*This editable version of the Health Care Cyber Requirements for Operational Technology document is provided to support construction project teams in adapting the requirements to their own projects. This document is intended to be issued with the contract documents. Please review the ASHE monograph* Best Practices Framework for Health Care Cyber-Physical Protection: For the Construction Project Team *for additional information.*

**Health Care Cyber Requirements for Operational Technology**

### Part 1 – General

#### Summary

* + 1. Provide complete functional cyberprotected system, coordinated with the construction schedule and between trades.
		2. Furnish cyber designer services and labor for cyberprotection of operational technology as indicated.
		3. The operational technology network and devices will be cyberhardened, while supporting all use-cases that require integration of data between systems.
		4. All IP devices will reside on the owner-provided network.
		5. Owner-provided:
			1. Network switches and firewalls.
			2. Anti-virus software.
			3. Virtualized or physical servers and workstations (unless manufacturer requires special server requirements).
			4. IP addresses and switch port assignments.
			5. Network security monitoring, intrusion detection, network flow behavior analysis, intrusion response.

OT network traffic is base-lined, and a method is used to detect and alert anomalous network traffic patterns or potential network intrusion, and block or modify network access.

#### Definitions:

* + 1. Operational Technology (OT): Technology that controls the physical environment. Examples of OT include: building management system, fire alarm, lighting control, shade control, physical access controls and security cameras, generator systems, etc.
		2. Use-Case: The sharing of data between two or more OT systems, providing a desired outcome directly or as result of data analytics. The OT systems may be provided by one or more vendors. An example of a use-case outcome may be a smoke damper closing upon a fire alarm event, or a generator test report automatically created and emailed.
		3. Cyberhardened:
			- 1. Defense in depth elements to achieve a cyberhardened system include network segmentation, changing device default settings, disabling unused services, etc.
				2. All internet traffic is routed through the firewall; no unauthorized access is allowed on the network.

#### Quality Assurance

1. This guide is based on the latest revisions of *NIST Special Publication 800-82* and *UFC 4-010-06 Cybersecurity of Facility-Related Control Systems* and the owner’s cybersecurity experience, and is rooted in IT cybersecurity best practices.
2. System and devices will be UL Listed.
3. OT devices will be cyber hardened per device manufacturer capabilities.
4. Cyber designer qualifications: The team will be led by an individual with minimum five years’ hands-on experience in successful cyber configurations on three comparably sized projects.
5. Cyber designer responsibilities:
	* + 1. Configure cyber network and devices per owner standards (appendix C).
			2. Lead each required meeting and track open items to completion.
			3. Confirm cyber configuration supports all project use-cases (appendix A).
6. Meetings:
	1. Preliminary and final meetings with owner for cyber network configuration:
		1. Cyber IP device configurations.
		2. OT IP inventory of device documentation.
		3. Patching and change management documentation through substantial completion to owner turnover.
	2. Provide hardening guides for all Level 2 and 3 devices (per UFC 4-010-06) to each user set and user group.

#### Submittals

1. Shop drawings:
	1. Cyber secure network configuration diagram:
		1. Including air-gapped networks not connected to the main OT network
		2. Include wireless, Bluetooth, cellular networks
	2. Cyber secure network riser:
		1. Including air-gapped networks not connected to the main OT network
	3. Provide total IP address quantity count and submit request to owner
	4. General purpose workstations and servers:
		1. Specifications and virtualization or physical installation requirements
	5. Special servers and appliances:
		1. Specifications and physical installation requirements
	6. Operational technology IP inventory of devices and IP master username/password list:
		1. Submit at project substantial completion
		2. Consolidate information for the entire OT network (from all manufacturers) of devices connected to the network

### Part 2 – Products

#### Acceptable manufacturers

* + - 1. Software loaded to the system must be approved by the Hospital Policy and Software Review Committee.

### Part 3 – Execution

#### Installation

1. Install per manufacturer’s recommendations.

1. Provide internet access via VPN and/or firewall rules to operational technology components that require internet access to function normally. Allow the device to connect only to required vendor systems over the internet. Tailor firewall and/or VPN rules to the IP addresses and ports required.
	1. Provide an air gap between networks where the integration of data with other systems is not required.
2. Network configuration, topology and services:
	1. Network topology:
		1. The OT network architecture document provides an example network topology that illustrates firewalled internet access from the OT network, VPN access into the OT network and network segmentation via VLAN.
		2. Network diagram:
			1. Identify hospital scope on the network diagram.
			2. Mimic the colors and levels of UFC 4-010-06 Figure 2-1; 5-level control system architecture diagram.
	2. Network switches:
		1. Owner to provide all OT network managed switches:
			1. Owner to configure, secure and route network switches.
		2. Construction staging switches may be used while awaiting hospital permanent switch installation:
			1. The construction staging switches will not connect to hospital network.
			2. No internet access is allowed to the construction staging switches.
		3. Switch port assignments specific to MAC address will be assigned by hospital staff.
	3. IP addresses:
		1. IP addresses will be assigned by hospital IP staff.
		2. IP addresses will be default internet-non-routable.
		3. Provide quantity of required addresses for all OT device groups.
	4. Encryption:
		1. Enable encryption and use on controllers and other OT component interfaces that offer the configuration. This allows secure transmission of unencrypted data (e.g., usernames and passwords) over an encrypted connection. One example is TLS encryption.
	5. Network applications:
		1. Domain Name System (DNS):
			1. DNS usage on OT networks is relatively rare at this time. Drop DNS requests before reaching the internet. If they are specifically required, use firewall rules to scope the use of DNS requests to the devices that require them.
		2. Hypertext Transfer Protocol (HTTPS):
			1. HTTPS is preferred.
			2. Where HTTP is used, the following best practices are required:
				1. Control access to web-based services on the physical or network layer using whitelisting.
				2. Apply access control to both source and destination.
				3. Implement authorization to access HTTP-based services at the application layer.
				4. Implement only the services needed.
				5. Log attempts of service usage.
		3. Secure FTP (SFTP) or Secure Copy (SCP):
			1. SFTP or SCP shall be used.
			2. TFTP will not be used on a new system (it may be used as a tool to talk to an existing system).
		4. Dynamic Host Configuration Protocol (DHCP):
			1. DHCP shall not be used without reservations.
			2. DHCP may be used if specified by the owner.
			3. Use a static configuration (typical for OT systems) instead of a dynamic IP address solution.
		5. Secure Shell (SSH):
			1. Where remote access is required to the control network, SSH will be used as an alternative to telnet, rlogin, rsh, rcp and other insecure remote access tools.
			2. SSH will be used over a VPN tunnel when accessing OT components remotely.
		6. Telnet:
			1. Secure Shell (SSH) will be used for administration, and encrypted tunnel (VPN) shall be used for inbound telnet session.
	6. General purpose management workstations and servers:
		1. Owner will virtualize or provide all servers, provide owner with specification requirements.
			1. If virtualization is not possible, provide owner with specification requirements.
		2. Anti-virus protection provided and managed by owner.
		3. User accounts for typical operation will not be privileged. Allow day-to-day usage of management computers without using administrative accounts.
		4. OT and IT connectivity will be dictated as required by use-cases. The device will not be used as a bridge.
		5. Security patches will be kept current.
		6. Workstation will only be used to administer the OT network and access the internet to download updates and access manufacturer websites; not to be used for general web use, including personal email or shopping.
	7. Appliances and specialty servers:
		1. User accounts for typical operation will not be privileged. Allow day-to-day usage of management computers without using administrative accounts.
		2. OT and IT connectivity will be dictated as required by use-cases. The device will not be used as a bridge.
		3. Security patches will be kept current.
		4. Where capable, provide and manage current anti-virus protection.
		5. Will be single purpose and only be used to administer OT network and access the internet to download updates and access manufacturer websites; not to be used for general web use, including personal email or shopping.
	8. Authentication and authorization:
		1. Users and passwords:
			1. No shared user accounts; each user of each system will have their own named user account and passwords.
			2. Default usernames and passwords provided by the manufacturer will be changed and documented.
			3. Where technically feasible, establish the following requirements for strong passwords:
				1. Password expiration: every 120 days.
				2. Minimum age of password: 1 day (password must be used minimum of 24 hours before being changed again).
				3. Minimum length: 8 characters.
				4. Password complexity: 3 of the following 4 groups must be used: UPPERCASE; lowercase; numeric; special characters
				5. Password history: last 5 passwords (cannot reuse last 5 passwords).
			4. Account lockout: after 5 consecutive unsuccessful logon attempts in 15 minutes.
			5. Renewed login: after 30 minutes of inactivity or by a system
		2. Authorization: Employ the principle of least privilege.
	9. Device configuration:
		1. Disabling unused features:
			1. Device features (example SSH or Telnet) that are not used for regular operation of the OT network will be disabled to reduce the attack surface.
	10. OT network devices and workstations:
		1. Operating systems (both server- and unit-based) will be the most current at bid time.
		2. Anti-virus software will be the most current at bid time (where anti-virus is used).
		3. Software loaded to the system must be approved by the owner software review committee.
	11. Patching and change management:
		1. OT manufacturer patches shall be applied prior to turn over to owner.
		2. Maintain a log of patch application and other changes made to the environment. Log should be in owner-acceptable spreadsheet format.
	12. OT IP inventory of devices and up-to-date master username/password list:
		1. Submit per hospital policy regarding data structure.
		2. See submittals in Part 1.
		3. OT-network-connected devices will be recorded and submitted. Data to include:
			1. OT system name
			2. Device name
			3. Device location (building, floor, closet, room #, etc.)
			4. 4-010-06 Level (1-5)
			5. Manufacturer, model, serial number
			6. Email point of contact
			7. Does device have username and password capabilities? (Y/N)
			8. Does password meet hospital policy for passwords? (Y/N)
			9. Is username and password changed from default value for Level 2 and higher devices? (Y/N)
			10. TLS 1.2 (or higher) enabled? (Y/N)
			11. HTTPS capable? (Y/N)
			12. Device MAC address
			13. Device firmware release
			14. Device operating system release
			15. VLAN # / name
			16. Patch panel number
			17. Switch port number
			18. Assigned IP address
			19. Assigned subnet
			20. Assigned gateway