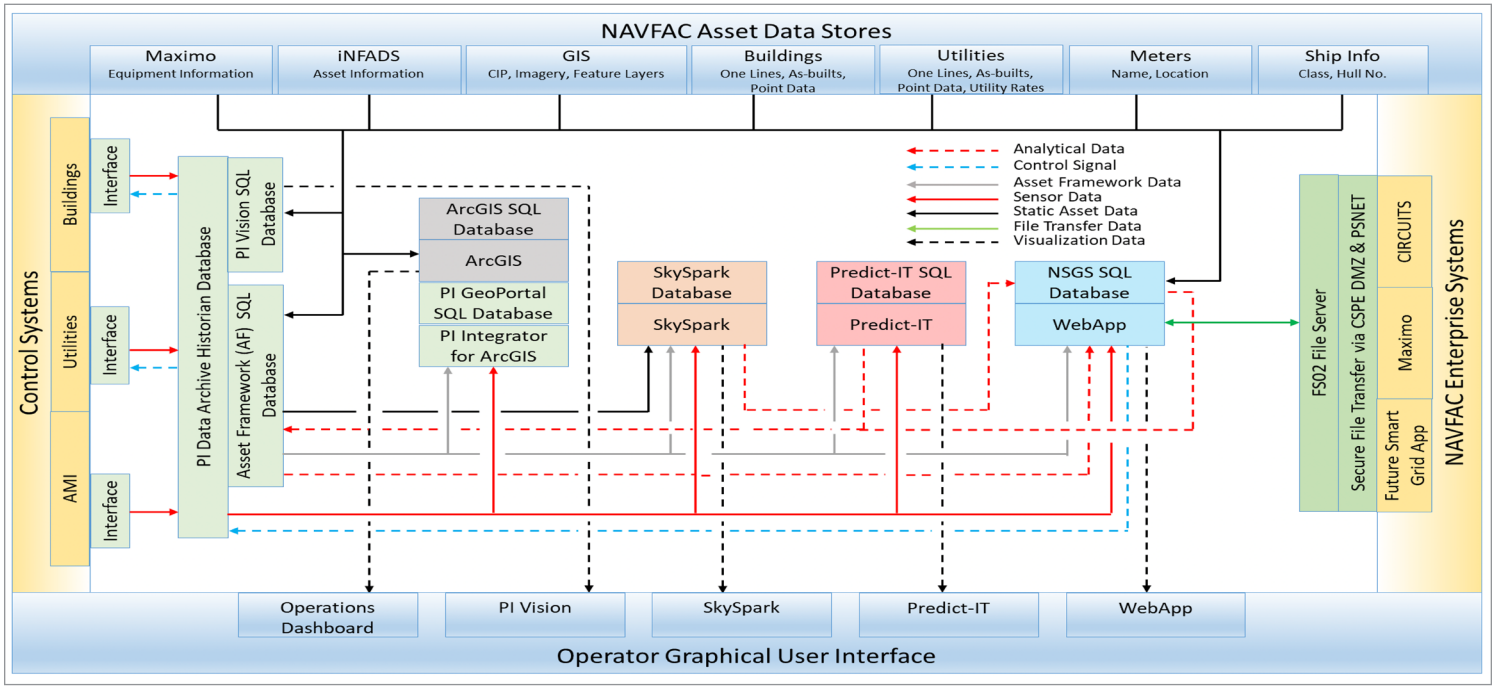


*Figure 11. Navy Smart Grid and Facility Energy Operations Center*[23]

[22] "Top IoT Sensors for Building Owners," Continental Automated Buildings Association (CABA), www.caba.org/top-iot-sensors/

[23] "T09-S03 Cybersecurity Executed: Case Study," Whole Building Design Guide, www.wbdg.org/continuing-education/energy-exchange/fempee19t9s3

The 2020 Schneider Electric – Science Center White Paper 500 Version 18 provides an example of next-generation BMS functionality and capability, as shown in Figures 12 and 13.[24] In that paper, the next-generation BMS has three key architecture attributes:

- Based on an open, integration platform
- Leverages cloud computing for analytics and AI-driven digital services
- Designed for mobility

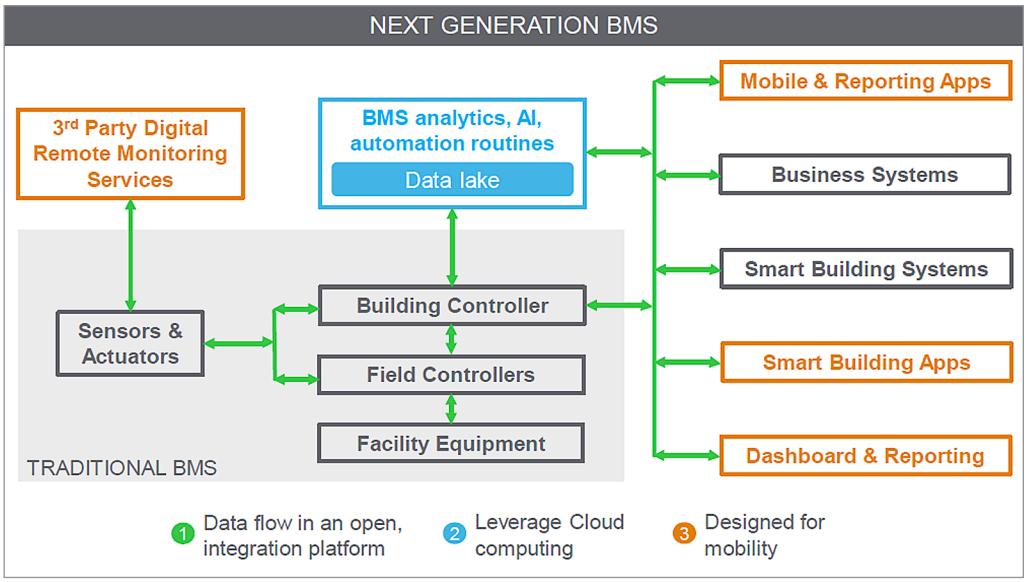


*Figure 12. Schneider Next-Generation BMS Functionality*

The next-generation BMS will be one system within an FSOC. The BMS will integrate and interface with numerous other Building OT systems such as HVAC, lighting, fire alarm, mass notification, electronic security, conveyance, meters, digital wayfinding systems, and the building IT systems used for utility meter consumption data, fault-detection data analytics, GIS/BIM/CMMS (geographic information system, building information modeling, computerized maintenance management systems) platforms, billing and payment systems, physical security, and emergency management.

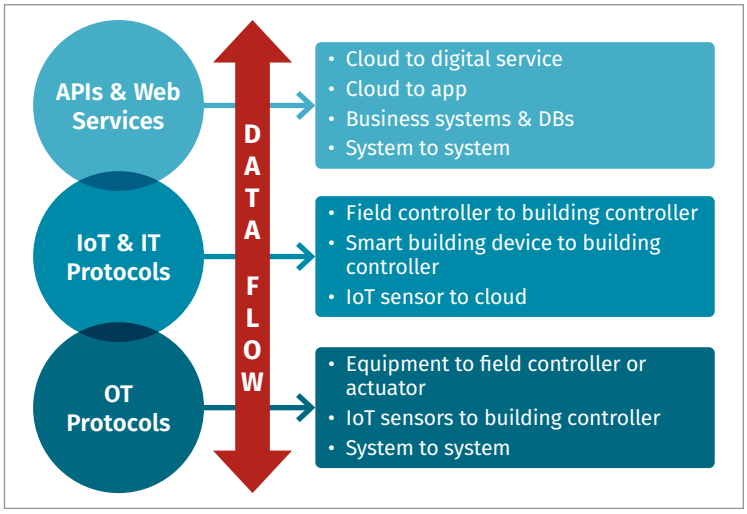


*Figure 13. Schneider Next-Generation BMS Data Flow, APIs, Web Services, and Protocols*

## The Tenant Experience

One of the faster growing segments of software growth for buildings is the tenant experience. The objective of the tenant experience is to provide the tenant and visitors the capability to interact with the Building OT control systems and other retail or concierge services via their mobile device over the internet. The software uses cloud services and the mobile device to provide services such as:

- Lobby reception visitor registration/management
- Wireless access point for internet access
- Wireless charging of mobile devices
- Digital keys touchless building and parking entry and departure, elevator call
- Assigned workspace workstation/phone/temperature/lighting management
- Conference room reservations
- In-building café and restaurant reservations
- Food delivery to assigned workspace

[24] "3 Essential Elements of Next Generation Building Management Systems," Smart Buildings Technology, www.smartbuildingstech.com/white-papers/whitepaper/21165234/schneider-electric-north-america-3-essential-elements-of-next-generation-building-management-systems

- Package delivery to assigned workspace
- Dry cleaning delivery to assigned workspace
- Fitness center schedules
- Internal location for emergency response and evacuation
- Property management contact and help desk information to report problems

Figure 14 shows an example of the tenant experience with the Capgemini platform.

The challenge of implementing tenant-experience software is the propagation of the attack surface, as shown in Figure 15. The current architectures that rely on defense in depth, network segmentation, antivirus/malware (AV/MW) protection, and continuous monitoring with SIEM and other tools traditionally rely on certificates and trusted connections.

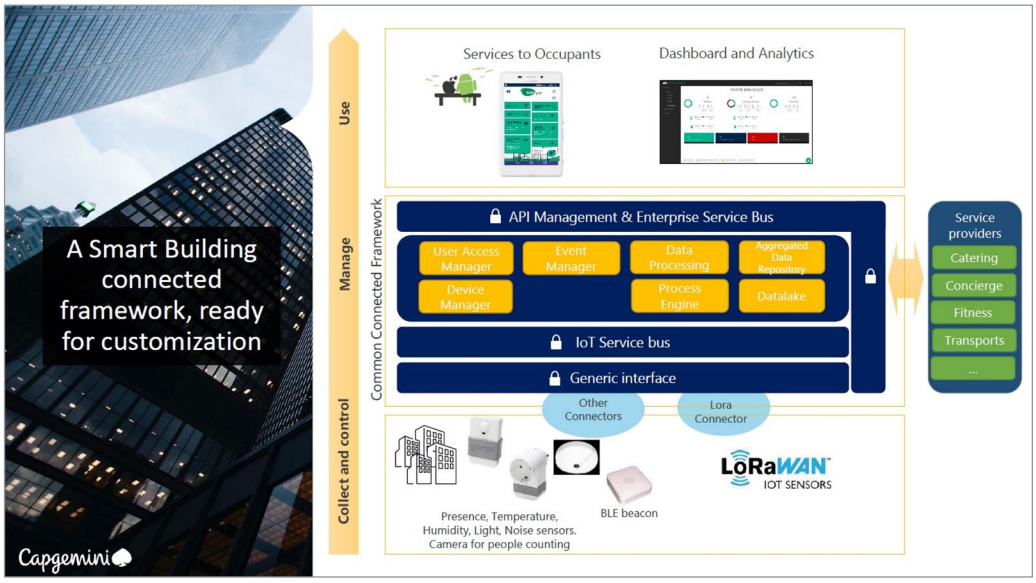


*Figure 14. Example of Tenant-Experience Software Integration to Make a Smart Building Smarter*[25]

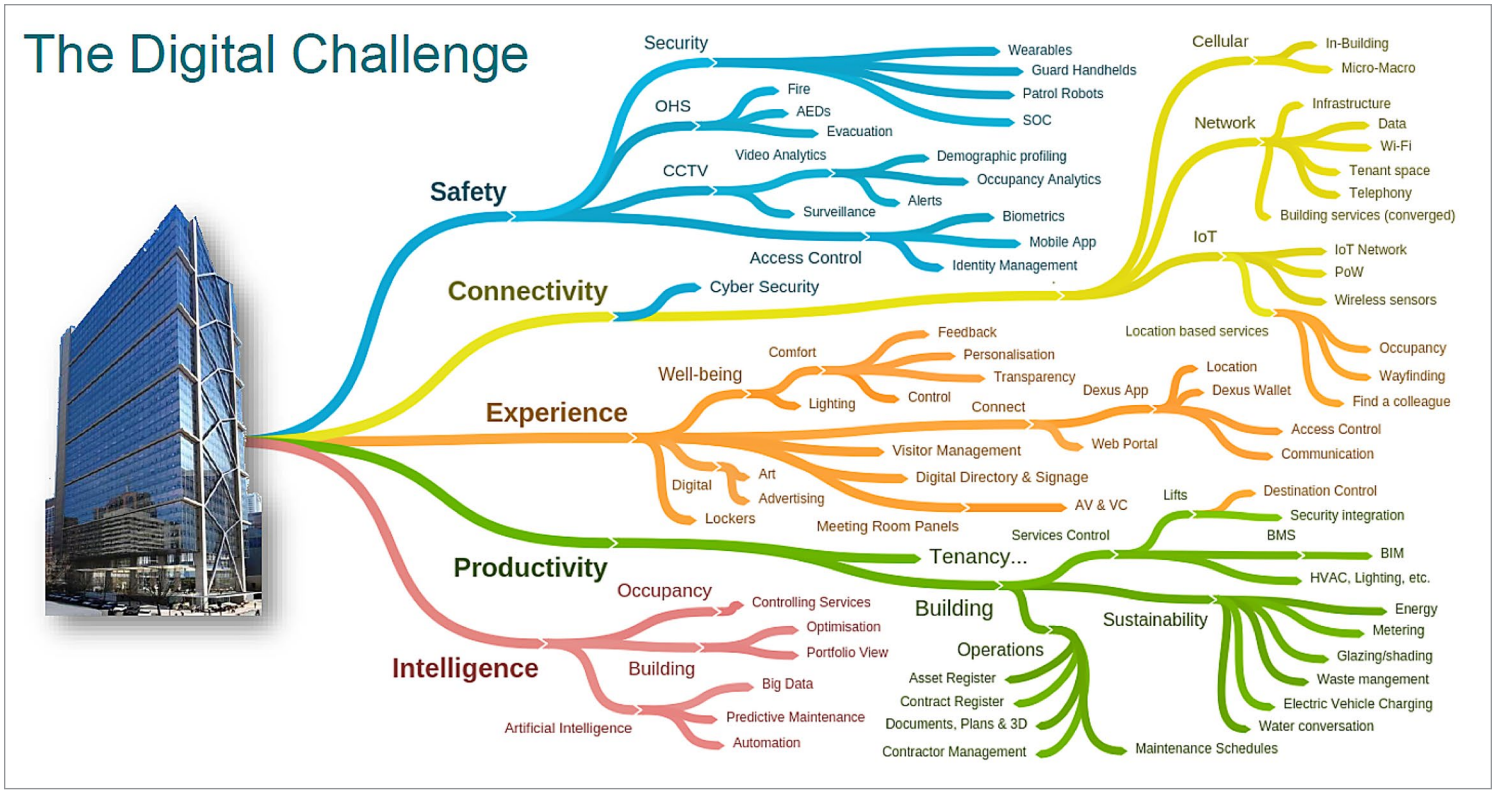


*Figure 15. Example of the Proliferation of the Attack Surface When Using Tenant-Experience Platforms*[26]

[25] Image made available through open source, www.realcomm.com/news/868/1/tenant-experience-applications-the-hot-topic-for-2018

[26] Image made available through open source presentation deck, www.realcomm.com/news/868/1/tenant-experience-applications-the-hot-topic-for-2018

## Building Control Systems Communication Protocols and Ports

Building OT control systems commonly use several protocols and ports to allow the devices and components within the layers to communicate both horizontally and vertically across the reference architecture.

### Internet Protocols (Levels 5, 4, and 3)

- IPv4 and IPv6
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Hypertext Transfer Protocol (HTTP) – Port 80
- Hypertext Transfer Protocol Secure (HTTPS) – Port 443

### Open Control Systems Protocols (Levels 3, 2)

- Modbus: Client/Server[27] – Port 502
- BACnet: Peer to Peer – Port 47808
- LonWorks/LonTalk: Peer to Peer – Port 1628/29
- DNP3: Parent/Child – Port 20000
- IEEE 802.x – Peer to Peer
- ZigBee – Peer to Peer
- Bluetooth – Master/Slave

**Building OT systems control protocols have a few major vulnerabilities: They were not developed with any security features, they communicate in clear text (not encrypted), and they do not require authentication. A controller performs an issued command but does not know whether the command comes from a trusted source or even if the command is valid.**

**The BACnet Secure Connect Interoperability Acceleration Program (BACnet/SC) is an addendum to the BACnet protocol recently released by the ASHRAE BACnet Committee. It is a secure, encrypted datalink layer that is specifically designed to meet the requirements, policies, and constraints of minimally managed to professionally managed IP infrastructures.**
**The need for using standardized and often already present IP network infrastructures for BACnet communication is increasing, and this security is a critical piece in the networking of building technologies (building internet of things – BIoT).[28]**

### Examples of Proprietary Control Systems Protocols

- Tridium NiagraAX/Fox
- Johnson Metasys
- OSISoft Pi System

To illustrate the vulnerability of the protocols and ports used in Building OT control systems, the next section explores the footprinting and reconnaissance of Building OT control systems.

[27] The Modbus Organization (https://modbus.org/) Board of Trustees has announced its intent to expunge all occurrences of inappropriate language of the query and response paradigm of Modbus communications. As a result, all instances of "master-slave" in the organization's literature and on its website will be removed. The client-server principle is a model for a communication protocol in which one device (the client) controls one or more other devices (the servers). In a standard Modbus network, there is 1 client and up to 31 servers.

[28] BACnet Secure Connect Interoperability Acceleration Program, BACnet, www.bacnetinternational.org/page/secureconnect

# The Attack Surface Grows: Building Systems on the Internet

In early 2009, as Shodan and other IP device search engines began to collect and categorize metadata associated with an IP device that was publicly internet-accessible, building control systems, devices, and components began to appear. In 2010 when the Department of Defense (DoD) first began to understand the depth of the problem, there were more than 20,000 BACnet Building OT control systems on Shodan. As of July 2021, there are still more than 2,500 Level 4 misconfigured Tridium systems and more than 350 Level 2 Distech controllers with direct internet connections. Figures 16 through 20 are Shodan screenshots of exposed Tridium BMS and Distech controllers.

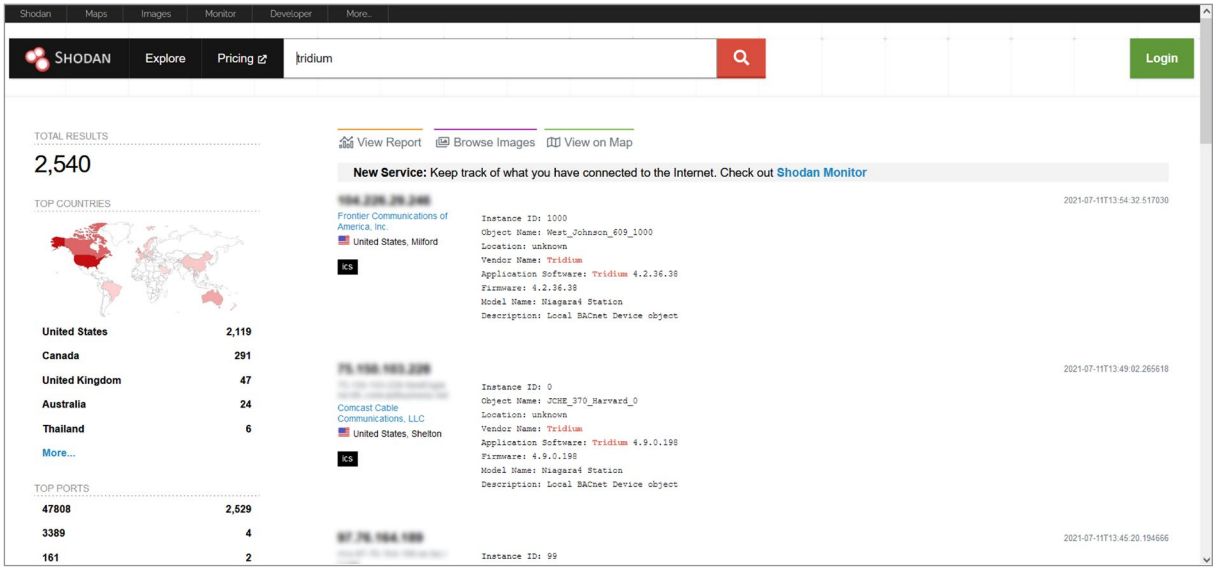


*Figure 16. Tridium Systems Exposed on Shodan*

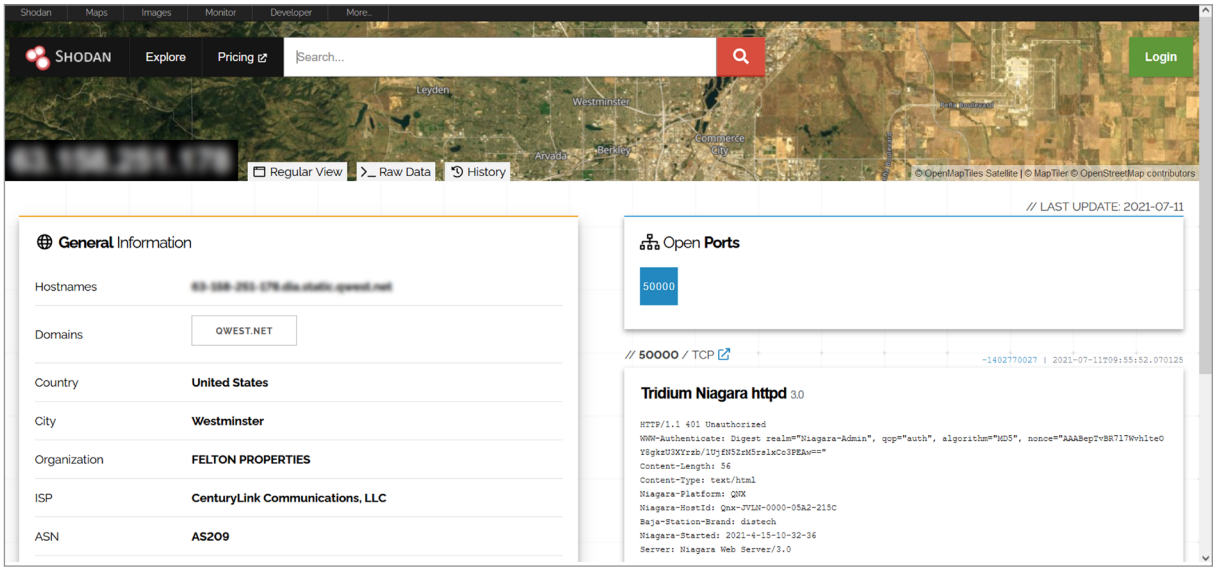


*Figure 17. Shodan Meta Data for Tridium Niagara System Exposed on Shodan*

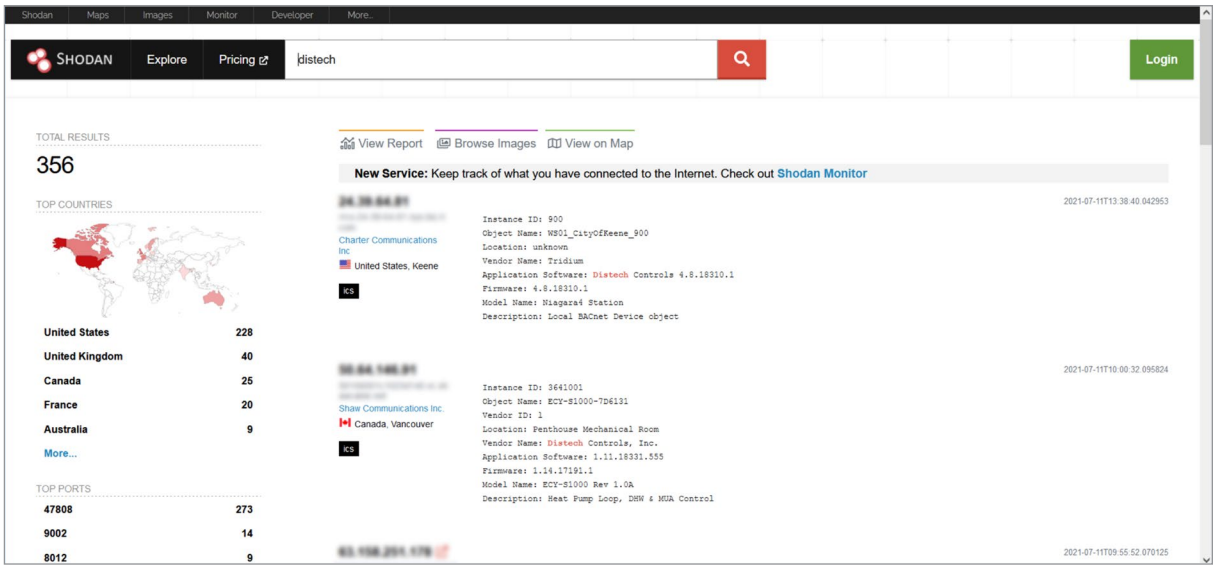


*Figure 18. Distech Controllers Exposed on Shodan and Connected to Tridium Systems*

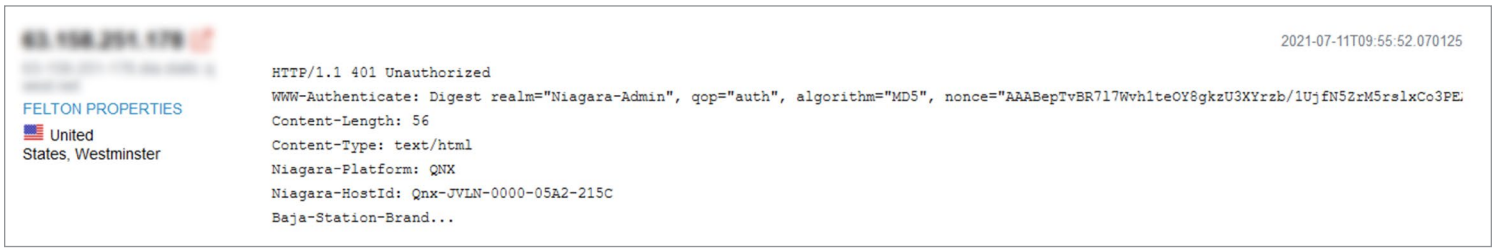


*Figure 19. Distech Controller Connected to Tridium Niagara with Hash and Nonce*

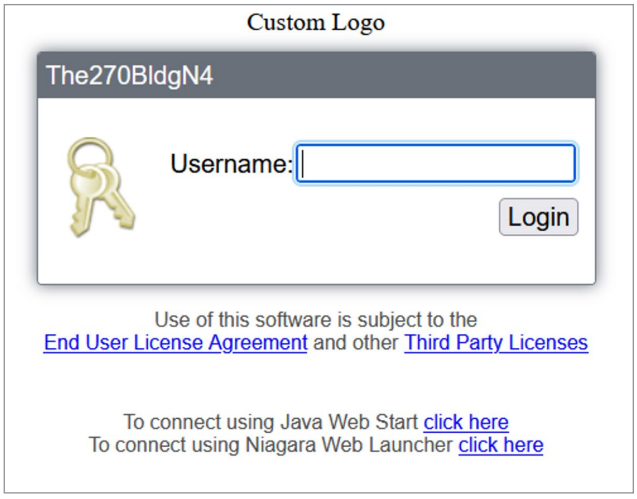


*Figure 20. Johnson Control Systems Facility Explorer Login from Shodan Distech Link*

## Building Control Systems Reference Architecture

The Department of Defense Unified Facility Criteria (UFC) 04-10-06 Cybersecurity of Facility-Related Control Systems has a general Control System Reference Architecture that any organization can use as a model for Building OT controls system, as shown in Figure 21.[29] The control systems are represented as a five-level architecture (based on the Purdue model and ISA 99[30]), where each level represents a collection of components that are logically grouped together by function and generally share a cybersecurity approach. (See the inset titled "Five-level Architecture Overview.") This architecture is defined as a general architecture suitable for a wide range of control systems, and thus we have two key considerations when using it to describe a specific control system:

- Not every implementation of a control system will make use of every level or every type of component shown at a level.
- The same device may reside in different levels, depending on its configuration. For example, some controllers may support different networks based on onboard switches, and thus the same device could reside in either Level 1 or Level 2.

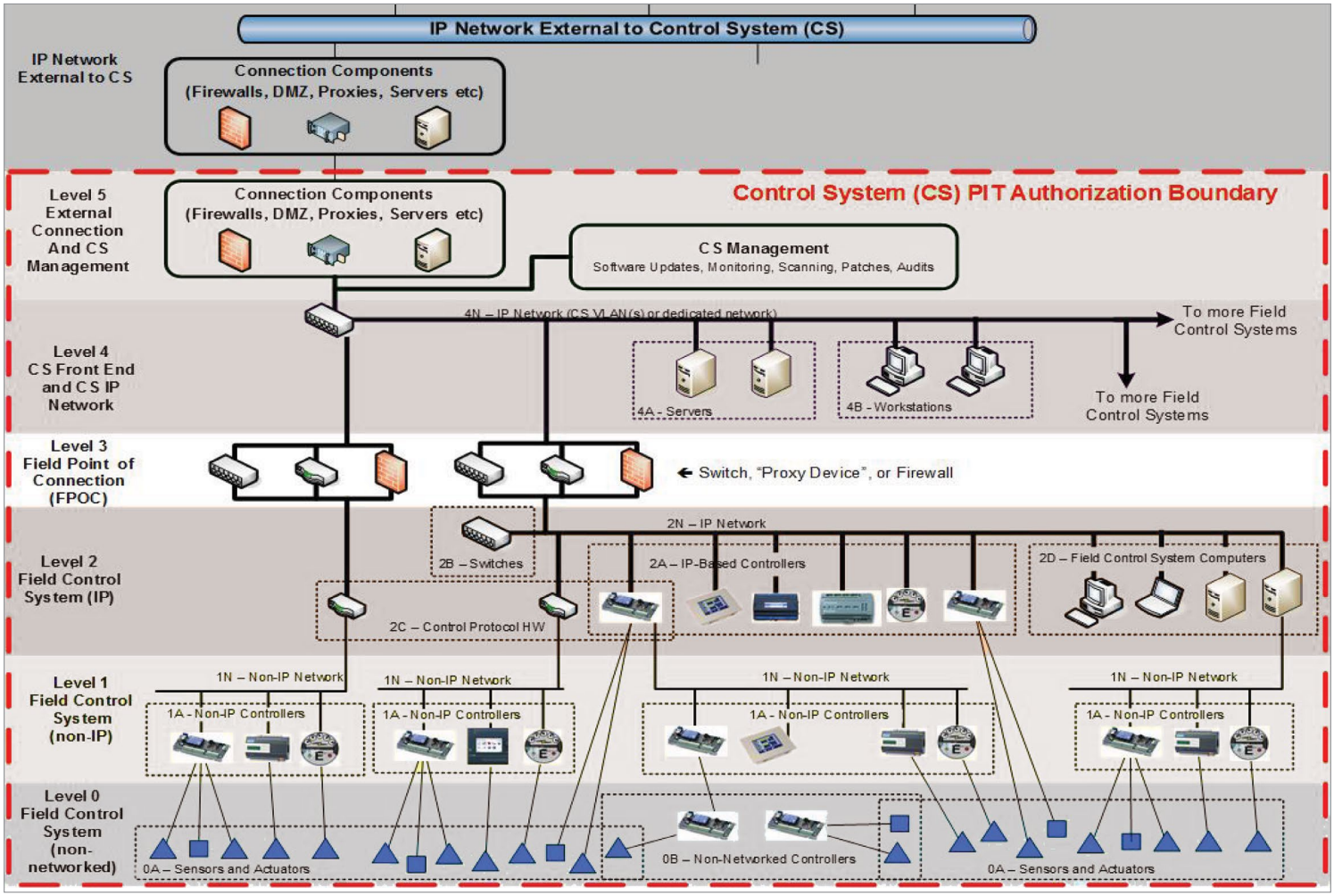


*Figure 21. DoD Five-Level Control System Reference Architecture*

[29] "UFC 4-010-06 Cybersecurity of Facility-Related Control Systems, With Change 1," Whole Building Design Guide, www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

[30] "ISA99, Industrial Automation and Control Systems Security," International Society of Automation, www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

In many cases, a device will fit multiple sublevels within the same principal level, usually within Level 2. For example, a Level 2A controller may act as a Level 2C router to a Level 1 network beneath it.

The reference architecture is used to define the authorization boundary for Building OT control systems and is a logical representation of its network. The actual physical system can span many miles. For example, high-rise commercial offices and campus systems can have many noncontiguous components.

Figures 22 through 36 show the five levels and typical components and devices.

### Five-Level Architecture Overview

**A brief description of each level (from simple to complex devices) of the five-level architecture follows:**

- **Level 5.** Interfaces to "external" networks (IP networks other than the control system network)
- **Level 4.** The site-wide IP network used for the control system, along with front-end servers and workstations (desktops and laptops)
- **Level 3.** The field point of connection (FPOC), which is a connection between the field control system IP network at Level 2 and the Level 4 IP network
- **Level 2.** Networked controllers on an IP network
- **Level 1.** Networked controllers not on an IP network (BACnet MS/TP, RS-485 [DNP, Modbus], LonWorks TP/FT-10)
- **Level 0.** Non-networked devices that communicate using analog signals. These include ("dumb") sensors and actuators as well as non-networked controllers (including their dedicated sensors and actuators). These communicate with Level 1 via hardware I/O (analog and binary signals).

**Note that some levels contain sublevels, as indicated in Figure 21 on the previous page.**

## Level 5: "External" Connection and CS Management

*Figure 22. Level 5 Demarcation Point or Main Point of Presence Where the External IS Meets the Internal Building OT Interface*

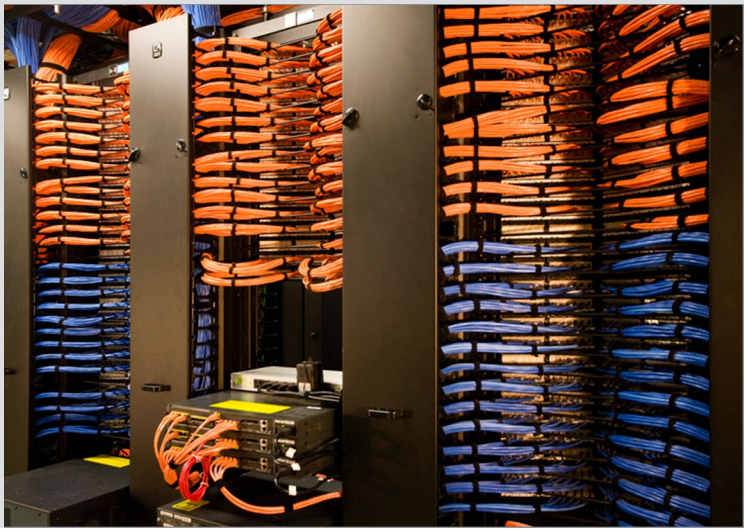

*Figure 23. Level 5 Racks and Servers Located in a Facility Operations Center/Security Operations Center/Energy Operations Center*

## Level 4: CS Front End and IP Network

*Figure 24. Level 4 Rack and Servers Located in an Energy Operations Center or Facility Operations Center*

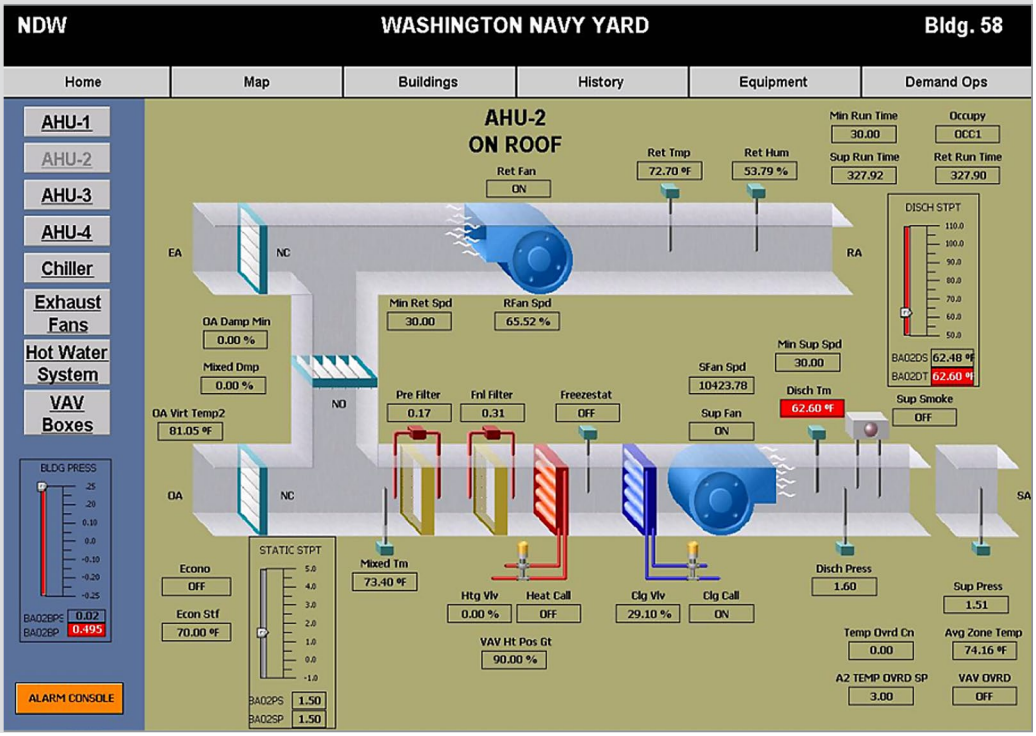


*Figure 25. Workstation or Wall Display of HMI for the Building OT*

**Until recently, most building control systems were very simple flat networks and minimal computers, usually in the building engineer's office under the desk. Building OT systems are now quite complex, with an ever-increasing number of IoT devices and components. Protection of Building OT systems now require a new generation of cyber technologies. Facilities engineers and technicians represent the front line of defense and need advanced cyber hunt and defend skills.**

## Level 3: Field Points of Connection (FPOCs)


*Figure 26. **3-FS:** Level 3 FPOC gateway (application layer proxy). The Level 4 network is Modbus over IP over 10/100Mbps Ethernet. The Level 1 network is proprietary over proprietary 2-wire media. Note this is the same device as in 2C-FS.*


*Figure 27. **3-LIP:** Level 3 FPOC Router Between Three LonTalk Networks: Level 1 Lon over TP/FT-10, Level 1 Lon over TP/FT-10, and Level 4 Lon over IP over Ethernet*

## Level 2: IP Portion of the Field Control System

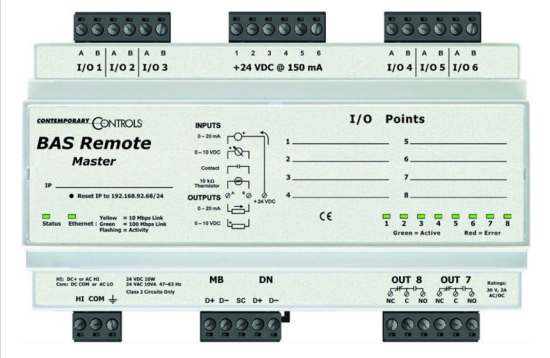


*Figure 28. **2A-CC:** Very basic Level 2A controller capable of monitoring six analog inputs and reporting their values to the network and setting two outputs. The network is BACnet over IP over 10/100Mbps.*


*Figure 29. **2A-JACE:** Programmable Level 2A controller. No analog inputs or outputs. The primary networking is proprietary over IP over 10/100Mbps Ethernet. For a small field control system, this might be the Level 3 FPOC.*


*Figure 30. **2C-FS:** A Level 2C gateway (application layer proxy). The Level 2 network is Modbus over IP over 10/100Mbps Ethernet. The Level 1 network is proprietary over proprietary 2-wire media.*

## Level 1: Non-IP Portion of the Field Control System


*Figure 31. **1A-VAV:** Variable air volume (VAV) box controller with multiple analog inputs and outputs. Also incorporates dedicated actuator and pressure sensor (normally Level 0 devices). The network is LonTalk over TP/FT-10 media at 78Kbps.*

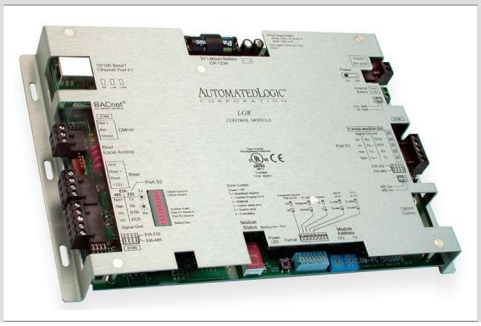


*Figure 32. **1A-LGR:** Programmable controller with no analog inputs or outputs. The primary network is BACnet over Ethernet (not IP) media at 10/100Mbps. Also supports BACnet over MS/TP media and proprietary protocol over RS-485 media. Can also be in Level 2.*


*Figure 33. **1N-Lswitch:** LonTalk router between two TP/FT-10 (media) network segments. This also has an RS-232 console port for configuration (generally not used).*

## Level 0: Sensors and Actuators

*Figure 34. **0-Temperature:** Thermistor Temperature Sensor (Nonlinear Resistance Change with Temperature)*


*Figure 35. **0-Actuator:** Motor and Valve Assembly, with Mechanical Position Indicator (0–10 VDC or 4–20 mA Analog Input Signal)*


*Figure 36. **0-Actuator:** Electric motor taking 4-20 mA or 0-10 VDC analog input signal and producing a 90-degree rotation.*

## International Society of Automation Reference Architecture

**The ISA and the IEC 62443 security standard for industrial automation and control systems is the most common standard for industrial control systems. Neither standard includes buildings as a distinct category; applying the ISA standard would require adaptation of new controls. In 2017, a working group delivered a report, IEC 62443 Standards and ISA Secure Certification: Applicability to Building Control Systems, with recommendations that ISA develop certifications and courses for building automation.[31] ISA now has a Technical Topic web page[32] and an Introduction to Building Automation Systems course and certificate.[33]**

**The ISA/IEC 62443 Physical Architecture model shown in Figure 37 and the Industrial Network with Zones and Conduits shown in Figure 38 highlight the primary differences between traditional industrial control systems and Building OT control systems.**

To meet the challenges of cybersecuring next-generation buildings, the next decade will move to a zero trust architecture (ZTA).

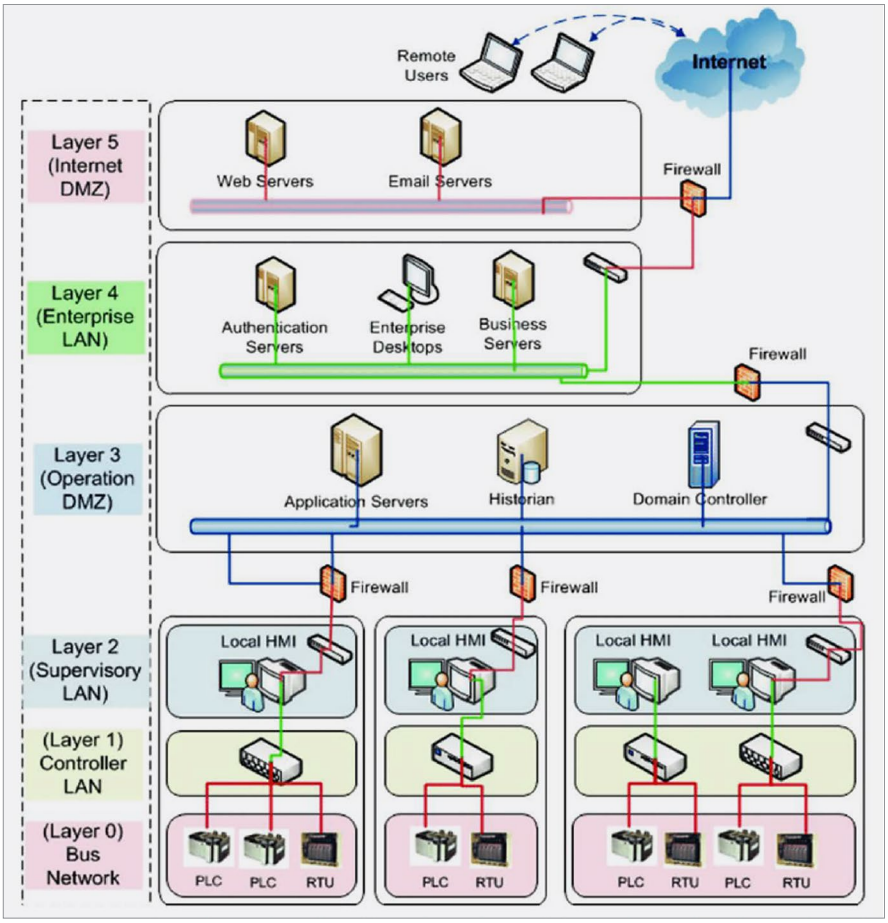


*Figure 37. IEC 62443 Physical Architecture Model of an Industrial Network*

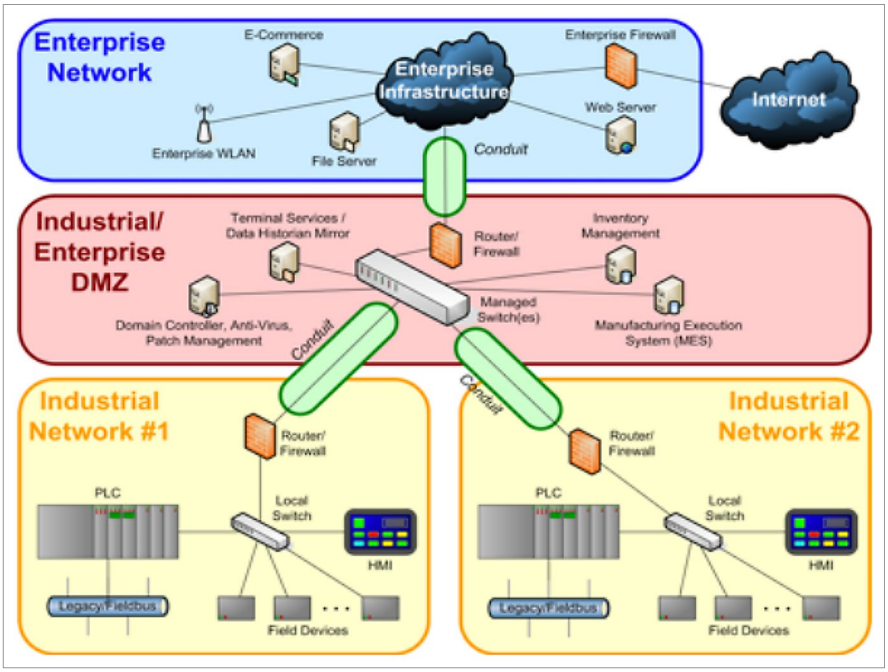


*Figure 38. ISA 62443 Reference Architecture Industrial Network Model of Zones and Conduits*

[31] "IEC 62443 Standards and ISA Secure Certification: Applicability to Building Control Systems," ISA Security Compliance Institute, https://isasecure.org/en-US/Documents/ISASecure-BCS-Study-(v0_8)

[32] "Building Automation," International Society of Automation, www.isa.org/technical-topics/building-automation

[33] "Introduction to Building Automation Systems (EA15)," International Society of Automation, www.isa.org/training-and-certification/isa-training/instructor-led/course-descriptions/ea15

# Zero Trust Architecture

The basic premise of a ZTA is exactly as the name implies: Trust neither anybody nor anything. Pre–zero trust, the traditional approach was to trust devices within the network perimeter boundary. Trust was usually tied to location and the use of certificates to establish a trust relationship.

### What is Zero Trust?

**As defined by NIST SP 800-207, "Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture."**

A ZTA differs markedly from a defense-in-depth architecture (shown in Figure 39).

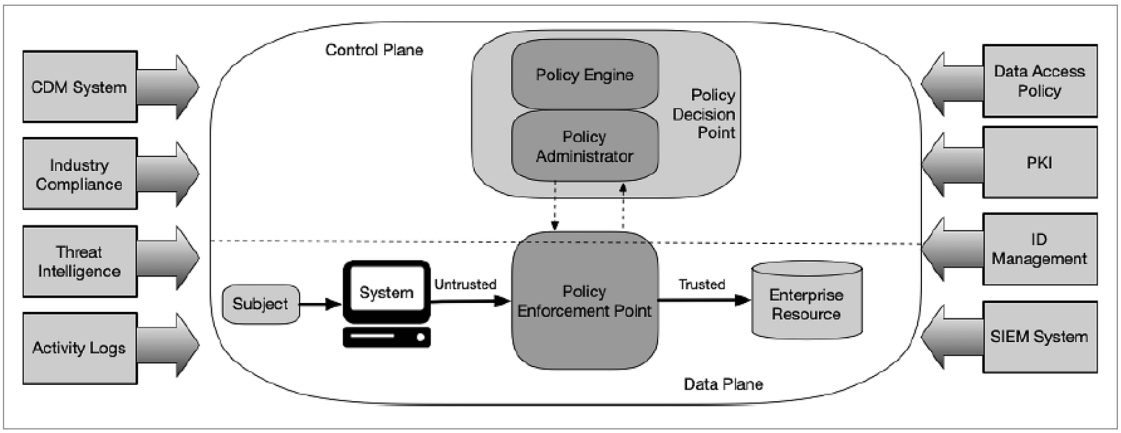


*Figure 39. NIST SP 800-207 ZTA Core Zero Trust Logical Components*

The ZTA provides the foundation to provide the needed access for contracted services/nonemployees to use the organizational access to the internet to perform maintenance tasks or attend a conference and connect to the organizational apps and databases (HVAC, lighting, meters) while obscuring enterprise resources, as shown in Figure 40.

### Building Control Systems Cybersecurity Solutions Overlay

**Building OT systems were historically considered "air gapped" and not a valuable target, and few vendors implemented rigorous security into the software or appliances. Most of the systems had "flat networks," meaning little or no segmentation or use of VLANs. The BACnet and Modbus protocols are unauthenticated and unencrypted and highly vulnerable. Since 2013, a number of BMSes have been exploited, and building owners and facility managers have begun to realize the significant economic harm a successful exploit could cause.**

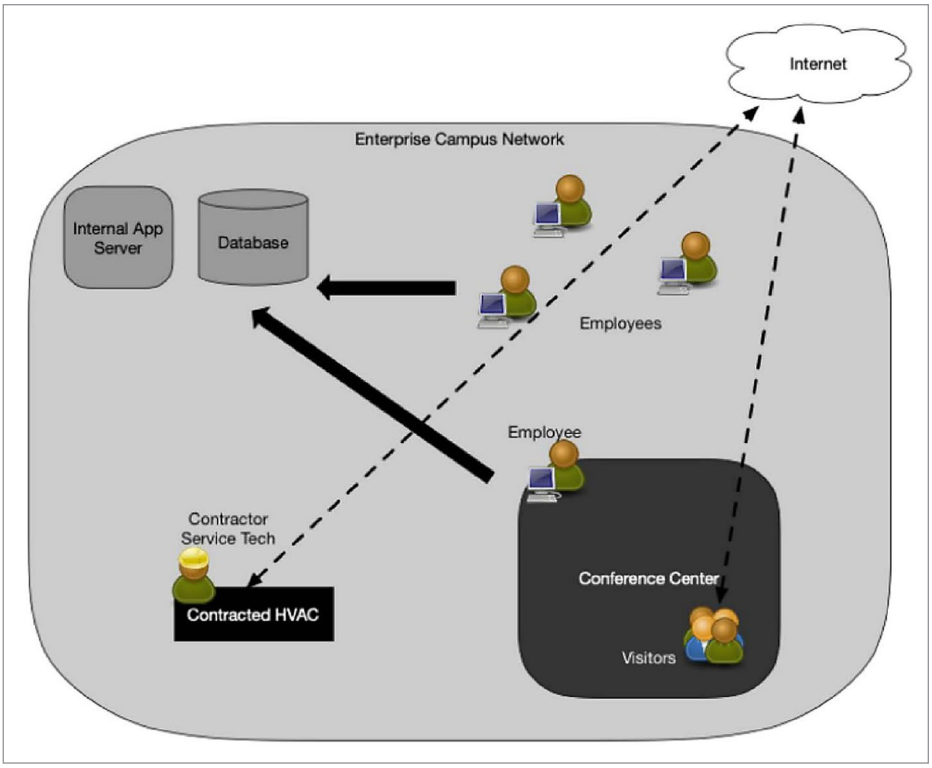


*Figure 40. Enterprise with Nonemployee Access*

Why attack the BMS?

- Extortion
- Business competition
- Vandalism
- Cyberterrorism
- Nation-state attack

Then consider the economics of commercial office buildings:

- Assume 200,000 rentable square feet (RSF) * $30–50/sf = $0.6–1M/month rent = $7.2–12M/year
- Assume 20 tenant companies, each grossing $1M/year = $20M/year
- Local community taxes @ 5% = $30M *.05 = $1.5M
- Potential physical damage = 200,000 * $50 to 150 SF = $10–30M
- Total at risk (average) = $10 + 20 + 1.5 + 20 = ***$51.5M for one commercial building***
- An owner/REIT (real estate investment trust) could have thousands of sites, and millions to billions of square feet

Recent ransomware attacks on control systems demonstrate the attractiveness and financial reward of targeting and exploiting the BMS.

Now consider the impact on a school campus, hospital, warehouse, veterinary, research and development center, manufacturing plant, or retail chain. As these systems become connected to the internet, the attack surface grows exponentially. Fortunately, vendors have risen to the challenge, and a cybersecurity solutions overlay can now provide defense-in-depth, advanced hunt and defend, threat intelligence, and endpoint detection. The Fortinet family of products illustrates how a layered approach can protect the BMS, as shown in Figures 41 through 44.

We can apply this cybersecurity overlay to any reference architecture.

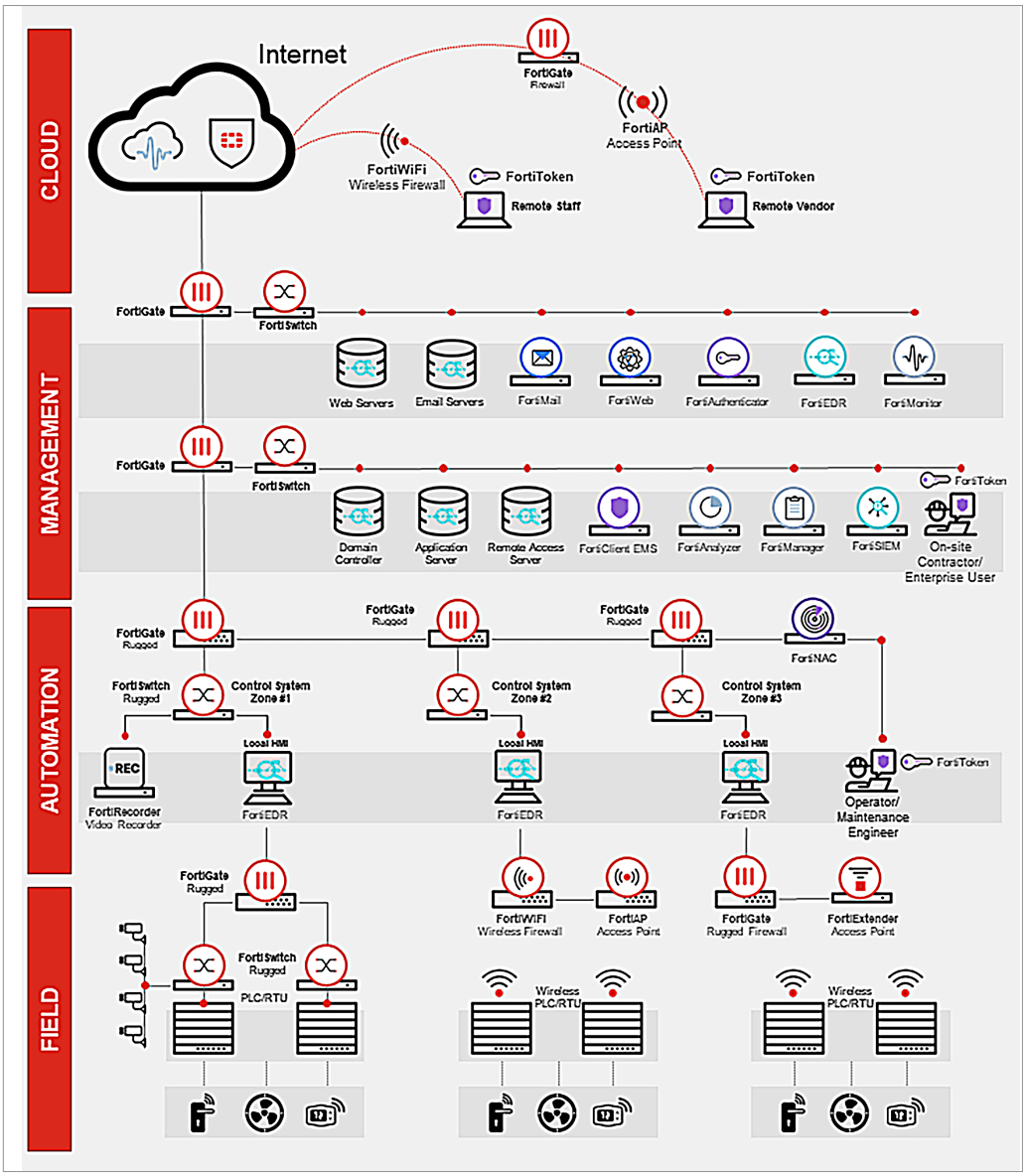


Figure 41. Fortinet Cybersecurity Solutions Overlay


Figure 42. FortiToken on Mobile Phone


Figure 43. FortiSwitch

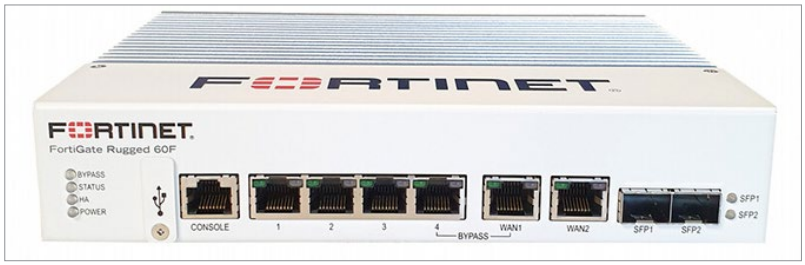


Figure 44. FortiGate

# Securing the Smart Building with the Fortinet Security Fabric

Although the growing trend of system interdependencies and interconnections allows for an extreme capability of data sharing and system-to-system integration, it also increases the need for security solutions that ensure appropriate access and communications while preventing potential adversary actions. Identify key cybersecurity facility-related areas of concern that need to be addressed with technical or procedural controls, including:

- Secure communications paths
- Network segmentation, including IoT and micro-segmentation
- Endpoint detection and response
- Secured remote access
- Transient asset defense
- System management
- Event logging
- Monitoring and alerting

By considering a solution provider and its partnerships across the OT sector and specifically within the building cybersecurity space, a facility management team can identify areas of coverage across providers that meet their specific needs. Table 1 maps Fortinet's products to specific BMS cybersecurity needs.

**Table 1. Fortinet Products for Specific Cybersecurity Needs**

| Cybersecurity Need | Solution Paths | Unique Capabilities |
|---|---|---|
| *Secure communications paths with BMS protocols coverage* | • FortiGate Next-generation Firewall (NGFW)<br>• FortiSwitch<br>• FortiAPs | Solutions provide capabilities to ensure approved devices are communicating over accepted validated protocols and allow for programmatic response across the Fortinet fabric to disable an endpoint if suspicious activity has triggered a response need.<br>Deep packet inspection on BMS protocols enabled for application control and MW intrusion prevention. |
| *Network segmentation and micro-segmentation* | • FortiGate<br>• FortiSwitch<br>• FortiAPs | Solutions provide the capability to control and restrict communications across enforcement points in north-to-south network communications throughout a defined network architecture, as well as communications within a network segment occurring east to west across a switched infrastructure (micro-segmentation) |
| *Secured remote access* | • FortiAuthenticator<br>• FortiClient<br>• FortiToken | Ensuring appropriate multifactor authentication and role-based access control for users, applications, and devices. Authentication of accessing endpoint and secure communications across remote session. |
| *Transient asset defense* | • FortiNAC<br>• Dragos partnership for OT | As assets move throughout a facility environment or campus, it is essential to ensure a particular asset or endpoint meets the requirements to participate within a defined segment. Within a traditional IT environment, the FortiNac device can provide protections and defined configuration policy requirements for an endpoint, and within an OT environment Fortinet has established a partnership with Dragos. The Dragos platform and deployed OT sensors can identify transient assets connecting within an OT segment and detect potentially malicious activity. |
| *System management* | • FortiManager | Unique solution capability of a single view across entire solution fabric and network device visibility and management. |
| *Critical BMS endpoint detection and response* | • FortiEDR | Solution approach focuses on pre-infection prevention and prediction, as well as post-infection detection and remediation of endpoint events. |
| *Event logging* | • FortiSIEM | Essential visibility, correlation, and response capabilities with collection across a diverse set of asset types and formats with OT context. |
| *Monitoring and alerting* | • FortiSIEM<br>• FortiAnalyzer<br>• Dragos partnership for OT | Event collection across a wide area of asset types and the capability to identify events of interest or potential malicious activity is an absolute requirement for a cybersecurity solution utilized within a traditional IT environment. It can prove challenging to identify a single solution that performs this function across both IT and OT areas. This represents another unique area where Fortinet has partnered with Dragos to leverage that company's OT-specific solution visibility, detection, and response capabilities. |

Fortinet also provides surveillance and communications solutions for smart buildings, as listed in Table 2.

All the Fortinet solutions can be seamlessly integrated within Fortinet Security Fabric[34] to offer a holistic cybersecurity platform for smart and digital infrastructures.

**Table 2. Fortinet Solutions for Smart Buildings**

| Requirements | Solution Paths | Unique Capabilities |
|---|---|---|
| Communications | • FortiFone<br>• FortiVoice | Robust IP phones with HD audio for versatile deployments and centralized control and simplified management of phone systems |
| Surveillance | • FortiCamera<br>• FortiRecorder | Centrally managed HDTV-quality reliable physical security coverage and platform for management of cameras, systems, and storage |

## Conclusion

Buildings are undergoing a revolution in how they are constructed, operated, used, renovated, and decommissioned. The next-generation cybersecure building will need a highly trained and cyber-skilled workforce, supported by new technologies and tools to ensure the physical safety of the occupant/visitor as well as the cyber safety of the building control and tenant information systems.

The pursuit of cybersecurity in traditional BMS operational environments has undergone a significant shift over the past 10 years. This shift has seen vendors and OEMs providing capabilities and support for asset owners and operators who choose to design cybersecurity solutions and architectures in new projects as well as integrating solutions into existing systems. Considering the cyber-to-physical systems being designed or deployed across the various building types and systems being controlled, it is important to take advantage of the cybersecurity progress made by the building community. Utilize its standards, controls frameworks, experienced personnel, and solutions providers to ensure that these systems are being designed, built, operated, and maintained in a cybersecure manner.

Achieving cybersecurity across complex systems could easily result in complex security solutions that could become overly burdensome to operate and maintain. Over time, as the solutions available in the market mature in capabilities and in ease of support, you'll achieve a great benefit by identifying the best set of products for a particular implementation. When solution providers identify partnerships that enrich customer experience and cybersecurity capabilities, the result can be a uniquely positive benefit for the asset owner and operator.

[34] Fortinet Security Fabric, www.fortinet.com/solutions/enterprise-midsize-business/security-fabric

## About the Authors

**Dr. Michael Chipley** is a cybersecurity subject matter expert supporting federal and private sector clients to meet current and evolving cybersecurity requirements for IT and OT systems. He is a contributor/writer to the NIST standards and DoD Risk Management Framework, and creator of the Whole Building Design Guide Cybersecurity and DoD ESCTP Cybersecurity websites. He has taken over 200 federal organizations and private sector companies through the NIST Risk Management Framework process to ensure that their IT and OT systems are cybersecure and that they can detect, contain, and report cyber events/incidents and recover back to normal operations.

Author **Tim Conway** serves as the technical director for ICS and SCADA programs at SANS and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Recognizing the need for ICS-focused cybersecurity training throughout critical infrastructure environments and an increased need for NERC CIP hands-on training, Tim co-authored and instructs ICS456: Essentials for NERC Critical Infrastructure Protection. During his career, Tim has served as the chair of the RFC CIPC, the NERC CIP Interpretation Drafting Team, the NERC CIPC GridEx Working Group, and the NBISE Smart Grid Cyber Security panel.

## Sponsors

**SANS would like to thank this paper's sponsors:**

FORTINET®

DRAGOS

# Appendix

## Building Codes

- **International Building Code (IBC 2018).** The International Building Code (IBC) either is in use or adopted in all 50 states of the United States of America, as well as the District of Columbia, Guam, Northern Marianas Islands, the U.S. Virgin Islands, and Puerto Rico. However, because it is the International Building Code and part of a series of International Codes (I-Codes), it is used in multiple locations worldwide, including the 15 countries of the Caribbean Community and Common Market (CARICOM), Jamaica, and Georgia.
- **International Code Council's I-Codes.** The International Codes (I-Codes), developed by the International Code Council, are a family of 15 coordinated, modern building safety codes that help ensure the engineering of safe, sustainable, affordable, and resilient structures. The I-Codes are the most widely accepted, comprehensive set of model codes used in the United States.
- **International Fire Code (IFC).** The IFC contains regulations to safeguard life and property from fires and explosion hazards. Topics include general precautions, emergency planning and preparedness, fire department access and water supplies, automatic sprinkler systems, fire alarm systems, special hazards, and the storage and use of hazardous materials.
- **International Plumbing Code (IPC).** The IPC provides minimum regulations for plumbing facilities in terms of both performance and prescriptive objectives and provides for the acceptance of new and innovative products, materials, and systems.
- **International Mechanical Code (IMC).** The IMC provides minimum regulations for mechanical systems using prescriptive and performance-related provisions that make possible the use of new materials, methods, and design.
- **International Energy Conservation Code (IECC).** The IECC addresses energy efficiency on several fronts, including cost savings, reduced energy usage, conservation of natural resources, and the impact of energy usage on the environment.
- **Uniform Building Code (UBC).** The UBC contains precise requirements that every building must follow. The UBC was replaced in 2000 by the new International Building Code (IBC).
- **State and Local Building Codes and Zoning.**[35]
- **American Society for Testing and Materials (ASTM) (Materials).** The ASTM is an international standards organization that develops and publishes voluntary consensus technical standards for a wide range of materials, products, systems, and services, with over 12,800 ASTM standards that operate globally.
- **American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) (Mechanical).** The ASHRAE is a nonprofit organization that develops and publishes standards for the heating, ventilating, and air conditioning industry.

[35] "Contacts for Building Codes by State," Buildings Guide, www.buildingsguide.com/blog/resources-building-codes-state/

- **National Fire Protection Association (NFPA) (Fire).** The NFPA is an international nonprofit organization devoted to eliminating death, injury, property, and economic loss due to fire, electrical, and related hazards.
- **National Electrical Code (NEC) (Electric).** The NEC, or NFPA 70, is a regionally adoptable standard for the safe installation of electrical wiring and equipment in the United States. It is part of the National Fire Code series published by the NFPA.

## Voluntary Standards

- **USGBC LEED Green Building Certification.** The U.S. Green Building Council (USGBC) Leadership in Energy and Environmental Design (LEED) is a green building certification program used for the design, construction, operation, and maintenance of green buildings, homes, and neighborhoods worldwide.
- **Green Globes Certification.** Green Globes is an online green building rating and certification tool that is used primarily in Canada and the United States that can be used for new construction (also applies to major renovations) and for sustainable interiors (applies to commercial/tenant interior projects or fit-ups).
- **EPA Energy Star Certification.** ENERGY STAR® is the government-backed symbol for energy efficiency, providing simple, credible, and unbiased information that consumers and businesses rely on to make well-informed decisions.

## Information Technology Standards

- **NIST 800 series.** The National Institute of Standards and Technology 800 publications are a series that elaborates on the U.S. federal government advanced computer security and network infrastructure policy.
- **IEC 60417.** International Electrotechnical Commission contains graphical symbols used to identify equipment or a part of equipment, indicate functional states, designate connections, provide information on packaging, or provide instruction for the operation of the equipment.
- **IEC 62443.** The International Electrotechnical Commission 62443 series was developed to secure industrial automation and control systems (IACS) throughout their lifecycle. It currently includes nine standards, technical reports (TRs), and technical specifications (TSs).
- **ISO/IEC 27001.** The International Organization for Standardization/ International Electrotechnical Commission has more than a dozen standards in the ISO/IEC 27000 family, which provides requirements for an information security management system (ISMS) for assets such as financial information, intellectual property, employee details, or information entrusted by third parties.
- **DoDI 8500/8510 Risk Management Framework.** The DoD 8500 policy series represents the Department of Defense's information assurance strategy and adopts the NIST 800 series as the basis of a common information assurance program across federal agencies.

## Risk and Financial Standards

- **SOC I and II.** System and Organization Controls (SOC), defined by the American Institute of Certified Public Accountants (AICPA), is the name of a suite of reports produced during an audit. It is intended for use by service organizations (organizations that provide information systems as a service to other organizations) to issue validated reports of internal controls over those information systems to the users of those services.
- **GPDR.** The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business.
- **DHS NIPP.** The National Infrastructure Protection Plan (NIPP 2013: Partnering for Critical Infrastructure Security and Resilience) outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.