# Operational Technology in Public Infrastructure: Procurement Challenges and Solution

Rev B, 2023

APPLIED CONTROL ENGINEERING

THE RIGHT SOLUTION. ON-TIME. ON-BUDGET.

# Presenter

- OT Cybersecurity Team Lead at Applied Control Engineering (ACE)
- Senior Member ISA
- MS Computer Engineering
- Global Industrial Cyber Security Professional (GICSP)
- Experience in control systems engineering and cybersecurity assessment in nuclear power, manufacturing, and many other verticals

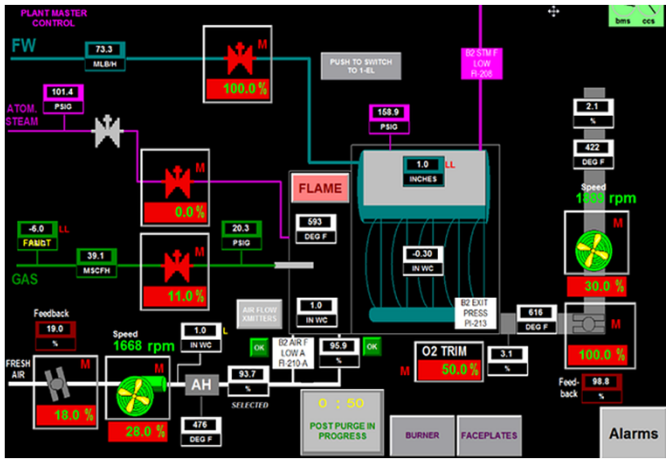
**Timothy P. Mullen, GICSP**

# Agenda

**For the purposes of this presentation, I will be using “OT” (operational technology) to refer to digital control systems, IACS, and all other permutations of computers participating in controlling the physical world**

- Introduction to common operational technologies in public and institutional settings
- Baseline on OT and OT Cybersecurity
- Typical Last Mile OT Supply Chain
- How to create desired security outcomes in OT
- Bottom Line Up Front: Explain how to address the OT purchasing environment to get secure deployments

# The machines are in control




## Some definitions

- OT: Operational Technology
  - The purpose of OT systems is to monitor and control physical processes such as machines, reactors, and factory lines
  - Includes traditional digital Industrial Control Systems (ICS) technologies alongside newer Industrial Internet of Things (IIOT) systems
  - Utilizes a large number of dedicated-purpose, embedded-system-style devices
    - Incumbent vulnerability, visibility, and management challenges

# IT vs OT

- Traditional song is that IT is more data focused and OT is more function focused
  - In terms of the C-I-A triad, IT cares about C-I-A while OT cares about A-I-C

## IT

- Technology served by technology
  - Need for upgrade cycles is understood
- In larger organizations often supported by dedicated network, infrastructure, security teams
- “Data” is typically an essential component of the system performing its critical functions

## OT

- Technology serves the machines
  - The “machine” is expected to run for decades after purchase
- Needs to be supported by technicians, controls engineers, and integrators
- The “data” component is often low-confidentiality and low-volume
- System downtime = no product produced

# Operational Technology: The Critical Infrastructure of Critical Infrastructure

- Fundamental utilities including electrical power, environmental control (heating and cooling), water, and other supplies are all controlled by Operational Technology

https://www.pnnl.gov/projects/om-best-practices/modular-boiler-systems

# Operational Technology

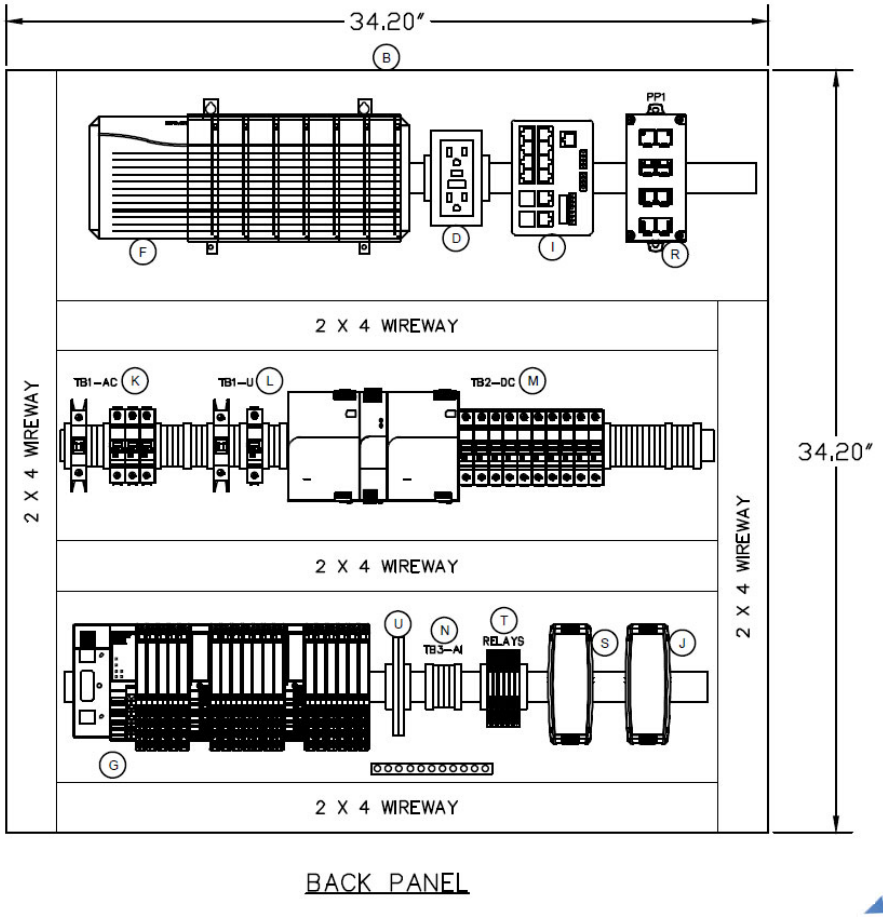
https://fo.uconn.edu/departments/facilities-energy-services/cogen/

https://www.pnnl.gov/integrated-building-assets


https://www.energy.gov/sites/default/files/styles/full_article_width/public/19631.JPG?itok=OOPya1Bq

# OT: System Versus Components

- Systems are purchased, and they are implemented with digital components (OT)
- Common components:
  - Network Switches
  - SFF/Industrial PCs
  - Servers
  - Controllers/PLCs
  - Field devices



# OT Components

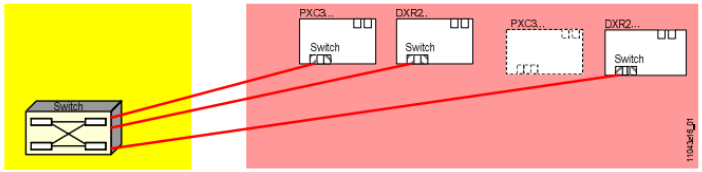
## 9.2 Network topologies

**Topologies**

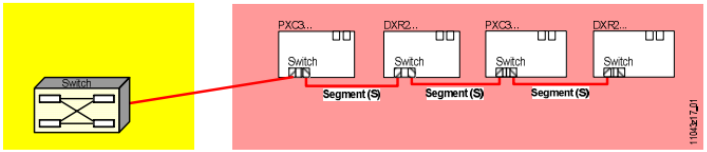
You can use the following bus topologies:

- Star topology (general).
- Line topology (for room automation).
- DXR2... and PXC3... can be mixed.

**Star topology**



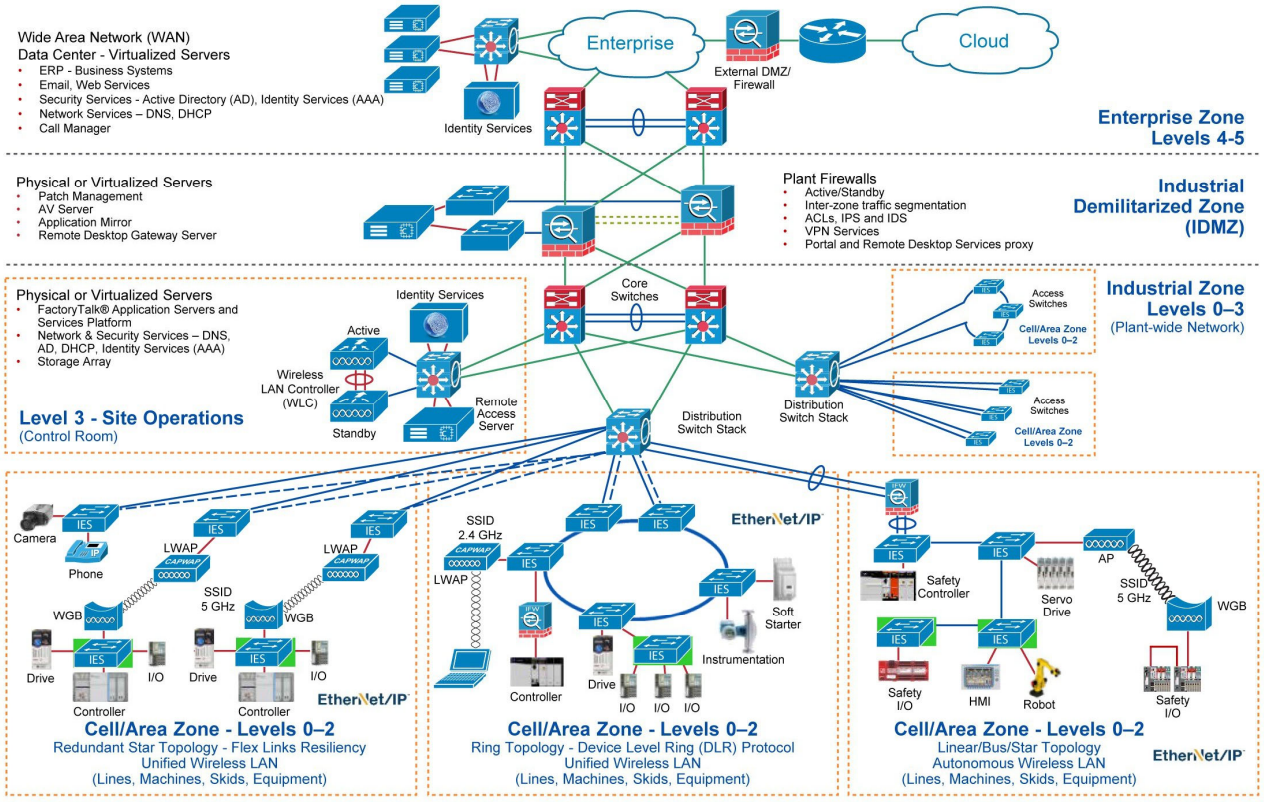

**Line topology**

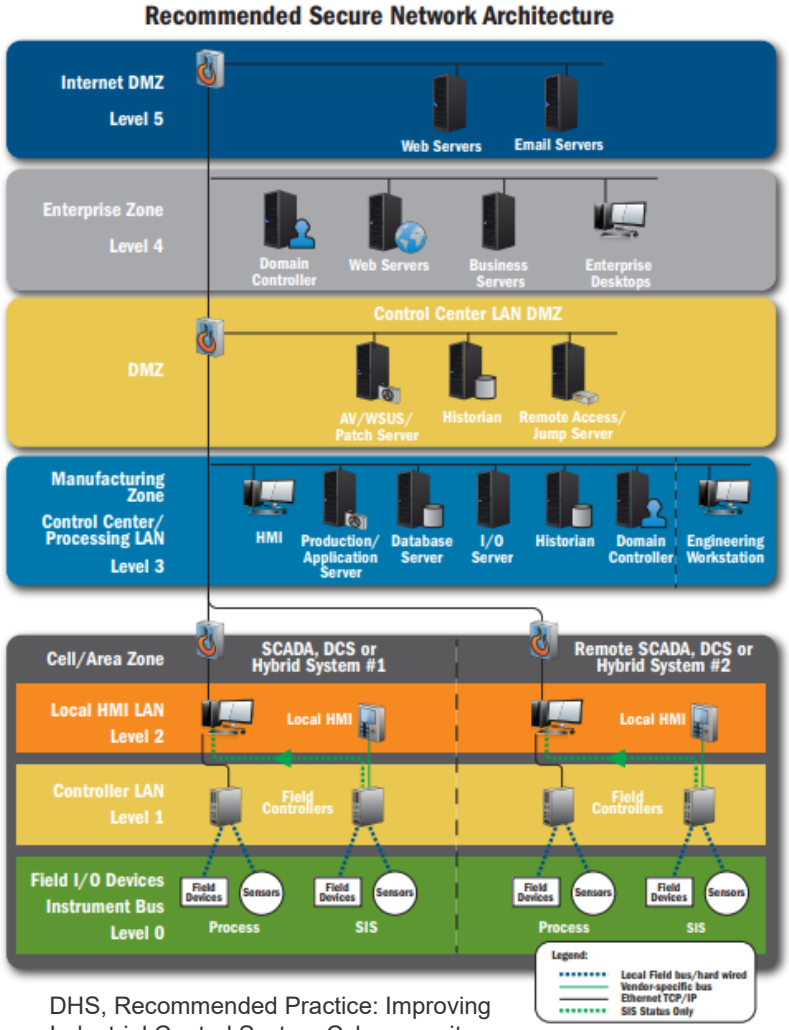



Notes

- The number of room automation stations is limited to 20 for a line topology (daisy chain).

# OT Cybersecurity




378088

DHS, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/OEM/DIG/CPwE-5-1-OEM-CRD/CPwE-5-1-OEM-CRD1.html

# Convergence? Maybe some day

- IT software developers
  - Move security problem to the Application layer (HTTPS, SSH, Kerberos, TLS)
  - Data confidentiality is most important function
- OT software developers
  - Heavy reliance on other network layers
    - PHY/DLL – Segmentation
    - Transport - VPNs

# That Pesky Security

- Reality in OT is that the network is THE most important security layer
  - Contrast with IT where zero-trust is reducing the network's role
- The goal of OT cybersecurity is preventing the system critical functions from being adversely impacted by a cyber incident
  - Design criteria to achieve this include:
    - Limiting logical pathways to reduce the number of attack vectors
    - Monitoring network traffic and alerting on off-normal conditions

# How did I end up with this thing?

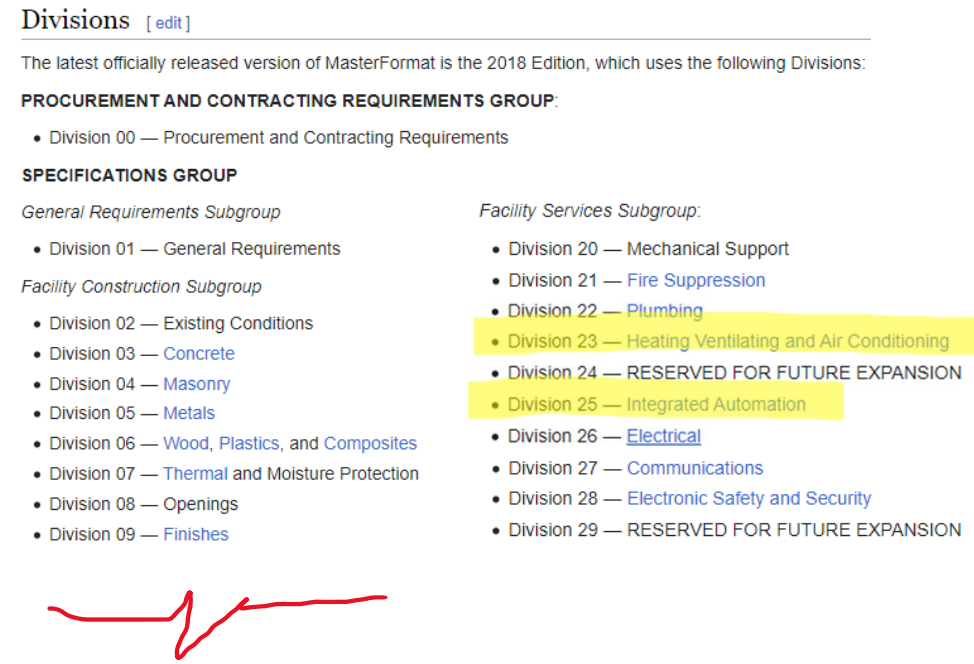
- Engineered facilities and systems are built to specification
  - Specifications are typically prepared by engineers or architects on behalf of facility owners
  - Describe what is supposed to be furnished by the construction contractor(s)
- Contractors bid on completing a unit of work based on prepared specifications, drawings, and scope of work provided
  - https://mmp.delaware.gov/Bids/

# Built to spec

- Scopes of work, drawing packages, and specifications are prepared for a *project*
  - Construction of new powerhouse to provide reliable on-site power
  - Upgrade of chillers in chiller plant to meet greater demand
  - Replacement of building controls to reduce energy costs with improved control
- Multiple disciplines of engineering and trades involved in most projects

# About CSI MasterFormat

- Within specifications, different requirements are organized into different sections.  In the US, the Construction Specification Institute's MasterFormat is the most commonly used template
- Divisions 23 and 25 most common for OT in facilities, but can appear in others
- Other formats possible



## Divisions [ edit ]

The latest officially released version of MasterFormat is the 2018 Edition, which uses the following Divisions:

**PROCUREMENT AND CONTRACTING REQUIREMENTS GROUP**:

- Division 00 — Procurement and Contracting Requirements

**SPECIFICATIONS GROUP**

*General Requirements Subgroup*

- Division 01 — General Requirements

*Facility Construction Subgroup*

- Division 02 — Existing Conditions
- Division 03 — Concrete
- Division 04 — Masonry
- Division 05 — Metals
- Division 06 — Wood, Plastics, and Composites
- Division 07 — Thermal and Moisture Protection
- Division 08 — Openings
- Division 09 — Finishes

*Facility Services Subgroup*:

- Division 20 — Mechanical Support
- Division 21 — Fire Suppression
- Division 22 — Plumbing
- Division 23 — Heating Ventilating and Air Conditioning
- Division 24 — RESERVED FOR FUTURE EXPANSION
- Division 25 — Integrated Automation
- Division 26 — Electrical
- Division 27 — Communications
- Division 28 — Electronic Safety and Security
- Division 29 — RESERVED FOR FUTURE EXPANSION

# Example Specifications for Bid

DELAWARE STATE POLICE HEADQUARTERS
OCTOBER 2023

CHILLER REPLACEMENT
OMB/DFM# MC1002000714

**SECTION 23 09 50**

**BUILDING AUTOMATION SYSTEM (BAS) GENERAL**

**PART 1 - GENERAL**

**1.01 SECTION INCLUDES**

A. General Requirements
B. Description of Work
C. Quality Assurance
D. System Architecture
E. Distributed Processing Units/Quantity and Location
F. Demolition and Reuse of Existing Materials and Equipment
G. Sequence of Work

**1.02 RELATED DOCUMENTS**

A. Section 23 09 69 - Variable Frequency Controllers
B. Section 23 09 51 - Building Automation System (BAS) Basic Materials, Interface Devices, and Sensors
C. Section 23 09 53 - BAS Field Panels
D. Section 23 09 54 - BAS Communication Devices
E. Section 23 09 55 - BAS Software and Programming
F. Section 23 09 58 - Sequences of Operation
G. Section 23 09 59 - BAS Commissioning

**1.03 DESCRIPTION OF WORK**

A. The building automation system (BAS) defined in this specification shall interface with OMB/Division of Facilities Management Network, and shall utilize the BACnet communication requirements as defined by ASHRAE/ANSI 135 (current version and addendum) for all communication.
B. This system shall be an extension of the existing Automated Logic System currently installed in building.
C. The systems to be controlled under work of this section basically comprise new HVAC systems. The HVAC systems being controlled are Pumps and Chillers. This Section defines the manner and method by which these controls function.
D. The BAS contractor shall provide Variable Frequency Controllers for all equipment identified as having a Variable Frequency Controller (or Variable Frequency Drives "VFD"). The Variable Frequency Controller shall be in accordance with specification section 23 09 69.

**1.04 APPLICATION OF OPEN PROTOCOLS**

A. Subject to the detailed requirements provided throughout the specifications, the BAS and digital control and communications components installed, as work of this contract shall be an integrated distributed processing system utilizing BACnet. System components shall communicate using true BacNET in accordance with ASHRAE Standard 135 and current addenda and annexes, including all workstations, all building controllers, and all application specific controllers. Gateways to other communication protocols are not acceptable

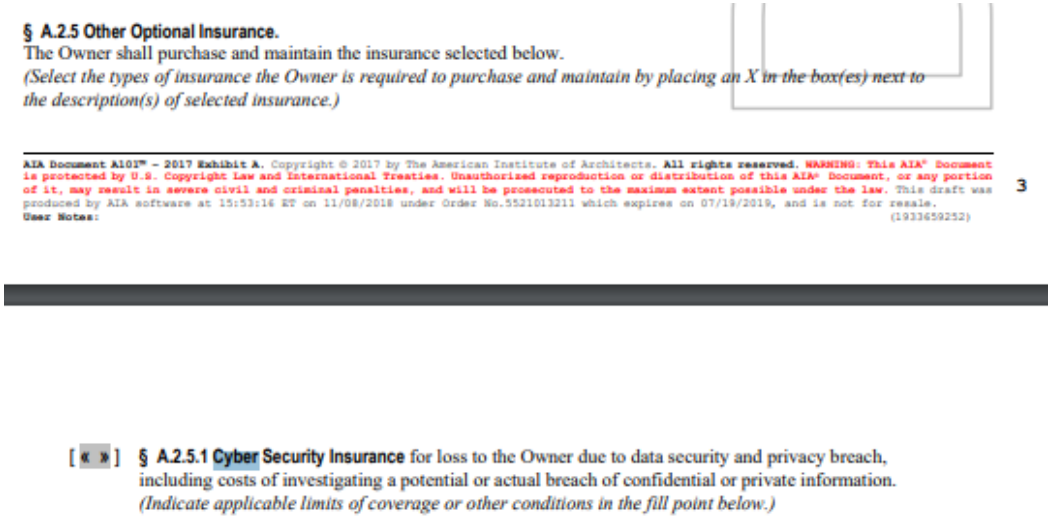


**1.03 DESCRIPTION OF WORK**

A. The building automation system (BAS) defined in this specification shall interface with OMB/Division of Facilities Management Network, and shall utilize the BACnet communication requirements as defined by ASHRAE/ANSI 135 (current version and addendum) for all communication.
B. This system shall be an extension of the existing Automated Logic System currently installed in building.
C. The systems to be controlled under work of this section basically comprise new HVAC systems. The HVAC systems being controlled are Pumps and Chillers. This Section defines the manner and method by which these controls function.
D. The BAS contractor shall provide Variable Frequency Controllers for all equipment identified as having a Variable Frequency Controller (or Variable Frequency Drives "VFD"). The Variable Frequency Controller shall be in accordance with specification section 23 09 69.

# Example

- The only place the “Cyber” appears in this document is in a draft insurance and bond example where it is an option for the owner to be required to purchase



§ A.2.5 Other Optional Insurance.
The Owner shall purchase and maintain the insurance selected below.
*(Select the types of insurance the Owner is required to purchase and maintain by placing an X in the box(es) next to the description(s) of selected insurance.)*





[ « » ] § A.2.5.1 Cyber Security Insurance for loss to the Owner due to data security and privacy breach, including costs of investigating a potential or actual breach of confidential or private information.
*(Indicate applicable limits of coverage or other conditions in the fill point below.)*

# Built to Spec

- OT components are often configured and deployed by specialty subcontractors to the prime contractor or another discipline, so another layer of distance from the security posture owner and the potential security implementor
- Lowest cost typically drives selection, so spending extra time configuring devices to be more secure (like changing default passwords) loses out
  - Sometimes lowest cost is mandatory requirement
- When security is not included in the specification, there is a *disincentive* to OT assets being configured in a more secure fashion
  - Changing default passwords takes more time than not, both in front end and in maintaining an otherwise unneeded password management system
  - Deploying unmanaged switches in a daisy-chain is fast and cheap

# What do we want? It's in the spec

- If security is a critical function that needs to be incorporated in to the design of the system, then it needs to be in a spec
- Prior art: Unified Facilities Criteria and Unified Facility Guide Specifications, parts of the Whole Building Design Guide

# UFGS 25 05 11 Cybersecurity For Facility-Related Control Systems

1.9 CYBERSECURITY DOCUMENTATION
1.9.1 Proposed STIG and SRG Applicability Report
1.9.2 Cybersecurity Interconnection Schedule
1.9.3 Network Communication Report
1.9.4 Control System Inventory Report
1.9.5 Software and Configuration Backups
1.9.6 Cybersecurity Riser Diagram
1.9.7 STIG, SRG and Vendor Guide Compliance Result Report
1.9.8 Control System Cybersecurity Documentation
1.9.8.1 Software Applications
1.9.8.2 For HVAC Control System Devices
1.9.8.2.1 HVAC Control System Devices FULLY Supporting User Accounts
1.9.8.2.2 All Other HVAC Control System Devices
1.9.8.3 For Lighting Control System Devices
1.9.8.3.1 Lighting Control System Devices FULLY Supporting Us Accounts
1.9.8.3.2 All Other Lighting Control System Devices
1.9.8.4 [_____] Control System Devices
1.9.8.5 Default Requirements for Control System Devices
1.10 SOFTWARE LICENSING
1.11 CYBERSECURITY DURING CONSTRUCTION
1.11.1 Contractor Computer Equipment
1.11.1.1 Operating System
1.11.1.2 Anti-Malware Software
1.11.1.3 Passwords and Passphrases
1.11.1.4 User-Based Authentication
1.11.1.5 Demonstration of Compliance
1.11.1.6 Contractor Computer Cybersecurity Compliance Statement
1.11.2 Temporary IP Networks
1.11.2.1 Network Boundaries and Connections
1.11.3 Government Access to Network
1.11.4 Temporary Wireless IP Networks
1.11.5 Passwords and Passphrases
1.11.6 Contractor Temporary Network Cybersecurity Compliance Statements
1.12 CYBERSECURITY DURING WARRANTY PERIOD

PART 2 PRODUCTS

2.1 ETHERNET SWITCH
2.1.1 Required Functionality
2.1.2 Configuration Requirements
2.2 DAISY CHAIN IP CONTROLLERS
2.3 DATABASE AND WEB SERVER SOFTWARE FOR MODERATE IMPACT SYSTEMS

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES
3.2 NETWORK REQUIREMENTS
3.2.1 Information Flow Enforcement In MODERATE Impact Systems
3.2.2 Wireless and Wired Broadcast Communication for Fire Protection Systems
3.2.3 Wireless and Wired Broadcast Communication for Systems Other than Fire Protection Systems
3.2.3.1 Wireless and Wired Broadcast IP Communications
3.2.3.2 Non-IP Wireless Communication
3.2.3.3 Wireless and Wired Broadcast Communication Request
3.2.3.4 Wireless Communication Testing
3.2.4 Non-IP Control Networks
3.2.5 IP Control Networks
3.2.5.1 IP Network Routers
3.2.5.2 IP Devices With Multiple Ethernet Connection
3.2.6 Cryptographic Protection
3.2.7 Device Identification and Authentication
3.2.7.1 For HVAC Control System Devices
3.2.7.2 For Lighting Control System Devices
3.2.7.3 [_____] Control System Devices
3.2.7.4 Default Requirements for Control System Devices
3.2.8 Cryptographic Module Authentication
3.3 ACCESS CONTROL REQUIREMENTS
3.3.1 User Accounts
3.3.1.1 Computers
3.3.1.2 Controllers

# UFGS 25 05 11 Cybersecurity For Facility-Related Control Systems

[ For all devices with a password, change the password from the default password. Coordinate selection of passwords with the Password Point of Contact. Do not use the same password for more than one device unless specifically instructed to do so. Provide a Confidential Password Report documenting the password for each device and describing the procedure to change the password for each device.

Do not provide the Password Summary Report in electronic format. Provide [two][_____] hardcopies of the Password Summary Report, each copy in its own sealed envelope.

][For all devices with a password, coordinate the changing of passwords with the project site following testing of the system but prior to turnover to the Government. Coordinate with Password Point of Contact to determine appropriate project site personnel to complete password changes. Accompany identified personnel to each device with a password and instruct personnel on the process of changing password. Record the time, date and personnel present when each device's password is changed and submit a Password Change Summary Report documenting this information.

Provide the Password Summary Report electronically in both PDF and Microsoft Excel.
]

3.4.6 Authenticator Feedback

{For Government Reference Only: This subpart relates to IA-6; CCI-000206}

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.



# Operational Technology in Public Infrastructure: Procurement Challenges and Solution

Rev B, 2023

APPLIED CONTROL ENGINEERING

THE RIGHT SOLUTION. ON-TIME. ON-BUDGET.