SECTION 25 0000 - INTEGRATED AUTOMATION AND OPERATIONAL TECHNOLOGY

GENERAL

1.1 INTENT

The intent of this specification is to define an IoT and Integrated Automation Topology that will successfully integrate the Facility Management and Control Systems into a common secure platform that will allow for a consistent graphical display of control and functionality regardless of the control system vendor in the facility.

This section defines the following 3 major systems, subsystems and components that make up the IoT and Integrated Automation Topology:

1. INTEGRATION PLATFORM
   a. Main Server Hardware
   b. Firewall and DNS
   c. Server Rack
   d. IoT Server Software Platform
   e. Power Distribution Unit (PDU)
   f. Uninterruptable Power Supply (UPS)

2. OPERATIONAL TECHNOLOGY NETWORK (OTN)
   a. Network Manager
   b. Graphical User Interface
   c. Edge Switches
   d. Fiber Optic Cabling

3. IoT GATEWAY
   a. Java Application Control Engine (JACE)

1.2 MASTER SYSTEM INTEGRATOR REQUIREMENTS

A. The Master Systems Integrator (MSI) shall connect the building stakeholders with their building control systems and provide useful, meaningful and important information and control capabilities. The MSI is responsible for the integration of building control services such as HVAC, Life Safety, Electrical Distribution, Lighting Control, Security, CCTV, Data Centers and other controlled assets as shown in the systems architecture. The MSI shall provide a unified database and graphical user interface tools by collaboration with the owners building control needs. The MSI is also responsible for ensuring that all systems comply with the cybersecurity requirements defined within this specification.

B. Roles & Responsibilities: Services required but not limited to:

1. Install IoT server software platform capable of handling the entire portfolio in a location defined by the owner.
2. Co-ordinate with owner on proper use of IT within the Enterprise to include but not limited to Authentication, Security Certificates, SSL, and or any owner IT requirements. This is required only if connection is made to the owner's network.
3. Jointly develop integrated software plan with the owners building team and vendors to make sure all systems will communicate properly.
4. Reviews and meets with building team to ensure the building control system information will be accessible and useful.
5. Develop the software layer responsible for integration, aggregation and communications to the building control systems.
6. Standardize software tagging library, templates and menu hierarchy system, develop strategy for long term template maintenance.
7. Create and maintain graphical controls, monitors and dashboards as defined by the functional requirements of the system.
8. Configure alarm interface / controls, scheduling and user management capabilities.
9. Commission connected systems for usability and sustainability (all the software tools should be incorporated).
10. Document software maintenance strategy and upgrade procedures
11. The MSI is responsible for ensuring that all systems comply with the cybersecurity requirements defined within this specification.
12. Prior to project turnover, commission the Integration Platform and all connected subsystems provided by the Integrated System Contractors based on the specified cybersecurity policies and procedures.
13. The MSI will provide the Owner with a written commissioning report summarizing the compliance findings across all systems.

C. Qualifications:

Specific Requirements per Company

1. Experience in implementing Niagara framework similar for projects of similar size and scope.
2. Must have a successful history in the design and installation of Niagara Framework
3. Must have 5 years consecutive licensing capabilities with the Niagara Framework.
4. Must have minimum of 2 employed individuals who meet System Requirements per individual
5. Firms shall have specialized in and be experienced with the installation of the Niagara Framework for not less than one year from date of final completion on at least three (3) projects of similar size and complexity. Submittals shall document this experience with references.
6. Must be a Totem Trusted^{TM} Partner fully certified in the Totem risk management policies and procedures.

D. Specific Requirements: per individual

1. Must have 3 years experience with the firm represented
2. Proof of Niagara AX and Niagara 4 Certification.
3. List and describe a Niagara Enterprise (more than one building) integration project and the programmers involvement
4. List and describe a Niagara integration project involving multiple communication protocols or databases.
5. List and describe a Niagara integration project involving multiple platforms such as HVAC, Lighting Control, Security, Life Safety, Utilities and other building control and or monitoring systems.
6. Provide proof of Totem Trusted^{TM} Risk Management Certification for the individuals assigned to this project.

1.3 APPROVED MASTER SYSTEMS INTEGRATORS

A. Insert MSI Name Here
B. Insert MSI Name Here
C. Insert MSI Name Here
D. Insert MSI Name Here

1.4 SPECIFICATION NOMENCLATURE

A. Acronyms used in this specification are as follows:

1. Actuator: Control device that opens or closes valve or damper in response to control signal.
2. AI: Analog Input.
3. AO: Analog Output.
4. Analog: Continuously variable state over stated range of values.
5. BMS: Building Management System.
6. DDC: Direct Digital Control.
7. Discrete: Binary or digital state.
8. DI: Discrete Input.
9. DO: Discrete Output.
10. FC: Fail Closed position of control device or actuator. Device moves to closed position on loss of control signal or energy source.
11. FO: Fail open (position of control device or actuator). Device moves to open position on loss of control signal or energy source.
12. FMCS: Facility Management and Control System
13. GUI: Graphical User Interface.

14. HVAC: Heating, Ventilating and Air Conditioning.
15. IBC: Interoperable BACnet Controller
16. IDC: Interoperable Digital Controller.
17. ILC: Interoperable Lon Controller.
18. JACE: Java Application Control Engine
19. LAN: Local Area Network.
20. Modulating: Movement of a control device through an entire range of values, proportional to an infinitely variable input value.
21. Motorized: Control device with actuator.
22. NAC: Network Area Controller.
23. NC: Normally closed position of switch after control signal is removed or normally closed position of manually operated valves or dampers.
24. NO: Normally open position of switch after control signal is removed; or the open position of a controlled valve or damper after the control signal is removed; or the usual position of a manually operated valve.
25. OOT: Object Oriented Technology
26. OTN: Operational Technology Network
27. OSS: Operating System Server, host for system graphics, alarms, trends, etc.
28. Operator: Same as actuator.
29. PC: Personal Computer.
30. Peer-to-Peer: Mode of communication between controllers in which each device connected to network has equal status and each shares its database values with all other devices connected to network.
31. P: Proportional control; control mode with continuous linear relationship between observed input signal and final controlled output element.
32. PI: Proportional-Integral control, control mode with continuous proportional output plus additional change in output based on both amount and duration of change in controller variable (reset control).
33. PICS: BACnet Product Interoperability Compliance Statement.
34. PID: Proportional-Integral-Derivative control, control mode with continuous correction of final controller output element versus input signal based on proportional error, its time history (reset) and rate at which it's changing (derivative).
35. Point: Analog or discrete instrument with addressable database value.

36. PMI: Power Measurement Interface

37. POT: Portable Operator's Terminal

38. WAN: Wide Area Network.

39. WBI: Web Browser Interface

1.5 QUALITY ASSURANCE

A. The Master Systems Integrator shall have a full service DDC office within 50 miles of the job site. This office shall be staffed with applications engineers, software engineers and field technicians. This office shall maintain parts inventory and shall have all testing and diagnostic equipment necessary to support this work, as well as staff trained in the use of this equipment.

B. Single Source Responsibility of Supplier: The Master Systems Integrator shall be responsible for the complete installation and proper operation of the control system including compliance with the system's cybersecurity policies and procedures. Master Systems Integrator shall exclusively be in the regular and customary business of design, installation and service of computerized building management systems similar in size and complexity to the system specified. The Master Systems Integrator shall be the manufacturer of the primary DDC system components or shall have been the authorized representative for the primary DDC components manufacturer for at least 5 years. All control panels shall be assembled by the Control System Contractor in a UL-Certified 508A panel shop.

C. Equipment and Materials: Equipment and materials shall be cataloged products of manufacturers regularly engaged in the production and installation of HVAC control systems. Products shall be manufacturer's latest standard design and have been tested and proven in actual use.

1.6 CYBERSECURITY POLICIES AND PROCEDURES

A. Risk Management Objectives. Cybersecurity threats to Operational Technology systems are increasing dramatically with consequences that impact occupant safety, loss of productivity, equipment damage, tenant satisfaction, and access to business data assets. The cybersecurity policies and procedures contained within this specification are intended to minimize these risks while preparing the organization to manage risk on an ongoing basis including recovering from a disastrous incident.

B. Owner Policies: The following policies are to be finalized and updated with the Owner prior to project completion in conjunction with the MSI. In some cases, the policies apply to post-construction support during and after the warranty period.

1. User Authorization Policy. The MSI is authorized to add, modify and delete users to the Integration Platform subject to compliance with the Owner's Password, User Removal, and Administrative User policies. In addition, the MSI will submit the results of a six-month User Audit during the warranty period to confirm compliance with these policies.
2. Password Policy. All users are to adhere to the following requirements:
   a. Every user is to have a unique username and password.
   b. No shared accounts are permitted.
   c. Passwords are to be a minimum of 8 ASCII characters in length including spaces. Easy to remember phrases are recommended.
   d. Passwords should never be reused.
   e. Passwords must be changed on first log-in.
   f. This policy applies to both the Integration Platform application and the associated Operating System (OS).
3. User Removal Policy. The MSI will remove access within one business day by their users who are no longer employed or whose job responsibilities have changed such that they no longer require access to the Integration Platform.
4. User Audit Policy. The list of users for the Integration Platform will be audited every 6 months to ensure that only authorized users remain and that their privileges are consistent with the role they perform. Accounts used for normal operations should not be able to perform elevated actions.
5. Administrative Users Policy. The Integration Platform shall have a minimum of 2 System Administrators and a maximum of 4 with at least one of the administrators being an employee of the owner. System administration privileges should be granted to those individuals whose role requires this privilege in order to fully configure and program the system including creating new users.
6. Internet Management. Internet access to the Integration Platform is to be managed to the Owner's IT department.
7. Backup Policy. The Integration Platform server is to have a system image backup performed by an enterprise grade backup service including daily incremental changes. Backups are to be stored in a secure location with redundancy. Systems capable of backing up downstream devices configurations are to be configured to do so. If critical components such as a database are hosted on a separate server then those services must also be backed up according to this policy. The MSI and Owner will determine at the onset of the project whether backups are to be managed by the Owner or the MSI under a separate service agreement.
8. Integration Platform Server Management Policy. The MSI and Owner will determine at the onset of the project whether management of the

Integration Platform server is to be the responsibility of the Owner or the MSI under a separate service agreement. Management of this server includes compliance with the following:

a. The server will be located in a secure environment. This means only intended administrators of the system are to physically access the system. Keyboard, mouse and monitor should not be attached when not in use. Unauthorized users should not be able to plug in any USB device.

b. Anti-virus / anti-malware software will be installed with new signatures and updates applied automatically. Virus updates will be monitored to detect possible negative impacts to the operation of the Integration Server application software.

c. The operating system (OS) software must be running a fully supported version with all security patches installed.

d. The hardware platform will be monitored for processor, memory and storage performance including real-time alerting.

e. The only application software resident on the Integration Platform Server will be the IoT Server Software.

9. Remote Communications Policy. The Integration Platform is not to be publicly accessible over the Internet. Connections are to be made through a VPN or other remote management solution. Refer to the Operational Technology Network section of this specification for details on the remote management solution. Management of the VPN is by the Owner.

10. Disaster Recovery Policy. In the event of a critical failure or breach of the Integration Platform, the Owner and MSI will develop a disaster recovery plan that includes the following topics at a minimum:

a. Backup restore procedure

b. Manual operation

c. Communication plan to internal staff and occupants

d. Failure analysis

C. System Configuration Policies: The Integration Platform will comply with the cybersecurity configuration policies defined in section 2.9.

1. Application Software Policy
2. Password Policy
3. Administrative Users Policy
4. Guest Accounts
5. Manufacturer Default Accounts
6. Auto-lockout Policy
7. Auto-logoff Policy
8. Activity Logging Policy
9. Authentication Encryption

D. Subsystem Configuration Policies: Each of the systems that are to be integrated by the MSI are also to be configured according to the Configuration Policies by their respective Contractor.

INTEGRATION PLATFORM

PART 1 – GENERAL

1.1 INTENT

A. The intent of this section is to define the Integration of the Building Systems and Control Systems in to the Integration Platform as provided by the Master Systems Integrator (MSI). This platform will allow for a consistent graphical display of all systems shown in the overall topology.

B. Reference associated divisions 14, 21, 23, 26, 27, 28, 33 or others controlled with Integrated Automation.

C. Refer to drawing M- (insert drawing number here) for a diagrammatic representation of the System Architecture/Topology.

1.2 SUMMARY

A. This section describes the Master Systems Integrator's (MSI) scope for the Integration Platform for the project.

B. Coordinates the responsibilities of the Mechanical and Electrical trade contractors pertaining to control products or systems, furnished by each trade, that will be integrated by this Division.

C. All labor, material, equipment and software not specifically referred to herein or on the plans, that is required to meet the functional intent of this specification, shall be provided without additional cost to the owner.

D. It is the owner's goal to implement an O*pen System* that will allow products from various suppliers to be integrated into a unified system in order to provide flexibility for expansion, maintenance, and service of the system. The owner shall be the named license holder of all software associated with any and all incremental work on the project(s).

1.3 SYSTEM DESCRIPTION

The Integration Platform shall include, but not be limited to, the following components/sub systems in order to provide a fully functional platform required for integrating the systems shown on the system architecture/topology on drawing M-(insert drawing number here):

a. **Main Server w/Key Board and Mouse**
b. **Firewall and DNS**
c. **Server Rack**
d. **IoT Server Software Platform**
e. **Uninterruptable Power Supply (UPS)**
f. **Power Distribution Unit (PDU)**

A. The intent of this specification is to provide a system that is consistent with BMS systems throughout the owner's facilities running the Niagara 4 Framework.

B. The MSI shall furnish all labor, materials and equipment necessary for a complete and operating Integration Platform, utilizing Direct Digital Controls as shown on the drawings and as described herein. Drawings are diagrammatic only. All controllers furnished in this section shall communicate on a peer-to-peer bus over an open protocol bus (Examples: LonTalk, BACnet, MODBUS). The MSI shall submit a Data Plan that includes database standards, graphics, dashboards, data tagging and program guidelines for the Engineer’s review.

C. System architecture shall fully support a multi-vendor environment and be able to integrate third party systems via existing vendor protocols including, as a minimum, LonTalk, BACnet and MODBUS.

D. System architecture shall provide secure Web access using any of the current versions of Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome browsers from any computer on the owner's LAN.

E. All control devices furnished with this Section shall be programmable directly from the Niagara 4 Workbench embedded toolset upon completion of this project. The use of configurable or programmable controllers that require additional software tools or tools that require a specific Niagara 4 license brand to operate for post-installation maintenance shall not be acceptable.

F. Any control vendor that shall provide additional BMS server software shall be unacceptable. Only systems that utilize the Niagara 4 Framework shall satisfy the requirements of this section.

G. The integration platform server shall host all graphic files for the control system. All graphics and navigation schemes for this project shall match those that are on the Niagara 4 Framework server.

H. A laptop computer including engineering/programming software to modify Operating System Server BMS programs and graphics shall be included.

I. Owner shall receive all Administrator level login and passwords for engineering toolset at first training session. The Owner shall have full licensing and full access rights for all network management, operating system server, engineering and programming software required for the ongoing maintenance and operation of the BMS.

J. OPEN NIC STATEMENTS - All Niagara 4 software licenses shall have the following NiCS: "accept.station.in=*"; "accept.station.out=*"and "accept.wb.in=*"and "accept.wb.out=*". All open NIC statements shall follow Niagara Open NIC specifications.

K. All JACE hardware licenses and certificates shall be stored on local MicroSD memory card employing encrypted “safe boot” technology.

L. All products of the Integration Platform shall be provided with the following agency approvals. Verification that the approvals exist for all submitted products shall be provided on request, with the submittal package. Systems or products not currently offering the following approvals are not acceptable.

1. Federal Communications Commission (FCC), Rules and Regulations, Volume II -July 1986 Part 15 Class A Radio Frequency Devices.
2. FCC, Part 15, Subpart B, Class B
3. FCC, Part 15, Subpart C
4. FCC, Part 15, Subpart J, Class A Computing Devices.
5. UL 504 - Industrial Control Equipment.
6. UL 506 - Specialty Transformers.
7. UL 910 - Test Method for Fire and Smoke Characteristics of Electrical and Optical-Fiber Cables Used in Air-Handling Spaces.
8. UL 916 - Energy Management Systems All.
9. UL 1449 - Transient Voltage Suppression.
10. Standard Test for Flame Propagation Height of Electrical and Optical - Fiber Cables Installed Vertically in Shafts.
11. EIA/ANSI 232-E - Interface Between Data Technical Equipment and Data Circuit Terminal Equipment Employing Serial Binary Data Interchange.
12. EIA 455 - Standard Test Procedures for Fiber Optic Fibers, Cables, Transducers, Connecting and Terminating Devices.
13. IEEE C62.41- Surge Voltages in Low-Voltage AC Power Circuits.
14. IEEE 142 - Recommended Practice for Grounding of Industrial and Commercial Power Systems.
    a. NEMA 250 - Enclosures for Electrical Equipment.
15. NEMA ICS 1 - Industrial Controls and Systems.
16. NEMA ST 1 - Specialty Transformers.

17. NCSBC Compliance, Energy: Performance of control system shall meet or surpass the requirements of ASHRAE/IESNA 90.1-1999.
18. CE 61326
19. C-Tick
20. cUL

1.4 SUBMITTALS

A. Eight copies of shop drawings of the entire Integrated Platform shall be submitted and shall consist of a complete list of equipment and materials, including manufacturers catalog data sheets and installation instructions. Shop drawings shall also contain complete wiring and schematic diagrams, software descriptions, calculations, and any other details required to demonstrate that the system has been coordinated and will properly function as a system. Terminal identification for all control wiring shall be shown on the shop drawings.

B. Submittal shall also include a trunk cable schematic diagram depicting operator workstations, control panel locations and a description of the communication type, media and protocol. Though the Division 23 contractors shall provide these diagrams for their portions of work, the Master Systems Integrator shall be responsible for integrating those diagrams into the overall trunk cable schematic diagrams for the entire Virtual Local Area Network (VLAN).

C. Submittal shall also include a copy of each of the graphics developed for the Graphic User Interface including a flowchart (site map) indicating how the graphics are to be linked to one another for system navigation. The graphics are intended to be 80% - 90% complete at this stage with the only remaining changes to be based on review comments from the A/E design team and/or EMU.

D. Upon completion of the work, provide a complete set of ‘as-built’ drawings and application software on compact disk. Drawings shall be provided as AutoCAD™ or Visio™ compatible files. Eight copies of the ‘as-built’ drawings shall be provided in addition to the documents on compact disk. Division 23 and 26 contractors shall provide as-builts for their portions of work. The Division 25 contractor shall be responsible for as-builts pertaining to overall BMS architecture and network diagrams. All as built drawings shall also be installed into the integrated platform server in a dedicated directory.

1.5 PRE-INSTALLATION MEETINGS

A. Convene minimum two weeks prior to starting work of this section.

1.6 DELIVERY, STORAGE AND HANDLING

A. Maintain integrity of shipping cartons for each piece of equipment and control device through shipping, storage and handling as required to prevent equipment damage. Store equipment and materials inside and protected from weather.

1.7 JOB CONDITIONS

A. Cooperation with Other Trades: Coordinate the Work of this section with that of other sections to insure that the Work will be carried out in an orderly fashion. It shall be this Contractor's responsibility to check the Contract Documents for possible conflicts between his Work and that of other crafts in equipment location, pipe, duct and conduit runs, electrical outlets and fixtures, air diffusers and structural and architectural features.

1.8 SEQUENCING

A. Ensure that products of this section are supplied to affected trades in time to prevent interruption of construction progress.

PART 2 – PRODUCTS

2.1 MANUFACTURERS

A. Vykon Tridium Niagara Framework version N4

2.2 GENERAL

A. The Integration Platform shall be comprised of a network of interoperable, stand-alone digital controllers, a network area controller, graphics and programming and other control devices for a complete system as specified herein.

B. The installed system shall provide secure strong password access to all features, functions and data contained in the overall BMS.

2.3 OPEN, INTEROPERABLE, INTEGRATED ARCHITECTURE

A. The intent of this specification is to provide a peer-to-peer networked, stand-alone, distributed control system utilizing Open protocols in one open, interoperable system.

B. The supplied computer software shall employ object-oriented technology (OOT) for representation of all data and control devices within the system. Physical connection of any BACnet control equipment, such as chillers, shall be via Ethernet or IP.

C. All components and controllers supplied under this contract shall be true "peer-to-peer" communicating devices. Components or controllers requiring "polling" by a host to pass data shall not be acceptable.

D. The supplied system shall incorporate the ability to access all data using HTML5 enabled browsers without requiring proprietary operator interface and configuration programs or browser plug-ins. An Open Database Connectivity (ODBC) or Structured Query Language (SQL) compliant server database is required for all system database parameter storage. This data shall reside on the Operating System Server located in the Facilities Office on the LAN. Systems requiring proprietary database and user interface programs shall not be acceptable.

E. A hierarchical topology is required to assure reasonable system response times and to manage the flow and sharing of data without unduly burdening the customer's internal Intranet network. Systems employing a "flat" single tiered architecture shall not be acceptable.

1. Maximum acceptable response time from any alarm occurrence (at the point of origin) to the point of annunciation shall not exceed 5 seconds for network connected user interfaces.
2. Maximum acceptable response time from any alarm occurrence (at the point of origin) to the point of annunciation shall not exceed 60 seconds for remote or dial-up connected user interfaces.

2.4 IoT SERVER HARDWARE

The main server shall be mounted in the server rack in a location designated on the drawings. Server shall be provided with a key board and mouse.

A. Minimum Computer Configuration (Hardware Independent).

1. Central Server. Owner shall provide a dedicated BAS server with configuration that includes the following components as a minimum:
2. Processor: Intel Xeon CPU E3-1240 v5 3.5GHz (or better), compatible with dual- and quad-core processors. Xeon E3 processor or better.
3. Memory: 8 GB minimum or more recommended for the Windows 64-bit version.
4. Hard Drive: 2 TB minimum requirements.
5. Display: Video card and monitor capable of displaying 1024 x 768 pixel resolution or greater.
6. Windows server 2016 Standard.
7. Network Support: Ethernet adapter (10/100 Mb with RJ-45 connector).
8. Connectivity: Full-time high-speed ISP connection recommended for remote site access (i.e. T1, ADSL, cable modem).
9. Provide Keyboard and Mouse
10. Internet Explorer (10.0 or later) running on Microsoft 7+. No special software shall be required to be installed on the PCs used to access the BAS via a web browser

.

2.5 FIREWALL and DNS SERVER

A. Security appliance shall be provided with an integrated DNS server.

B. Security appliance in metal housing, with extended temperature range, SD card slot, up to 2 VPN tunnels, 2-click firewall for maximum ease of configuration, router with NAT/1:1 NAT

C. Routers with intelligent firewall, up to 200 Mbps of data throughput, Gigabit connectivity, SFP Slots Stateful. Inspection Firewall for maximum security and very simple configuration, interchangeable configuration memory

D. Basis of design shall be Phoenix Contact, Model FL MGUARD GT/GT-2700197

Approved vendors: Phoenix Contact, Cisco, BlueCat and InfoBlox

2.6 SERVER RACK

A. Shall be standard four post frame cabinets, wall mounted cabinets with 0.375" square mounting holes on front and back rails for a minimum of 42 standard EIA rack spaces. Provide with (25) 12-24 cage nuts and screws for square mounting holes.

B. Shall be UL Listed, designed to be self-standing with leveling feet, constructed of steel or aluminum, shall be firmly fastened to the floor, fastened to ladder rack for extra support, and properly grounded

C. Shall be provided with perforated, quick release, lockable front and rear doors.

D. Shall be provided with (2) locking, easy to remove side panels.

E. Shall be provided with vented top panel with cable access ports.

F. Shall be provided with fan kit.

G. Shall be provided with front and back vertical cable management on both sides.

H. Shall be provided with OSHPD approved seismic tie-down as required.

2.7 IoT SERVER SOFTWARE

The IoT Server Software shall allow multiple Niagara-based JACE controllers, along with other IP-based controllers, to be networked together through the OTN. This software shall provide real-time graphical information to standard Web-browser clients and provide server-level functions. These functions include centralized data logging/trending, alarming, tagging, archiving to external databases, alarming, dashboarding, system navigation, master scheduling, database management, and integration with other enterprise software applications through an XML interface (oBIX standard). Also, shall provide a comprehensive graphical engineering toolset for application development.

A. The BAS Contractor shall provide system software based on server/thin-client architecture, designed around the open standards of web technology. The BAS server shall communicate using Ethernet and TCP. Server shall be accessed using a web browser over Owner intranet and remotely over the Internet.

B. The intent of the thin-client architecture is to provide the operator(s) complete access to the BAS system via a web browser. The thin-client web browser Graphical User Interface (GUI) shall be browser and operating system agnostic, meaning it will support HTML5 enabled browsers without requiring proprietary operator interface and configuration programs or browser plug-ins. Microsoft, Firefox, and Chrome browsers (current released versions), and Windows as well as non-Window operating systems.

C. The BAS server software shall support at least the following server platforms (Windows 7, 8.1, Server 12). The BAS server software shall be developed and tested by the manufacturer of the system stand-alone controllers and network controllers/routers.

D. The web browser GUI shall provide a completely interactive user interface and shall provide a HTML5 experience that supports the following features as a minimum:

1. Trending.
2. Scheduling.
3. Electrical demand limiting.
4. Duty Cycling.
5. Downloading Memory to field devices.
6. Real time 'live' Graphic Programs.
7. Tree Navigation.
8. Parameter change of properties.
9. Set point adjustments.
10. Alarm / event information.
11. Configuration of operators.
12. Execution of global commands.
13. Add, delete, and modify graphics and displayed data.

E. Software Components: All software shall be the most current version. All software components of the BAS system software shall be provided and installed as part of this project. BAS software components shall include:

1. Server Software, Database and Web Browser Graphical User Interface.
~~2.~~ 5 Year Software Maintenance license. Labor to implement not included.
3. Embedded System Configuration Utilities for future modifications to the system and controllers.
4. Embedded Graphical Programming Tools.
5. Embedded Direct Digital Control software.
6. Embedded Application Software.

F. BAS Server Database: The BAS server software shall utilize a Java Database Connectivity (JDBC) compatible database such as: MS SQL 8.0, Oracle 8i or IBM DB2. BAS systems written to Non -Standard and/or Proprietary databases are NOT acceptable.

G. Thin Client - Web Browser Based: The GUI shall be thin client or browser based and shall meet the following criteria:

1. Web Browser's for PC's: Only the current released browser (Explorer/Firefox/Chrome) will be required as the GUI and a valid connection to the server network. No installation of any custom software shall be required on the operator's GUI workstation/client. Connection shall be over an intranet or the Internet.
2. Secure Socket Layers: Communication between the Web Browser GUI and BAS server shall offer encryption using 128-bit encryption technology within Secure Socket Layers (SSL). Communication protocol shall be Hyper-Text

Transfer Protocol (HTTP).

H. Web Browser Graphical User Interface

1. Web Browser Navigation: The Thin Client web browser GUI shall provide a comprehensive user interface. Using a collection of web pages, it shall be constructed to "feel" like a single application, and provide a complete and intuitive mouse/menu driven operator interface. It shall be possible to navigate through the system using a web browser to accomplish requirements of this specification. The Web Browser GUI shall (as a minimum) provide for navigation, and for display of animated graphics, schedules, alarms/events, live graphic programs, active graphic set point controls, configuration menus for operator access, reports and reporting actions for events.

2. Login: On launching the web browser and selecting the appropriate domain name or IP address, the operator shall be presented with a login page that will require a login name and strong password. Navigation in the system shall be dependent on the operator's role-based application control privileges.

3. Navigation: Navigation through the GUI shall be accomplished by clicking on the appropriate level of a navigation tree (consisting of an expandable and collapsible tree control like Microsoft's Explorer program) and/or by selecting dynamic links to other system graphics. Both the navigation tree and action pane shall be displayed simultaneously, enabling the operator to select a specific system or equipment and view the corresponding graphic. The navigation tree shall as a minimum provide the following views: Geographic, Network, Groups and Configuration.
   a. Geographic View shall display a logical geographic hierarchy of the system including: cities, sites, buildings, building systems, floors, equipment and objects.
   b. Groups View shall display Scheduled Groups and custom reports.
   c. Configuration View shall display all the configuration categories (Operators, Schedule, Event, Reporting and Roles).

4. Action Pane: The Action Pane shall provide several functional views for each subsystem specified. A functional view shall be accessed by clicking on the corresponding button:
   a. Graphics: Using graphical format suitable for display in a web browser, graphics shall include aerial building/campus views, color building floor-plans, equipment drawings, active graphic set point controls, web content and other valid HTML elements. The data on each graphic page shall automatically refresh.
   ~~b.~~ Dashboards: User customizable data using drag and drop HTML5 elements. Shall include Web Charts, Gauges, and other custom developed widgets for web browser. User shall have ability to save custom dashboards.

c. Search: User shall have multiple options for searching data based upon Tags. Associated equipment, real time data, Properties, and Trends shall be available in result.
d. Properties: Shall include graphic controls and text for the following: Locking or overriding objects, demand strategies, and any other valid data required for setup. Changes made to the properties pages shall require the operator to depress an 'accept/cancel' button.
e. Schedules: Shall be used to create, modify/edit and view schedules based on the systems hierarchy (using the navigation tree).
f. Alarms: Shall be used to view alarm information geographically (using the navigation tree), acknowledge alarms, sort alarms by category, actions and verify reporting actions.
g. Charting: Shall be used to display associated trend and historical data, modify colors, date range, axis and scaling. User shall have ability to create HTML charts through web browser without utilizing chart builder. User shall be able to drag and drop single or multiple data points, including schedules, and apply status colors for analysis.
h. Logic - Live Graphic Programs: Shall be used to display' live' graphic programs of the control algorithm, (micro block programming) for the mechanical/electrical system selected in the navigation tree.
i. Other actions such as Print, Help, Command, and Logout shall be available via a drop-down window.

I. Color Graphics: The Web Browser GUI shall make extensive use of color in the graphic pane to communicate information related to set points and comfort. Animated .gifs or .jpg, vector scalable, active set point graphic controls shall be used to enhance usability. Graphics tools used to create Web Browser graphics shall be non-proprietary and conform to the following basic criteria:

1. Display Size: The GUI workstation software shall graphically display in a minimum of 1024 by 768 pixels 24 bit True Color.
2. General Graphic: General area maps shall show locations of controlled buildings in relation to local landmarks.
3. Color Floor Plans: Floor plan graphics shall show heating and cooling zones throughout the buildings in a range of colors, as selected by Owner. Provide a visual display of temperature relative to their respective set points. The colors shall be updated dynamically as a zone's actual comfort condition changes.
4. Mechanical Components: Mechanical system graphics shall show the type of mechanical system components serving any zone through the use of a pictorial representation of components. Selected I/O points being controlled or monitored for each piece of equipment shall be displayed with the appropriate engineering units. Animation shall be used for rotation or moving mechanical components to enhance usability. .
5. Minimum System Color Graphics: Color graphics shall be selected and

displayed via a web browser for the following:

a. Each piece of equipment monitored or controlled including each terminal unit.
b. Each building.
c. Each floor and zone controlled.

J. Hierarchical Schedules: Utilizing the Navigation Tree displayed in the web browser GUI, an operator (with proper access credentials) shall be able to define a Normal, Holiday or Override schedule for an individual piece of equipment or room, or choose to apply a hierarchical schedule to the entire system, site or floor area. For example, Independence Day ' Holiday' for every level in the system would be created by clicking at the top of the geographic hierarchy defined in the Navigation Tree. No further operator intervention would be required and every control module in the system with would be automatically downloaded with the ' Independence Day' Holiday. All schedules that affect the system/area/equipment highlighted in the Navigation Tree shall be shown in a summary schedule table and graph.

1. Schedules: Schedules shall comply with the LonWorks and BACnet standards, (Schedule Object, Calendar Object, Weekly Schedule property and Exception Schedule property) and shall allow events to be scheduled based on:
   a. Types of schedule shall be Normal, Holiday or Override.
   b. A specific date.
   c. A range of dates.
   d. Any combination of Month of Year (1-12, any), Week of Month (1-5, last, any), Day of Week (M-Sun, Any).
   e. Wildcard (example, allow combinations like second Tuesday of every month).
2. Schedule Categories: The system shall allow operators to define and edit scheduling categories (different types of "things" to be scheduled; for example, lighting, HVAC occupancy, etc.). The categories shall include: name, description, icon (to display in the hierarchy tree when icon option is selected) and type of value to be scheduled.
3. Schedule Groups: In addition to hierarchical scheduling, operators shall be able to define functional Schedule Groups, comprised of an arbitrary group of areas/rooms/equipment scattered throughout the facility and site. For example, the operator shall be able to define an ' individual tenant' group - who may occupy different areas within a building or buildings. Schedules applied to the ' tenant group' shall automatically be downloaded to control modules affecting spaces occupied by the ' tenant group'.

4. Intelligent Scheduling: The control system shall be intelligent enough to automatically turn on any supporting equipment needed to control the environment in an occupied space. If the operator schedules an individual room in a VAV system for occupancy, for example, the control logic shall automatically turn on the VAV air handling unit, chiller, boiler and/or any other equipment required to maintain the specified comfort and environmental conditions within the room.
5. Partial Day Exceptions: Schedule events shall be able to accommodate a

time range specified by the operator (ex: board meeting from 6 pm to 9 pm overrides Normal schedule for conference room).

6. Schedule Summary Graph: The schedule summary graph shall clearly show Normal versus Holiday versus Override Schedules and the net operating schedule that results from all contributing schedules. Note: In case of priority conflict between schedules at the different geographic hierarchy, the schedule for the more detailed geographic level shall apply.

K. Alarms: Alarms associated with a specific system, area, or equipment selected in the Navigation Tree, shall be displayed in the Action Pane by selecting an ' Alarms' view. Alarms, and reporting actions shall have the following capabilities:

1. Alarms View: Each Alarm shall display an Alarms Category (using a different icon for each alarm category), date/time of occurrence, current status, alarm report and a bold URL link to the associated graphic for the selected system, area or equipment. The URL link shall indicate the system location, address and other pertinent information. An operator shall easily be able to sort events, edit event templates and categories, acknowledge or force a return to normal in the Events View as specified in this section.

2. Alarm Categories: The operator shall be able to create, edit or delete alarm categories such as HVAC, Maintenance, Fire, or Generator. An icon shall be associated with each alarm category, enabling the operator to easily sort through multiple events displayed.

3. Alarm Templates: Alarm template shall define different types of alarms and their associated properties. As a minimum, properties shall include a reference name, verbose description, severity of alarm, acknowledgement requirements, and high/low limit and out of range information.

4. Alarm Areas: Alarm Areas enable an operator to assign specific Alarm Categories to specific Alarm Reporting Actions. For example, it shall be possible for an operator to assign all HVAC Maintenance Alarm on the 1st floor of a building to email the technician responsible for maintenance. The Navigation Tree shall be used to setup Alarm Areas in the Graphic Pane.

5. Alarm Time/Date Stamp: All events shall be generated at the DDC control module level and comprise the Time/Date Stamp using the standalone control module time and date.

6. Alarm Configuration: Operators shall be able to define the type of Alarm generated per object. A ' network' view of the Navigation Tree shall expose all objects and their respective Alarm Configuration. Configuration shall include assignment of Alarm, type of Acknowledgement and notification for return to normal or fault status.

7. Alarm Summary Counter: The view of Alarm in the Graphic Pane shall provide a numeric counter, indicating how many Alarms are active (in

alarm), require acknowledgement and total number of Alarms in the BAS Server database.

8. Alarm Auto-Deletion: Alarms that are acknowledged and closed shall be auto-deleted from the database and archived to a text file after an operator defined period.

9. Alarm Reporting Actions: Alarm Reporting Actions specified shall be automatically launched (under certain conditions) after an Alarm is received by the BAS server software. Operators shall be able to easily define these Reporting Actions using the Navigation Tree and Graphic Pane through the web browser GUI. Reporting Actions shall be as follows:

   a. Print: Alarm information shall be printed to the BAS server's PC or a networked printer.
   b. Email: Email shall be sent via any POP3-compatible e-mail server (most Internet Service Providers use POP3). Email messages may be copied to several email accounts. Note: Email reporting action shall also be used to support alphanumeric paging services, where email servers support pagers.
   c. File Write: The ASCII File write reporting action shall enable the operator to append operator defined alarm information to any alarm through a text file. The alarm information that is written to the file shall be completely definable by the operator. The operator may enter text or attach other data point information (such as AHU discharge temperature and fan condition upon a high room temperature alarm).
   d. Write Property: The write property reporting action updates a property value in a hardware module.
   e. SNMP: The Simple Network Management Protocol (SNMP) reporting action sends an SNMP trap to a network in response to receiving an alarm.
   f. Run External Program: The Run External Program reporting action launches specified program in response to an event.

L. Trends: As system is engineered, all points shall be enabled to trend. Trends shall both be displayed and user configurable through the Web Browser GUI. Trends shall comprise analog, digital or calculated points simultaneously. A trend log's properties shall be editable using the Navigation Tree and Graphic Pane.

1. Viewing Trends: The operator shall have the ability to view trends by using the Navigation Tree and selecting a Trends button in the Graphic Pane. The system shall allow y- and x-axis maximum ranges to be specified and shall be able to simultaneously graphically display multiple trends per graph.
2. Local Trends: Trend data shall be collected locally by Multi-Equipment/Single Equipment general-purpose controllers, and periodically

uploaded to the BAS server if historical trending is enabled for the object. Trend data, including run time hours and start time date shall be retained in non-volatile module memory. Systems that rely on a gateway/router to run trends are NOT acceptable.

3. Resolution. Sample intervals shall be as small as one second. Each trended point will have the ability to be trended at a different trend interval. When multiple points are selected for displays that have different trend intervals, the system will automatically scale the axis.
4. Dynamic Update. Trends shall be able to dynamically update at operator-defined intervals.
5. Zoom/Pan. It shall be possible to zoom-in on a particular section of a trend for more detailed examination and ' pan through' historical data by simply scrolling the mouse.
6. Numeric Value Display. It shall be possible to pick any sample on a trend and have the numerical value displayed.
7. Copy/Paste. The operator shall have the ability to pan through a historical trend and copy the data viewed to the clipboard using standard keystrokes (i.e. CTRL+C, CTRL+V).

M. Security Access: Systems that Security access from the web browser GUI to BAS server shall require a Login Name and Strong Password. Access to different areas of the BAS system shall be defined in terms of Role-Based Access Control privileges as specified:

1. Roles: Roles shall reflect the actual roles of different types of operators. Each role shall comprise a set of ' easily understood English language' privileges. Roles shall be defined in terms of View, Edit and Function Privileges.
   a. View Privileges shall comprise: Navigation, Network, and Configuration Trees, Operators, Roles and Privileges, Alarm/Event Template and Reporting Action.
   b. Edit Privileges shall comprise: Set point, Tuning and Logic, Manual Override, and Point Assignment Parameters.
   c. Function Privileges shall comprise: Alarm/Event Acknowledgement, Control Module Memory Download, Upload, Schedules, Schedule Groups, Manual Commands, Print and Alarm/Event Maintenance.

2. Geographic Assignment of Roles: Roles shall be geographically assigned using a similar expandable/collapsible navigation tree. For example, it shall be possible to assign two HVAC Technicians with similar competencies (and the same operator defined HVAC Role) to different areas of the system.

N. Graphical Programming

1. The system software shall include a Graphic Programming Language (GPL) for all DDC control algorithms resident in all control modules. Any system that does not use a drag and drop method of graphical icon programming shall not be accepted. All systems shall use a GPL method used to create a sequence of operations by assembling graphic microblocks that represent each of the commands or functions necessary to complete a control

sequence. Microblocks represent common logical control devices used in conventional control systems, such as relays, switches, high signal selectors etc., in addition to the more complex DDC and energy management strategies such as PID loops and optimum start. Each microblock shall be interactive and contain the programming necessary to execute the function of the device it represents.

2. Graphic programming shall be performed while on screen and using a mouse; each microblock shall be selected from a microblock library and assembled with other microblocks necessary to complete the specified sequence. Microblocks are then interconnected on screen using graphic "wires," each forming a logical connection. Once assembled, each logical grouping of microblocks and their interconnecting wires then forms a graphic function block which may be used to control any piece of equipment with a similar point configuration and sequence of operation.

3. Graphic Sequence: The clarity of the graphic sequence shall be such that the operator has the ability to verify that system programming meets the specifications, without having to learn or interpret a manufacturer's unique programming language. The graphic programming shall be self-documenting and provide the operator with an understandable and exact representation of each sequence of operation.

4. GPL Capabilities: The following is a minimum definition of the capabilities of the Graphic Programming software:
   a. Function Block (FB): Shall be a collection of points, microblocks and wires which have been connected together for the specific purpose of controlling a piece of HVAC equipment or a single mechanical system.
   b. Logical I/O: Input/Output points shall interface with the control modules in order to read various signals and/or values or to transmit signal or values to controlled devices.
   c. Microblocks: Shall be software devices that are represented graphically and may be connected together to perform a specified sequence. A library of microblocks shall be submitted with the control contractors bid.
   d. Wires: Shall be Graphical elements used to form logical connections between microblocks and between logical I/O.
   e. Reference Labels: Labels shall be similar to wires in that they are used to form logical connections between two points. Labels shall form a connection by reference instead of a visual connection, i.e. two points labeled 'A' on a drawing are logically connected even though there is no wire between them.
   f. Parameter: A parameter shall be a value that may be tied to the input of a microblock.
   g. Properties: Dialog boxes shall appear after a microblock has been inserted which has editable parameters associated with it. Default parameter dialog boxes shall contain various editable and non-editable fields, and shall contain 'push buttons' for the purpose of selecting default parameter settings.
   h. Icon: An icon shall be graphic representation of a software program.

Each graphic microblock has an icon associated with it that graphically describes its function.

i. Menu-bar Icon: Shall be an icon that is displayed on the menu bar on the GPL screen, which represents its associated graphic microblock.

j. Live Graphical Programs: The Graphic Programming software shall support a ' live' mode, where all input/output data, calculated data and set points shall be displayed in a ' live' real-time mode.

2.7 TAGGING

The purpose of a data modeling standard is to provide a consistent, standardized methodology for naming and describing data points associated with the the IoT and Integrated Automation Topology for this project. This includes the facility automation systems, equipment systems, energy metering systems, other smart devices including mobile assets, and associated descriptive information known as metadata.

A. The MSI shall coordinate with the site Systems Integrator (SI) to insure that all equipment, controllers and devices and data points are tagged per Appendix-A and Appendix-B (Niagara Station Object Structure Guidelines) in division 25 of this specification as part of the Integration scope. Appendix-A and Appendix-B

B. The Project Haystack standard shall be used for this project paired with a Building Location tagging Library. The building location tagging library shall include *Compass Directional,* which will be bi-directional (ie, NE, SW, NW, SE) and the *Building Level* (ie. 1st floor, 2nd floor, 3rd floor, etc..). The project haystack tagging libraries are embedded within the Niagara Software Platform. The building location tagging library shall be developed to work seamlessly with haystack and operate as an integrated solution for tagging.

C. Project-Haystack facilitates “mapping” of Haystack semantic tagging with other relevant standards. The Project Haystack data modeling standard for Buildings and Equipment systems shall use a simple metamodel based on the broadly accepted concept of “tags” shown below.

1. Relations: When using Appendix-B (Niagara Station Object Structure Guidelines), note that the “relations” column is for reference only and the MSI shall be responsible for documenting their process using the Appendix- A spreadsheet. Methodology for relations shall be reviewed and approved by the owner.
2. Tags: Tags are name/value pairs, associated with entities like AHUs, electric meters, etc. Tags are simple and dynamic, add structure, and provide the flexibility needed to establish standardized models of diverse systems and equipment. Tags are a modeling technique that allows easy customization of data models on a per-task, per-project or per-equipment basis, while

retaining the ability to be interpreted by external applications using a standard, defined methodology and vocabulary. Tags shall support the definition of the following essential data elements:

a. Entity: An Entity is an abstraction for a physical object in the real world. Entities include sites, facilities, equipment, sensor points, weather stations, etc. In software systems, an entity might be a modeled as a record in a database, an object in a building automation system, or maybe just a row in a csv file or spreadsheet.
b. Id: The id tag is used to model the unique identifier of an entity in a system using a Ref value type. Ref value types are determined by individual application. The scope of an entity may be undefined, but must be unique within a given system or project. This identifier may be used by other entities to cross-reference entities, associations, and systems.
c. Dis: The dis tag is used with entities to define display text used to describe an entity. Dis values are intended to be short (less than 30 or 40 characters), but fully descriptive of the entity for a human user.

3. Tag Kinds: The standard shall provide the following permitted tag value types:
   a. Marker: this tag type is merely a marker annotation with no meaningful value. Marker tags are used to indicate a "type" or "is-a" relationship.
   b. Bool: boolean "true" or "false".
   c. Number: integer or floating point number annotated with a Unit of Measurement, where ideally, units of measure are prescribed for various tasks.
   d. Str: a string of Unicode characters.
   e. Uri: a Unversal Resource Identifier.
   f. Ref: reference to another entity. The Project Haystack specification does not currently prescribe specific identities or reference mechanisms, but should be used to cross link entities. Refs are formatted with a leading "@" and require a specific subset of ASCII characters be used: a-z, A-Z, 0-9, underbar, colon, dash, or dot.
   g. Bin: a binary blob with a MIME type formatted as Bin(text/plain)
   h. Date: an ISO 8601 date as year, month, day: 2011-06-07.
   i. Time: an ISO 8601 time as hour, minute, seconds: 09:51:27.354.
   j. DateTime: an ISO 8601 timestamp followed by timezone name: 2011-06-07T09:51:27-04:00 New_York 2012-09-29T14:56:18.277Z UTC

4. Standard Library of Tags and Library Extensibility: The Project Haystack data modeling standard shall provide a comprehensive library of standard tags to address common equipment, building systems, and devices types. The standards development community shall engage in an open discussion forum to enable industry experts and interested parties to discuss, submit, fine-tune and eventually approve additional tags or standard schemas to address equipment, systems, and applications of numerous types. The open forum process shall be transparent to enable continued development of a

taxonomy that will enable semantic understanding of facilities engineering data across and outside of the industry.

5. REST API: The Project Haystack data modeling standard shall provide a documented Representational State Transfer, Application Programming Interface (REST API) to define a simple mechanism to exchange “tagged” data over web services.
   a. REST servers are programmed to implement a set of ops or operations. An operation is a uri that receives a request and returns a response. Standard operations are defined to query databases, setup subscriptions, or read/write histories of time-series data. Operations are pluggable so vendors can enhance open REST interfaces with customized, value-added functionality for their own business purposes.
   b. Both requests and responses are modeled as grids. Grids are encoded using standard Multipurpose Internet Mail Extensions (MIME) types for grid serialization, may be pluggable using HTTP content negotiation, and other standardized web service protocols.
   c. The Project Haystack REST API utilizing the “ops” design is more akin to a Remote Procedure Call (RPC) model, but the term REST is used to distinguish the design from traditional WS-* web services that use Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), and other Internet standards although the current design could easily tunnel through those technologies

6. Applications: The goal of the Project Haystack data modeling standard is to ensure consistent modeling of building systems, devices and associated data. The following application requirements outline the use of the modeling standard in applications related to buildings, energy, and facility management.

7. Minimum Model Requirements: The Haystack Project implementation shall utilize defined data modeling tags to create an expanding, and coherent model with the following minimum items, hierarchy and relationships when used in facilities-oriented applications.

8. Sites: Including display name, description, size (area) as a minimum. References to Internet-available weather stations are highly recommended, as are creating tags to represent other relevant characteristics of a Site such as the year the site was constructed, facility usage type, occupancy class, schedule(s) of operation, building systems type (e.g., packaged or central HVAC).

9. Equipment: Including standardized associations with sites via id reference and display name as a minimum. Equipment and software vendors, model

numbers, year of installation, and similar descriptive meta data are also recommended.

10. Points: Including standardized associations with sites and equipment via id reference, units of measure as a minimum. Where possible, ranges of acceptable values are recommended.

11. Exposing the Project Haystack Model via REST API: Software and web service applications, including control system devices will expose the model definitions described above using the Project Haystack REST API published as part of the Project Haystack standard, openly accessible and kept up to date at http://project-haystack.org/doc/Rest

12. Software Reference Implementations: The Project-haystack standard shall provide a reference implementation in Java, providing sample code for implementation of the Haystack REST protocol in software applications.

13. Open Source Modules for Commercially Available Products: The Project Haystack Community has developed, and makes available, a comprehensive implementation of the Haystack protocol in the form of a software module for use with NiagaraAX-based systems. The module, known as NHaystack, is licensed under the Academic Free License ("AFL") v. 3.0. Public access to the NHaystack software module shall be maintained via the project-haystack.org site.

14. Open Source: The Project Haystack Facilities Engineering Data Modeling Standard for Smart Device Data modeling methodology, standards, supporting documentation and reference implementations shall be available via an open source license at no cost.
    a. The open source license shall use the Open Source Initiative Academic Free License 3.0 model. Full details on the terms of the license are available at: http://project-haystack.org/doc/License and http://opensource.org/licenses/AFL-3.0

2.9 CYBERSECURITY CONFIGURATION POLICIES

A. Application Software Policy. The Integration Platform application software version shall be fully supported by the manufacturer and updated to the most recent patch level.

B. Password Policy. All users will be configured according to the Owner’s Password Policy.

C. Administrative Users Policy. All users will be configured according to the Owner’s Administrative Users Policy.

D. Guest Accounts. Guest accounts will be disabled if available or removed if possible.

E. Manufacturer Default Accounts. Manufacturer default users are to be removed and replaced with the system owner admin account before putting the system into service. If not possible the manufacturer passwords are to be changed before putting the system into service.

F. Auto-lockout Policy. The auto-lockout feature is to be enabled with a maximum of 10 log-on attempts.

G. Auto-logoff Policy. The system shall automatically log off users after 30 minutes of inactivity.

H. Activity Logging Policy. The system will record all user activity for a minimum of one week locally and the activity logs archived to a secure central location.

I. Authentication Encryption. All network-based authentication must be strongly encrypted.

2.10 POWER DISTRIBUTION UNIT (PDU)

Provide a *switched type* power distribution unit designed to provide power to multiple devices. The PDU shall be an intelligent network-grade power distribution that can control outlets individually in order to perform functions such as scheduled re-boots or maintenance shut downs. The unit shall also include an integrated network management system (NMS) built into the PDU. The NMS shall allow the administrator to perform operational tasks such as load monitoring, event logging and scheduled power cycling of the outlets and load shedding. The PDU shall also include the following features:

2. A digital meter that shows load and voltage
3. Ethernet SNMP connection for remote monitoring and control of outlets

Manufacturers: Subject to compliance with requirements, provide products and services by one of the following:

a. Basis of design: CyberPower PDU81001
b. Other Owner Approved Equal

2.11 UNINTERRUPTABLE POWER SUPPLY (UPS)

PART 1 – GENERAL

1.1 SUMMARY

A. Section Includes:

1. Three-phase, on-line, double-conversion, static-type, UPS units with the

following features:

a. Surge suppression.

b. Rectifier-charger.

c. Inverter.

d. Static bypass transfer switch.

e. Maintenance Bypass/Isolation switch cabinet.

f. Battery and battery disconnect device.

g. Battery monitoring.

h. Output circuit breaker.

B. Related Sections:

1. Division 26 Section “Power Distribution Units (PDU)”.

1.2 SUBMITTALS

A. Product Data: For each type of product indicated. Include data on features, components, ratings, and performance.

B. Shop Drawings: Detail equipment assemblies and indicate dimensions, weights, components, and location and identification of each field connection. Show access, workspace, and clearance requirements; details of control panels; and battery arrangement. Include wiring diagrams.

C. Factory Test Reports: Comply with specified requirements.

D. Field quality-control reports.

E. Operation and Maintenance Data:

F. Warranties.

1.3 QUALITY ASSURANCE

A. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70 and marked for intended location and application.

B. UL Compliance: Listed and labeled under UL 1778.

C. NFPA Compliance: Mark UPS components as suitable for installation in computer rooms according to NFPA 75.

D. Comply with Cleveland Clinic Design Standards and ITD Standards.

1.4 WARRANTY

A. Special Battery Warranties: Specified form in which manufacturer and Installer agree to repair or replace UPS system storage batteries that fail in materials or workmanship within specified warranty period.

1. Warranted Cycle Life for Premium Valve-Regulated, Lead-calcium Batteries: Equal to or greater than that represented in manufacturer's published table, including figures corresponding to the following, based on annual average battery temperature of 77 deg F (25 deg C):

Discharge Rate	Discharge Duration	Discharge End Voltage	Cycle Life
8 hours	8 hours	1.67	40 cycles
30 minutes	30 minutes	1.67	125 cycles
15 minutes	1.5 minutes	1.67	750 cycles

B. Special UPS Warranties: Specified form in which manufacturer and Installer agree to repair or replace components that fail in materials or workmanship within special warranty period.

1. Special Warranty Period: one year from date of Substantial Completion.

PART 2 - PRODUCTS

2.1 OPERATIONAL REQUIREMENTS

A. Automatic operation includes the following:

1. Normal Conditions: Load is supplied with power flowing from the normal power input terminals, through the rectifier-charger and inverter, with the battery connected in parallel with the rectifier-charger output.

2. Abnormal Supply Conditions: If normal supply deviates from specified and adjustable voltage, voltage waveform, or frequency limits, the battery supplies energy to maintain constant, regulated inverter power output to the load without switching or disturbance.

3. If normal power fails, energy supplied by the battery through the inverter continues supply-regulated power to the load without switching or disturbance.

4. When power is restored at the normal supply terminals of the system, controls
automatically synchronize the inverter with the external source before transferring the load. The rectifier-charger then supplies power to the load

through the inverter and simultaneously recharges the battery.

5. If the battery becomes discharged and normal supply is available, the rectifier-charger charges the battery. On reaching full charge, the rectifier-charger automatically shifts to float-charge mode.

6. If any element of the UPS system fails and power is available at the normal supply terminals of the system, the static bypass transfer switch switches the load to the normal ac supply circuit without disturbance or interruption.
7. If a fault occurs in the system supplied by the UPS, and current flows in excess of the overload rating of the UPS system, the static bypass transfer switch operates to bypass the fault current to the normal ac supply circuit for fault clearing.

8. When the fault has cleared, the static bypass transfer switch returns the load to the UPS system.

9. If the battery is disconnected, the UPS continues to supply power to the load with no degradation of its regulation of voltage and frequency of the output bus.

B. Manual operation includes the following:

1. Turning the inverter off causes the static bypass transfer switch to transfer the load directly to the normal ac supply circuit without disturbance or interruption.

C. Maintenance Bypass/Isolation Switch Operation: Switch is interlocked so it cannot be operated unless the static bypass transfer switch is in the bypass mode. Device provides manual selection among the three conditions in subparagraphs below without interrupting supply to the load during switching:

1. Full Isolation: Load is supplied, bypassing the UPS. Normal UPS ac input circuit, static bypass transfer switch, and UPS load terminals are completely disconnected from external circuits.

2. Maintenance Bypass: Load is supplied, bypassing the UPS. UPS ac supply terminals are energized to permit operational checking, but system load terminals are isolated from the load.

3. Normal: Normal UPS ac supply terminals are energized and the load is supplied through either the static bypass transfer switch and the UPS rectifier-charger and inverter, or the battery and the inverter.

D. Environmental Conditions: The UPS shall be capable of operating continuously in the following environmental conditions without mechanical or electrical damage or degradation of operating capability, except battery performance.

1. Ambient Temperature for Battery: 77+/- 9 Deg F (25 +/- 5 deg C).

2. Relative Humidity: 0 to 95 percent, non-condensing.
3. Altitude: Sea level to 4000 feet (1220 m).

2.2 PERFORMANCE REQUIREMENTS

A. The UPS shall perform as specified in this article while supplying rated full-load current, composed of any combination of linear and nonlinear load, up to 100 percent nonlinear load with a load crest factor of 3.0, under the following conditions or combinations of the following conditions:

1. Inverter is switched to battery source.

2. Steady-state ac input voltage deviates up to plus or minus 10 percent from nominal voltage.

3. Steady-state input frequency deviates up to plus or minus 5 percent from nominal frequency.

4. THD of input voltage is 15 percent or more with a minimum crest factor of 3.0, and the largest single harmonic component is a minimum of 5 percent of the fundamental value.

5. Load is 100 percent unbalanced continuously.

B. Minimum Duration of Supply: If battery is sole energy source supplying rated full UPS load current at 90 percent power factor, duration of supply is 11 minutes.

C. Input Voltage Tolerance: System steady-state and transient output performance remains within specified tolerances when steady-state ac input voltage varies plus 15, minus 20 percent from nominal voltage.

D. Overall UPS Efficiency: Equal to or greater than 94 percent at 100 percent load, 75 percent load, and 50 percent load.

E. Maximum Acoustical Noise: 68 dBa, emanating from any UPS component under any condition of normal operation, measured 3 feet from nearest surface of component enclosure.

F. Maximum Energizing Inrush Current: Six times the full-load current.

G. Maximum AC Output-Voltage Regulation for Loads up to 100 Percent Unbalanced: Plus or minus 2 percent over the full range of battery voltage.

H. Output Frequency: 60 Hz, plus or minus 0.5 percent over the full range of input voltage, load, and battery voltage.

I. Limitation of harmonic distortion of input current to the UPS shall be as follows:

1. Description: Either a tuned harmonic filter or an arrangement of rectifier-charger

circuits shall limit THD to 5 percent, maximum, at rated full UPS load current, for power sources with X/R ratio between 2 and 30.

J. Maximum Harmonic Content of Output-Voltage Waveform: 1% total harmonic distortion (THD) for linear loads, 5% THD for 100% non linear loads crest factor of 3.1 without m\kW/kVA derating.

K. Minimum Overload Capacity of UPS at Rated Voltage: 110% for 60 minutes, 125 percent for 10 minutes, and 150 percent for 60 seconds in all operating modes.

L. Maximum Output-Voltage Transient Excursions from Rated Value: For the following instantaneous load changes, stated as percentages of rated full UPS load, voltage shall remain within stated percentages of rated value and recover to, and remain within, plus or minus 2 percent of that value within 100 ms:

1. 50 Percent: Plus or minus 5 percent.
2. 100 Percent: Plus or minus 5 percent.
3. Loss of AC Input Power: Plus or minus 1 percent.
4. Restoration of AC Input Power: Plus or minus 1 percent.

M. Input Power Factor: 0.70 lagging to 1.0 when supply voltage and current are at nominal rated values and the UPS is supplying rated full-load current.

N. EMI Emissions: Comply with FCC Rules and Regulations and with 47 CFR 15 for Class A equipment.

2.3 UPS SYSTEMS

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. Eaton “Power Ware”.
2. LTI Power Systems Inc.
3. Liebert Corporation “NX” series.

B. Electronic Equipment: Solid-state devices using hermetically sealed, semiconductor elements. Devices include rectifier-charger, inverter, static bypass transfer switch, and system controls.

C. Enclosures: Comply with NEMA 250, Type 1, unless otherwise indicated.

D. Control Assemblies: Mount on modular plug-ins, readily accessible for maintenance.

E. Surge Suppression: Protect rectifier-charger, inverter, controls, and output components. Input surges should be sustained without damage per criteria listed in IEC 1000-4-5.

2.4 RECTIFIER-CHARGER

A. Capacity: Adequate to supply the inverter during rated full output load conditions and simultaneously recharge the battery from fully discharged condition to 95 percent of full charge within 10 times the rated discharge time for duration of supply under battery power at full load.

B. Output Ripple: Limited by output filtration to less than 0.5 percent of rated current peak-to-peak.

C. Control Circuits: Immune to frequency variations within rated frequency ranges of normal and emergency power sources. Rectifier restarts and walks in and gradually assumes the battery recharge and inverter loads. Adjustable up to 30 seconds and is visibly displayed on the front panel.

D. Battery Float-Charging Conditions: Comply with battery manufacturer's written instructions for battery terminal voltage and charging current required for maximum battery life.

2.5 INVERTER

A. Description: Pulse-width modulated, utilizing IGBT’s with sinusoidal output.

2.6 OUTPUT CIRCUIT BREAKER

A. Single output circuit breaker.

B. Thermal magnetic, three-pole, molded case circuit breaker:

1. Internal to system cabinet.
2. Full size.

C. Rating: 100% Continuous duty at rated full UPS load current, sized per Manufacturer’s recommendations.

2.7 STATIC BYPASS TRANSFER SWITCH

A. Description: Solid-state switching device providing uninterrupted transfer. A contactor or electrically operated circuit breaker automatically provides electrical isolation for the switch.

B. Switch Rating: Continuous duty at the rated full UPS load current, minimum.

2.8 BATTERY

A. Description: Valve-regulated, recombinant, lead-calcium units, factory assembled in an isolated compartment of UPS cabinet, complete with battery disconnect switch.

1. Arrange for drawout removal of battery assembly from cabinet for testing and inspecting.

B. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. C&D Technologies, Inc.; Standby Power Division.
2. Enersys.

2.9 MAINTENANCE BYPASS/ISOLATION SWITCH

A. Description: Manually operated switch or arrangement of switching devices with mechanically actuated contact mechanism arranged to route the flow of power to the load around the rectifier charger, inverter, and static bypass transfer switch.

1. Switch shall be electrically and mechanically interlocked to prevent interrupting power to the load when switching to bypass mode.

2. Switch shall electrically isolate other UPS components to permit safe servicing.

B. Comply with NEMA PB 2 and UL 891.

C. Switch Rating: Continuous duty at rated full UPS load current.
D. Mounting Provisions: Matching system cabinet.
E. Key interlock requires unlocking maintenance bypass/isolation switch before switching from normal position with key that is released only when the UPS is bypassed by the static bypass transfer switch. Lock is designed specifically for mechanical and electrical component interlocking.

2.10 CONTROLS AND INDICATIONS

A. Description: Group displays, indications, and basic system controls on a common control panel on front of UPS enclosure.

B. Minimum displays, indicating devices, and controls include those in lists below. Provide sensors, transducers, terminals, relays, and wiring required to support listed items. Alarms include audible signals and visual displays.

C. Indications: Plain-language messages on a digital LCD. [edit list for project requirements]

1. Quantitative indications shall include the following:

a. Input voltage, each phase, line to line.
b. Input current, each phase, line to line.
c. Bypass input voltage, each phase, line to line.

d. Bypass input frequency.
e. System output voltage, each phase, line to line.
f. System output current, each phase.
g. System output frequency.
h. DC bus voltage.
i. Battery current and direction (charge/discharge).
j. Elapsed time discharging battery.
k. Time remaining on discharge.
2. Basic status condition indications shall include the following:
a. Normal operation.
b. Load-on bypass.
c. Load-on battery.
d. Inverter off.
e. Alarm condition.

2. Alarm indications shall include the following:

a. Bypass ac input overvoltage or undervoltage.
b. Bypass ac input overfrequency or underfrequency.
c. Bypass ac input and inverter out of synchronization.
d. Bypass ac input wrong-phase rotation.
e. Bypass ac input single-phase condition.
f. Battery system alarm.
g. Control power failure.
h. Fan failure.
i. UPS overload.
j. Battery-charging control faulty.
k. Input overvoltage or undervoltage.
l. Input circuit breaker tripped.
m. Input wrong-phase rotation.
n. Approaching end of battery operation.
o. Battery undervoltage shutdown.
p. Maximum battery voltage.
q. Inverter fuse blown.
r. Inverter inductor overtemperature.
s. Inverter overtemperature.
t. Inverter output overvoltage or undervoltage.
u. UPS overload shutdown.
v. Inverter output contactor open.
w. Inverter current limit.

3. Controls shall include the following:

a. Inverter on-off.
b. UPS start.
c. Battery test.
d. Alarm silence/reset.
e. Output-voltage adjustment.

D. Dry-form "C" contacts shall be available for remote indication of the following conditions:

1. UPS on battery.
2. UPS on-line.
3. UPS load-on bypass.
4. UPS in alarm condition.
5. UPS off (maintenance bypass closed).

2.11 EMERGENCY MODULE OFF

A. Emergency-Power-Off Switch: Capable of local operation by means of activation by red pushbutton under protective cover on UPS module control panel.
B. Provisions for a remote emergency power off function by means of activation by external dry contacts which completely removes power from the critical bus.

2.13 MAINTENANCE BYPASS/ISOLATION SWITCH CABINET

A. Description: Manually operated switch or arrangement of switching devices with mechanically actuated contact mechanism arranged to route the flow of power to the load around the rectifiercharger, inverter, and static bypass transfer switch.
1. Switch shall be electrically and mechanically interlocked to prevent interrupting power to the load when switching to bypass mode.
2. Switch shall electrically isolate other UPS components to permit safe servicing.

B. Switch Rating: Continuous duty at rated full UPS load current.

C. Mounting Provisions: Matching cabinet for right side location see drawings and one-line for 2 breaker requirement and voltages.

D. Key interlock requires unlocking maintenance bypass/isolation switch before switching from a normal position with key that is released only when the UPS is bypassed by the static bypass transfer switch. Lock is designed specifically for mechanical and electrical component interlocking.

2.14 BASIC BATTERY MONITORING

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. Albercorp.

B. Battery compartment high-temperature detector initiates an alarm when a temperature greater than 75 deg C occurs within the compartment.

C. Cell/Jar DC Resistance, and Inter-tier Resistance readings.

D. The BMS hardware shall be integrated into the battery cabinet and installed at the manufacturer’s factory. Diagnostic monitoring software provided for installation on customer provided PC/ server with monitor display.

E. The BMS input AC power shall wire directly from a fused output in the UPS.

F. Annunciation of Alarms: through BMS Diagnostic software at Alber system central monitoring point sent via Ethernet network connection.

G. Auxiliary contacts for connection to Site Scan monitoring as described in earlier paragraphs.

2.15 SOURCE QUALITY CONTROL

A. Factory test complete UPS system before shipment. Use simulated battery testing. Include the following:

1. Test and demonstration of all functions, controls, indicators, sensors, and protective devices.
2. Full-load test.
3. Transient-load response test.
4. Overload test.
5. Power failure test.

B. Report test results.

PART 3 - EXECUTION

3.1 INSTALLATION

A. Equipment Mounting: Examine UPS system before installation. Reject equipment that is

moisture damaged or physically damaged. Examine elements and surfaces to receive UPS for
compliance with installation tolerances and other conditions affecting performance of the Work
Comply with requirements for installation as specified by supplier.

B. Maintain minimum clearances and workspace at equipment according to manufacturer's written
instructions and NFPA 70.

C. Connections: Interconnect system components. Make connections to supply and load circuits
according to manufacturer's wiring diagrams unless otherwise indicated.

D. Grounding Separately Derived Systems: If not part of a listed power supply for a dataprocessing room, comply with NFPA 70 requirements for connecting to grounding electrodes and for bonding to metallic piping near isolation transformer.

E. Identify components and wiring according to Division 26 Section "Identification for Electrical Systems."

3.2 FIELD QUALITY CONTROL

A. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

B. Tests and Inspections:

1. Comply with manufacturer's written instructions.
2. Inspect interiors of enclosures, including the following:
   a. Integrity of mechanical and electrical connections.
   b. Component type and labeling verification.
   c. Ratings of installed components.

3. Inspect batteries and chargers according to requirements in NETA Acceptance Testing Specifications.
4. Test manual and automatic operational features and system protective and alarm functions.
5. Test communication of status and alarms to remote monitoring equipment.
6. Provide load bank test per Manufacturer’s recommendation. Record results.

C. The UPS system will be considered defective if it does not pass tests and inspections.

D. Record of Start up Tests and Inspections: Maintain and submit documentation of tests and inspections, including references to manufacturers' written instructions and other test and inspection criteria. Include results of start up tests, inspections, and retests.

E. Prepare start up test and inspection reports.

3.3 DEMONSTRATION

A. Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain the UPS.

.

3.4 MANUFACTURERS

A. Subject to compliance with requirements, provide products and services by one of the following:

a. CyberPower
b. Other Owner Approved Equal

OPERATIONAL TECHNOLOGY NETWORK

PART 1 – GENERAL

1.1 WORK REQUIRED BY CONTRACT DOCUMENTS

A. In general, the Operational Technology Network (OTN) shall be provided, installed, programmed and commissioned by the Master Systems Integrator (MSI). Refer to drawing M-??? for system architecture/topology.

B. The MSI shall furnish and install a separate OTN network that is optimized for the needs and safety of Operational Technology (OT) devices, services, and building technologies (i.e. Security, Lighting Control, Elevators, Fire Alarm and Building Automation). The OTN shall be Fiber Ethernet based.

C. The OTN shall be an intelligent network that presents network information in the context of automation equipment. The solution provided shall be designed to be easily scalable and repeatable so it can be easily deployed to a wide variety of building technology applications.

D. The OTN is designed for standalone or networked IP operation with all the required software and hardware to ensure the building systems operation. Outside network connections should only be through the Firewall supplied with the operational network platform firewall.

E. The OTN Software shall include a web based Network Management Tool. The OTN Hardware shall include all Fiber Switches, Fiber to Copper Switches, and all Fiber and Ethernet cabling and associated wiring devices.

F. The MSI shall supply the data from all connected systems to the Owner in a graphical format. The graphics shall be web based and work on all devices capable of running up to date versions of Google Chrome, Safari, Mozilla and or Internet Explorer.

1.2 REFERENCED STANDARDS

The structured cabling system installation shall comply with the latest edition of all applicable codes, standards, and regulations including, but not limited to:

1. ANSI/TIA/EIA-568 Commercial Building Telecommunications Wiring Standard
2. ANSI/TIA/EIA-569 Commercial Building Standard for Telecommunications Pathways & Spaces
3. ANSI/TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure
4. ANSI J-STD-607-A Commercial Building Grounding & Bonding Requirements for Telecommunications
5. NFPA-70 National Electric Code (NEC)
6. NFPA 780 Standard for Installation of Lightning Protection Systems
7. NFPA 101 - Life Safety Code
8. American Society of Testing Material (ASTM)
9. Federal Communications Commission (FCC)
10. Institute of Electrical & Electronics Engineers (IEEE)
11. International Standards Organization (ISO)
12. Occupational Safety & Health Administration (OSHA)
13. Underwriters Laboratories (UL)
14. State and local codes

1.3 SYSTEM DESCRIPTION

A. The MSI shall provide a turnkey installation of all passive elements in the OT Network, including hardware, software, switches, riser cable, patch panels, termination blocks, equipment racks, wire management, ladder rack, labeling, and connectors.

B. The OTN shall be supplied with a software network management tool on premise and hosted within its own hardware.

C. The OTN shall be protected by its own Uninterruptable Power Supply (UPS).

1. There shall be a single login to view and manage the entire networking system.
2. The entire system shall be managed via single-management IP address.
3. The user interface shall be web browser-based.
4. The user interface shall be locally hosted on the networking equipment.
5. The user interface shall be in graphical format.

6. The user interface shall support all required operations via point-and-click interaction.
7. The user interface shall be supported on a tablet or smartphone.
8. The user interface shall provide configuration of all items as per Table A (see Appendix A).
9. The graphical user interface (GUI) shall support bulk configuration of all items as per Table A.
10. The GUI shall display the manufacturer name of all connected devices
11. The GUI shall graphically display all items as per Table B (see Appendix B).
12. The system shall alert the user either graphically or via email for all items as per Table C (see Appendix C).
13. The user shall be able to perform a PoE reset for any individual device in the system with a single click from the GUI.
14. The system shall maintain historical information for all data in Table B.
15. The tables in the GUI shall be sortable and filterable based on relevant data, including but not limited to:
    a. Bandwidth
    b. PoE consumption
    c. Text description
    d. VLAN
    e. Connection status
16. The system shall provide a backup and restore mechanism in a user editable format i.e., CSV.
17. The system shall support bulk firmware upgrades for all edge switches in one operation.
18. The system shall allow system-wide auto-creation of a VLAN simply by specifying one or more ports to be on that VLAN, and automatically ensure that traffic passes between the selected ports. There must not be any restriction on port location.

APPENDIX A

Item	Setting	Location
PoE	Enable/Disable	Per port
VLAN	Access/Trunk/Local	Per port
VLAN	ID	Per port
PoE	Weekly schedule	Per port
Port status	Enable/Disable	Per port
Port label	Text description	Per port
Switch label	Text description	Per switch
Switch status	Enable/Disable	Per switch
Port security	MAC filter	Per port

System name	Text description	Per system
System details	Text description	Per system

19. I*Table A: Configuration Settings (Read/Write)*
20.

APPENDIX B

Item	Setting	Location
Link Status	Up/Down and Speed	Per port
PoE	Power Consumption	Per port
PoE	Power Budget (Used/Available)	Per switch
Connected Device	Manufacturer Name	Per port
Connected Device	MAC Address	Per port
Traffic	Upstream Bandwidth	Per port
Traffic	Downstream Bandwidth	Per port
Traffic	Upstream Bandwidth	Per switch
Traffic	Downstream Bandwidth	Per switch
Traffic	Upstream Bandwidth	Entire Switch
Traffic	Downstream Bandwidth	Entire Switch

21. *Table B: Status Information (Read Only)*

APPENDIX C

Item	Information	Location	Threshold
PoE	Power Consumption	Per port	User configurable
PoE	Power Budget (Used/Available)	Per switch	Fixed warning levels
Connected Device	Manufacturer Name	Per port	Notification on change
Connected Device	MAC Address	Per port	Notification on change
Traffic	Upstream Bandwidth	Per port	User configurable
Traffic	Downstream Bandwidth	Per port	User configurable
Traffic	Upstream Bandwidth	Per switch	User configurable
Traffic	Downstream Bandwidth	Per switch	User configurable
Traffic	Upstream Bandwidth	Entire Switch	Fixed warning levels
Traffic	Downstream Bandwidth	Entire Switch	Fixed warning levels

22. *Table C: Alarm*
23.

PART 2 – PRODUCTS`

2.1 NETWORK MANAGER (Front End Switch):

The Network Manager shall serve as the Front End for the network. This switch shall allow the entire network to be centrally managed and monitored in real time from a graphical user interface that is web-hosted directly on the switch. The switch shall have LED status indicators displaying Alarms, Power, Link and Redundancy. Unit shall have the ability to be rack or wall mounted and supplied with brackets if wall mounted. The switch shall support all protocols used in Building Automation and Security. EPON Standard shall be IEEE 802.3ah GEPON, 1 Gbps bidirectional, 1310/1490- nm. Shall support single-strand, single-mode Optical Fiber OS1/OS2 9/125 µm, up to 8 km reach. Shall be able to handle traffic from Ethernet, TCP/IP or UDP/IP, BACNet/Ethernet, BACNet/IP. Switch shall have a minimum 3 year warranty.

2.2 EDGE SWITCHES (Fiber to Ethernet and Fiber to Fiber):

Edge switches shall be selected based on specific project topology. Edge switches shall be designed to allow all ports from every switch to be monitored and managed from the front end aggregation switch and graphical user interface. PoE specification shall be 802.3at PoE+, 30W available on every port (also 802.3af, 15W per port). Switches shall have the ability to be mounted via, DIN, Wall, or Rack as needed. EPON Standard shall be IEEE 802.3ah GEPON, 1 Gbps bidirectional, 1310/1490- nm. Shall support single-strand, single-mode Optical Fiber OS1/OS2 9/125 µm. Connector shall be Simplex SC/UPC Female Connector. Shall be able to handle traffic from Ethernet, TCP/IP or UDP/IP, BACNet/Ethernet, BACNet/IP. Switch shall have a minimum 3 year warranty.

2.3 FIBER OPTIC CABLING

A. Fiber optic cabling shall be provided between the OTN switches, splitters and the OTN Server location.

B. Fiber optic cabling shall utilize aluminum interlocking armor covering an internal plenum jacket.

C. Indoor/outdoor fiber optic cable shall meet or exceed the performance criteria found in TIA/EIA 568C.3 Optical Fiber Cabling Components.

D. Fiber optic cable shall be UL□ and c (UL□) Listed.

2.4 FIBER SPECIFICATION

A. Single-mode fiber (SMF) 9/125

1. Either OS1 or OS2 grade fiber is acceptable.
2. The fiber must have an internal diameter of 9 microns, and an external diameter of 125 microns.
3. Fiber must be terminated with SC/UPC connectors.

4. Only a single strand of fiber is required for each fiber run. Pairs are only required if product uses separate wavelengths of light to enable bidirectional traffic on a single fiber.
5. Insertion losses must be less than 0.3 dB / termination plus 1.0 dB / km.

2.5 TERMINATION TECHNIQUES

It is important to have high quality terminations to ensure that the planned OTN Budget is not broken. The following recommendations for the following termination strategies, in order:

1. Pre-terminated fibers, ordered and manufactured to appropriate lengths. (Best)
   a) These can be ordered with pull-eyes for pulling through conduit.
2. On-site fusion splicing with pre-terminated SC/UPC pigtails. (Good)
3. On-site termination with SC/UPC connectors. (Quality can vary)

2.6 CABLE TYPES & INSTALLATION CONSIDERATIONS

A. The type of cabling does not matter. Follow manufacturer's recommendations based on a single strand of fiber.
B. Based on the topology & environment, the type of fiber cabling desired may vary significantly, for instance:
   1. Single Strand 3mm Jacket for simple runs - In ceiling, cable tray, floor-to-floor conduit
   2. 6 or 12 strand cable with MPO connectors / breakout panel for longer runs or complex designs
C. Heavy Jacket 24 strand cable for outdoor or trench scenarios.
D. When using a multi-strand cable, it is not necessary to terminate all strands if they are not needed for the design.
E. Patch Panels are not required, but they may help with fiber organization and cable management for complex designs.
F. Splitters shall be ordered with long or custom fiber lead lengths. In some cases, intermediate fiber may not be required. Product shall also provide indoor patch cables in 1,3,5, and 20 meter lengths.
G. Ensure that the fiber installer has experience working with Single mode Fiber.

2.7 BEST PRACTICES

A. All fibers should be clearly labelled and documented, including damaged or unterminated strands.
   1. For detailed recommendations consult ANSI/TIA/EIA-606.

B. All fibers should be tested by the best means available
   2. Tier 1 insertion loss testing or Tier 2 OTDR testing at 1310 and 1550 nm with detailed reporting.

Approved vendors: Insert Vendors Here

GATEWAY

PART 1 – GENERAL

1.1 QUALITY ASSURANCE- System Startup and Commissioning

A. Each point in the system shall be tested for both hardware and software functionality. In addition, each mechanical and electrical system under control of the BAS will be tested against the appropriate sequence of operation specified herein. Successful completion of the system test shall constitute the beginning of the warranty period. A written report will be submitted to the owner indicating that the installed system functions in accordance with the plans and specifications.

B. The SI shall commission and set in operating condition all major equipment and systems, such as the chilled water, hot water and all air handling systems, in the presence of the equipment manufacturer's representatives, as applicable, and the Owner and Architect's representatives.

C. Startup Testing shall be performed for each task on the startup test checklist, which shall be initialed by the technician and dated upon test was completion along with any recorded data such as voltages, offsets or tuning parameters. Any deviations from the submitted installation plan shall also be recorded.

D. Required elements of the startup testing include:

1. Measurement of voltage sources, primary and secondary
2. Verification of proper controller power wiring.
3. Verification of component inventory when compared to the submittals.
4. Verification of labeling on components and wiring.
5. Verification of connection integrity and quality (loose strands and tight connections).
6. Verification of bus topology, grounding of shields and installation of termination devices.
7. Verification of point checkout.
8. Each I/O device is landed per the submittals and functions per the sequence of control.
9. Analog sensors are properly scaled and a value is reported
10. Binary sensors have the correct normal position and the state is correctly reported.
11. Analog outputs have the correct normal position and move full stroke when so commanded.
12. Binary outputs have the correct normal state and respond appropriately to energize/de-energize commands.
13. Documentation of analog sensor calibration (measured value, reported value and calculated offset).
14. Documentation of Loop tuning (sample rate, gain and integral time constant).

E. A performance verification test shall also be completed for the operator interaction with the system. Test elements shall be written to require the verification of all operator interaction tasks including, but not limited to the following:

1. Graphics navigation.
2. Trend data collection and presentation.
3. Alarm handling, acknowledgement and routing.
4. Time schedule editing.
5. Application parameter adjustment.
6. Manual control.
7. Report execution.
8. Automatic backups.
9. Web Client access.

F. A cybersecurity verification test shall be completed by the SI to include all of the following system configuration checks:

1. The application software shall be running the latest version and patch level from the manufacturer.
2. The real time operating system software (RTOS) shall be running the latest version and patch level as required by the manufacturer.
3. Unless unavailable, all network traffic settings will be configured for encrypted communications.
4. The IP address of the Gateway is not public facing.

G. A cybersecurity verification test shall be completed by the SI to include all of the following user configuration checks:

1. Manufacturer default users have been removed and replaced with the owner’s System Administration account.
2. Any guest accounts are disabled.
3. All SI users conform to the Owner’s password policy as itemized below for both application and platform access:
   a. Every user has a unique name and password.
   b. Only strong passwords are allowed.
   c. The auto-lockout feature is enabled, with a maximum of 10 log-on attempts.
   d. The auto-logoff feature is enabled, and users are logged off after 30 minutes of inactivity.
   e. Each user is assigned access privileges consistent with their responsibility.
   f. A minimum of 2 and a maximum of 4 system administrator accounts.

1.2 WARRANTY

All components, system software, and parts furnished and installed by the SI shall be guaranteed against defects in materials and workmanship for 1 year of substantial completion. Labor to repair, reprogram, or replace these components shall be furnished by the BSI at no charge during normal working hours during the warranty period. Materials furnished but not installed by the SI shall be covered to the extent of the product only. Installation labor shall be the responsibility of the trade contractor performing the installation. All corrective software modifications made during warranty periods shall be updated on all user documentation and on user and manufacturer archived software disks. The Contractor shall respond to the request for warranty service within 24 standard working hours.

1.3 TRAINING

A. The SI shall provide both on-site and classroom training to the Owner's representative and maintenance personnel per the following description:

B. On-site training shall consist of a minimum of (40) hours of hands-on instruction geared at the operation and maintenance of the systems. The curriculum shall include:

1. System Overview
2. System Software and Operation
3. System access
4. Software features overview
5. Changing set-points and other attributes
6. Scheduling
7. Editing programmed variables
8. Displaying color graphics
9. Running reports
10. Workstation maintenance
11. Viewing application programming
12. Operational sequences including start-up, shutdown, adjusting and balancing.

PART 2 – PRODUCTS

2.1 JAVA APPLICATION CONTROL ENGINE (JACE)

A. The FMCS shall be comprised of Java Application Control Engine or Controllers (JACE) within each facility. The JACE shall connect to the owner's local network, wide area network, or operational technology network (OTN) depending on configuration. Access to the system, either locally in each building, or remotely from a central site or sites, shall be accomplished through standard Web browsers, via the Internet and/or local area network. Each JACE is capable of communicating to LonMark/LonTalk (IDC) and/or BACnet (IBC) controllers and other open and legacy protocol systems/devices provided under Division 23 Temperature Control System.

B. The FMCS shall be based on the Niagara 4 Framework, a Java-based framework developed by Tridium. Niagara 4 provides an open automation infrastructure that integrates diverse systems and devices (regardless of manufacturer, communication standard or software) into a unified platform that can be easily managed in real time over the Internet using a standard Web browser. Systems not developed on the Niagara4 Framework platform are not acceptable.

2.2 MANUFACTURERS

A. Manufacturers: Subject to compliance with requirements, provide products and services by one of the following:

1. Tridium Vykon
2. Other Owner Approved Equal

2.3 COMMISSIONING SOFTWARE- BacNet Monitoring Tool

PART 1 - GENERAL

A. The MSI shall provide a monitoring tool as a software cloud service or as an on-premise solution in the form of a Virtual Machine Appliance or a computing server that will analyze the performance and overall health of the integrated control systems.

B. The BACnet application protocol shall be monitored on a periodic basis, and provide results based on a Health Score, and details for deeper analysis. The monitoring tool shall graphically display the information.

C. The monitoring tool shall provide a Network Health Score. The Network Health Score shall provide a score based on % with a color-coded health level.

D. There shall be a method for automatic capture and analysis of the BACnet data.

PART 2 – DATA

A. There shall be a dashboard with a running trend log to quickly view the Network Health

B. The monitoring tool shall accept data in the PCAP (.cap / .pcap / .pcapng) format.

C. The monitoring tool shall maintain historical data for up to 1 year.

D. The monitoring tool shall allow retrieval of historical data for up to 1 year in PCAP format.

E. The monitoring tool shall be able to host multiple users to share the same data.

F. The monitoring tool shall be able to share the data between different users (provided the users have access to the monitoring tool).

G. The monitoring tool shall support monitoring of multiple sites or networks.

H. The monitoring tool shall allow for grouping of the uploaded files for organization.

I. The monitoring tool shall look for:

a. Duplicate networks, devices and sources
b. Broadcast rate
c. Top broadcaster source
d. Reject, abort, error, missing acknowledgement and checksum error packets
e. Excessive COV and Confirmed COV packets
f. MS/TP token disruptions
g. Unresponsive BACnet devices
h. Longest response times
i. Alarm rates

J. The monitoring tool shall show a BACnet device list with the following information:

a. Object ID
b. Network ID
c. IP address if applicable
d. Manufacturer ID and associated registered manufacturer name

K. The monitoring tool shall easily find the offending device and provide direction on corrective action.

PART 3 - SECURITY

A. The monitoring tool shall provide alerts when the Network Health Score changes by a percentage or when it crosses a threshold shall be HTTPS using TLS certificates or greater.

B. User authentication shall be protected by password and minimum password strength is enforced.

C. All passwords are stored shall be encrypted using hashed and salted techniques.

D. User accounts shall be automatically locked upon 5 sequential unsuccessful login attempts.

E. All cloud data that is stored shall have anonymized filenames to remove any descriptive information (e.g. customer name, location name, date).

PART 4 - ALERTING

A. The monitoring tool shall provide alerts via email.

B. The monitoring tool shall provide alerts when the Network Health Score changes by a percentage or when it crosses a threshold.

PART 5 - REPORTING, CUSTOMIZATION and EXPORTING

A. The monitoring tool shall export the BACnet device list in CSV or PDF, with the above information.

B. There shall be an API for 3rd party integration.

C. The monitoring tool shall provide a report of all issues.

D. There shall be custom filtering of the information.

E. The monitoring tool shall provide the ability to save queries and filters of deeper analysis for future use.

F. The monitoring tool shall allow for comments within the file and the comments shall be available in the reports.

2.4 MANUFACTURERS

A. Manufacturers: Subject to compliance with requirements, provide products and services by one of the following:

1. Optigo- Visual BacNet
2. Other Owner Approved Equal

PART 3 – EXECUTION

3.1 COMMISSIONING AUDITS

A. Integration Platform Audits. The MSI will audit the Integration Platform using the Totem Trusted^{TM} Commissioning Audit prior to project completion, validating that the system was installed and configured according to all of the specified cybersecurity policies and procedures. A written report summary will be provided to the Owner confirming the results of the audit.

B. Integrated System Audits. The MSI will provide access to the Totem Trusted^{TM} Platform to each of the Integrated System Contractors for the purpose of responding to the Totem Trusted^{TM} Commissioning Audit for their respective system. The MSI will review the results with each Contractor prior to submitting a written report summary to the Owner.

END OF SPECIFICATION