****
NAVFAC NW **NFGS-25 10 10.00 24 (November 2018)**
based on UFGS-25 10 10 (November 2015)

Preparing Activity: NAVFAC NW **Superseding**
UFGS-25 10 10.00 24 (April 2018)

REGIONAL FACILITIES GUIDE SPECIFICATIONS

Use this specification for NAVFAC NW projects only.

References are in agreement with UMRL dated October 2018
****

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 10 10.00 24

UTILITY MONITORING AND CONTROL SYSTEM (UMCS) FRONT END AND INTEGRATION (NAVFAC NW)

PART 1 GENERAL

-- End of Section Table of Contents --

****

NAVFAC NW **NFGS-25 10 10.00 24 (November 2018)**
based on UFGS-25 10 10 (November 2015)

Preparing Activity: NAVFAC NW **Superseding**
UFGS-25 10 10.00 24 (April 2018)

REGIONAL FACILITIES GUIDE SPECIFICATIONS

Use this specification for NAVFAC NW projects only.

References are in agreement with UMRL dated October 2018

****

SECTION 25 10 10.00 24

UTILITY MONITORING AND CONTROL SYSTEM (UMCS) FRONT END AND INTEGRATION (NAVFAC NW)

NAVFAC NW Version 3.2; issued 11/27/2018

****

NOTE: NAVFAC NW Version 3.2; issued 11/27/2018

This guide specification covers the requirements for a integrated Building Control Systems (BCS) and Utility Control System (UCS) within the NAVFAC Northwest Area of Responsibility to the existing NW Regional Controls Network, including the front end, using the Niagara Framework.

******Please note that the NW has transitioned to calling the centralized control network "UMCS" (Utilities Monitoring and Control System) instead of the legacy title "ICS" (Industrial Control System) to align with NAVFAC nomenclature enterprise-wide. Please see UFC 3-470-01 "Utility Monitoring and Control System Front End and Integration" for more information. *******

This specification includes tailoring options to select the protocol(s) required to be supported at the Monitoring and Controls Software (Front-end).

This guide specification covers the requirements for integrating Niagara based supervisory controllers onto the regional Control System (CS) network (called "UMCS IP network" throughout the specification for clarity) for facilities and utilities under Commander Navy Region Northwest as well as for facilities at Naval Hospital Bremerton. The intent of this specification is for the project to:

1. Interface and communicate with the existing NAVFAC UMCS IP Network under the established Authority to Operate (ATO) managed by NAVFAC NW CIO4. If the project's scope of work requires the contractor to achieve a completely new ATO via the

Risk Management Framework, do not use this specification. The NAVFAC UMCS utilizes Niagara AX based Architecture which use Transmission Control Protocol / Internet Protocol (TCP/IP) and Hypertext Transfer Protocol (HTTP) to communicate with Building Level Controllers via the NAVFAC UMCS Network.

2. Select equipment and software to maintain Fleet Cyber security Readiness and accreditation of the UMCS and Fleet Cyber Command Authority to Operate the UMCS.

3. Create a graphical user interface for this project that complies with the graphical interface standards listed in Appendix B. Create custom graphical page content similar to the examples in Appendix C for the systems installed or modified in this project. Create unique new graphical page content where the new function differs from that existing currently in the NAVFAC UMCS, or variations of existing graphical pages are required based on Government review comments.

Edit this guide specification for project specific requirements by adding, deleting, or revising text. For bracketed items, choose applicable items(s) or insert appropriate information.

Remove information and requirements not required in the specific project, whether or not brackets are present.
Comments, suggestions and recommended changes for this guide specification are welcome. This regional GS (RGS) or NFGS is maintained by Kimberly Paulson of the NAVFAC NW Capital Improvements CI4 (Design) Mechanical Engineering Branch. Please contact her at (360) 315-4451 or kimberly.paulson@navy.mil with any comments or questions. Contact NAVFAC NW CIO4 UMCS ISSM (Information System Security Manager)for information related to the cybersecurity processes or Authority to Operate.
****

PART 1 GENERAL

1.1 SUMMARY

The Utility Monitoring and Control System (UMCS) shall perform supervisory monitoring and supervisory control of base-wide building control systems and utility control systems using Niagara Framework with Fox protocol as specified and shown. The UMCS shall interface with local building or other control systems installed per other Sections.

Version 3.2 Appendices A - F referenced throughout this UFGS can be found on the Whole Building Design Guide web page for this spec (https://www.wbdg.org/ffc/navy-navfac/regional-specifications/nfgs-25-10-10-00-24._ Click on the hyperlink next to the words "Related Materials" for "UMCS Front-End Integration (NAVFAC NW) APPENDICES A-Fv3.2"

(PDF file).

1.1.1 System Requirements

Provide a UMCS as specified and shown, and in accordance with the following characteristics:

The Control System consists of a high-speed, peer-to-peer network of workstations, servers, routers, network switches and stand-alone supervisory controllers. This network provides the capability to integrate BACnet, LonWorks, MODBUS, OPC and other open and proprietary communication protocols into one open, interoperable system.

A web based controller and server with a network interface card gathers data from this system and generates web pages accessible through an Internet Explorer™ web browser on each workstation connected to the network. Operators are able to perform normal and expanded operator functions through this web browser interface.

The system installed in this project, including all associated equipment and accessories, shall tie into the existing Niagara-based Control System. Each SC shall communicate to other open and legacy protocol systems/devices installed in the facility.

The UMCS is comprised of supervisory controllers which are based on a hierarchical architecture incorporating Niagara Framework™ ("Niagara"). All new and replacement equipment shall be compliant with the NiagaraFramework.

1.1.1.1 General System Requirements

a. The system shall perform supervisory monitoring and control functions including Scheduling, Alarm Handling, Trending, Overrides, Report Generation, and Electrical Demand Limiting as specified.

b. The system shall include a Graphical User Interface which shall allow for graphical navigation between systems, graphical representations of systems, access to real-time data for systems, ability to override points in a system, and access to all supervisory monitoring and control functions. See Appendices B and C for additional information.

c. All software used by the UMCS and all software used to install and configure the UMCS shall be licensed to and delivered to the NAVFAC NW CIO.

d. All software used by the UMCS shall be compatible with 64-bit (x64) versions of Windows operating system.

e. All necessary documentation, configuration information, configuration tools, programs, drivers, and other software shall be licensed to and otherwise remain with the Government such that the Government or their agents are able to repair, replace, upgrade, and expand the system without subsequent or future dependence on the Contractor. Software licenses shall not require periodic fees and shall be valid in perpetuity.

f. Provide sufficient documentation and data, including rights to documentation and data, such that the Government or their agents can execute work to repair, replace, upgrade, and expand the system without subsequent or future dependence on the Contractor.

g. The UMCS shall interface directly to BACnet (ASHRAE 135), LonwWorks (CEA-709.1-D), Modbus, OPC DA, and Niagara Framework field control systems as specified.

h. For UMCS systems with Monitoring and Control Software functionality implemented in Monitoring and Control (M&C) Controller Hardware, provide sufficient additional controller hardware to support the full capacity requirements as specified.

i. All Niagara Framework components shall have an unrestricted interoperability license with a Niagara Compatibility Statement (NiCS) following the Tridium Open NiCS Specification and shall have a value of "ALL" for "Station Compatibility In", "Station Compatibility Out", "Tool Compatibility In" and "Tool Compatibility Out". Note that this will result in the following entries in the license.dat file:

```
"accept.station.in=*"
"accept.station.out=*"
"accept.wb.in=*"
"accept.wb.out=*"
```

1.1.1.2 Niagara Framework Requirements

The UMCS shall use the Niagara Framework and shall communicate with Niagara Framework field control systems using the Fox protocol and HTTP over the Government furnished IP network.[Extend the Government's IP network as indicated in the project documents.].

1.1.2 General Cybersecurity Requirements

****

NOTE: The following paragraph provides a place to include general system-level information assurance requirements above and beyond the requirements already incorporated into the Product and Execution parts of this specification. This paragraph may or may not be required depending on how Information Assurance is being addressed for the project and site.

Provide specific requirements for Information Assurance - simply incorporating the references through the use of the default test is generally NOT sufficient.

****

Cybersecurity for the system shall be addressed in accordance with 25 50 00.00 20 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS and the following requirements.

1.1.2.1 Cyber Security

Prior to initiating any work on site pertaining to the UMCS each contractor employee who will work on programming or existing UMCS infrastructure shall:

a. Complete the SAAR-N form and the NAVFAC NW CS IA Addendum (provided by NAVFAC NW and included as Appendix F) and provide to Contracting Officer;

b. Complete the annual Department of Defense Information Assurance Awareness training;

c. Have proof of a clean background investigation with a least a Facility Access Determination (FAD)

Contractor should plan on the clearance activities listed above taking 12 weeks for personnel not already holding a Government security clearance. Clearance activities can take longer than 12 weeks for individuals found to have clearance issues during their background check.

Admin Rights: Contractors will not be granted full admin rights to any government-owned computer. Local accounts on government computers are not allowed; contractors whose personnel who have submitted their forms and have a proper background check or clearance will be granted access for the duration of the project.

USB 'thumb' drives are prohibited on Government equipment. Government-supplied USB hard drives are acceptable and can be checked out from CIO.

The Contractor shall not connect contractor owned computer equipment to the regional Controls System network, nor leave behind any telecommunication infrastructure (i.e., cellular modems) that allows remote access into installed equipment. All points of ingress and egress will be authorized and maintained by NAVFAC NW CIO and only after all required network ports and protocols are identified and documented.

The Contractor will be allowed to check out UMCS laptops for field use. Laptops for field use while on-site may be checked out from the UMCS laptop pool managed by NAVFAC NW CIO at NBK-Bangor, WA. Laptop check-out reservations should be scheduled at least one week in advance ensuring availability.

Provide secure password protection for each device/system; provide all integration necessary to incorporate centralized authentication i.e. ensuring single sign on leveraging Lightweight Directory Access Protocol (LDAP) provided by NAVFAC NW supported Active Directory Architecture. Password information shall be need-to-know, and the Contractor shall not disclose it to others. Password information shall be submitted via hard copy correspondence or CD to the Contracting Officer's Representative. Passwords shall not be conveyed by e-mail or 3rd party means, except encrypted email is acceptable.

If at any of the above security requirements are violated, the individual(s) will have (at a minimum) their Government computer access privileges revoked. All IT related possessions may be confiscated pending an investigation.

1.1.3 Symbols, Definition and Abbreviations

Symbols, definitions, and engineering unit abbreviations used in displays, submittals and reports shall be as currently used in the existing CS graphical user interface unless noted otherwise. See Appendix B for more information.

1.1.4 System Units and Accuracy

****

NOTE: Accuracy of calculations and precision and resolution of displays for the CS is specified in terms of the accuracy of the sensors used in the building controls connected to the CS. Edit the brackets to indicate a reference to the direct digital controls specification appropriate to this project.

****

Displays, print-outs and calculations shall be performed in English (inch-pound) units. Calculations shall have accuracy equal to or exceeding sensor accuracy as specified in Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC. Displays and printouts shall present values to at least one significant figure.

1.1.5 Data Packages/Submittal Requirements

****

NOTE: Coordinate the review of all submittals with the appropriate responsible person within NAVFAC NW.

In the NW AOR, Curt Hickle is the CS Program Manager. He maintains a portal site with information and resources to assist anyone involved in coordinating an CS project. It can be viewed by going to this portal address: https://hub.navfac.navy.mil/webcenter/portal/nw/Control+Systems(CS) All construction project submittals should be reviewed by CIO4 for compliance with product specifications.

All graphics submittals shall be reviewed by CIO3 for consistency to the standards.

The CS portal page lists the PW and CIO Core personnel who should be included on submittal review (including the SAES, RFP or DBB documentation). The list is maintained there instead of this Regional Guide Specification.

The acquisition of all technical data, data bases and computer software items that are identified herein will be accomplished strictly in accordance with the Federal Acquisition Regulation (FAR) and the Department of Defense Acquisition Regulation Supplement (DOD FARS). Those regulations as well as the Services implementations thereof should also be consulted to ensure that a delivery of critical items of technical data is not inadvertently lost. Specifically, the Rights in Technical Data and Computer Software Clause, DOD FARS 52.227-7013, and the Data Requirements Clause, DOD FAR 52.227-7031, as well as any requisite software licensing agreements will be made a part of the CONTRACT CLAUSES or SPECIAL CONTRACT REQUIREMENTS.

In addition, the appropriate DD Form 1423 Contract Data Requirements List, will be filled out for each distinct deliverable data item and made a part of the contract. Where necessary, a DD Form 1664, Data Item Description, will be used to explain and more fully identify the data items listed on the DD Form 1423. It is to be noted that all of these clauses and forms are required to ensure the delivery of the data in question and that such data is obtained with the requisite rights to use by the Government.

Include with the request for proposals a completed DD Form 1423, Contract Data Requirements List. This form is essential to obtain delivery of all documentation. Each deliverable will be clearly specified, both description and quantity being required.

****

Technical data packages consisting of computer software and technical data (meaning technical data which relates to computer software) which are specifically identified in this project and which may be defined/required in other specifications shall be delivered strictly in accordance with the CONTRACT CLAUSES and in accordance with the Contract Data Requirements List, DD Form 1423. Data delivered shall be identified by reference to the particular specification paragraph against which it is furnished. All submittals not specified as technical data packages are considered shop drawings under the Federal Acquisition Regulation Supplement (FARS) and shall contain no proprietary information and shall be delivered with unrestricted rights.

1.2 REFERENCES

****

NOTE: This paragraph is used to list the publications cited in the text of the guide specification. The publications are referred to in the text by basic designation only and listed in this paragraph by organization, designation, date, and title.

Use the Reference Wizard's Check Reference feature when you add a Reference Identifier (RID) outside of the Section's Reference Article to automatically place the reference in the Reference Article. Also use the Reference Wizard's Check Reference feature to update the issue dates.

References not used in the text will automatically be deleted from this section of the project specification when you choose to reconcile references in the publish print process.

****

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE 135	(2016) BACnet—A Data Communication Protocol for Building Automation and Control Networks

CONSUMER ELECTRONICS ASSOCIATION (CEA)

CEA-709.1-D	(2014) Control Network Protocol Specification
CEA-709.3	(1999; R 2015) Free-Topology Twisted-Pair Channel Specification

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 1815	(2015; CORR 2016) Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815 [Distributed Network Protocol (DNP3)]
IEEE C62.41	(1991; R 1995) Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

LONMARK INTERNATIONAL (LonMark)

LonMark Interoperability Guide	(2005) LonMark Application-Layer Interoperability Guide and LonMark Layer 1-6 Interoperability Guide; Version 3.4
LonMark SNVT List	(2014) LonMark SNVT Master List; Version 15
LonMark XIF Guide	(2001) LonMark External Interface File Reference Guide; Revision 4.402

MODBUS ORGANIZATION, INC (MODBUS)

Modbus	(2006) Modbus Application Protocol Specification; Version 1.1b and Modbus Messaging on TCP/IP Implementation Guide; Version V1.0b

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2018) Enclosures for Electrical Equipment (1000 Volts Maximum)

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 262	(2019) Standard Method of Test for Flame Travel and Smoke of Wires and Cables for Use in Air-Handling Spaces
NFPA 70	(2017; ERTA 1-2 2017; TIA 17-1; TIA 17-2; TIA 17-3; TIA 17-4; TIA 17-5; TIA 17-6; TIA 17-7; TIA 17-8; TIA 17-9; TIA 17-10; TIA 17-11; TIA 17-12; TIA 17-13; TIA

17-14; TIA 17-15; TIA 17-16; TIA 17-17) National Electrical Code

OPC FOUNDATION (OPC)

OPC DA — (Ver 3.0; Errata) OPC Data Access (DA)

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-568-C.1 — (2009; Add 2 2011; Add 1 2012) Commercial Building Telecommunications Cabling Standard

TIA-606 — (2017c) Administration Standard for the Telecommunications Infrastructure

TIA-607 — (2011b) Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises

TRIDIUM, INC (TRIDIUM)

Niagara Framework — (2012) NiagaraAX User's Guide

Tridium Open NiCS — (2005) Understanding the NiagaraAX Compatibility Statement (NiCS)

U.S. FEDERAL COMMUNICATIONS COMMISSION (FCC)

FCC EMC — (2002) FCC Electromagnetic Compliance Requirements

FCC Part 15 — Radio Frequency Devices (47 CFR 15)

UNDERWRITERS LABORATORIES (UL)

UL 1778 — (2014; Reprint Sep 2017) UL Standard for Safety Uninterruptible Power Systems

UL 60950 — (2000; Reprint Oct 2007) Safety of Information Technology Equipment

1.3 DEFINITIONS

The following list of definitions may contain terms not found elsewhere in this Section but are included here for completeness. Some terms are followed with a protocol reference in parenthesis (for example: (BACnet)) indicating to which protocol the term and definition applies.

1.3.1 Access Switch

An access switch has one or two trunk port connections. An access switch permits access to primarily end devices and not to other switches.

1.3.2 Alarm Generation

The process of comparing a point value (the point being alarmed) with a pre-defined alarm condition (e.g. a High Limit) and performing some action based on the result of the comparison.

1.3.3 Alarm Handling

See Alarm Routing

1.3.4 Alarm Routing

Alarm routing is M&C software functionality that starts with a notification that an alarm exists (typically as the output of an Alarm Generation process) and sends a specific message to a specific alarm recipient or device.

1.3.5 BACnet (BACnet)

The term BACnet is used in two ways. First meaning the BACnet Protocol Standard - the communication requirements as defined by ASHRAE 135 including all annexes and addenda. The second to refer to the overall technology related to the ASHRAE 135 protocol.

1.3.6 BACnet Interoperability Building Blocks (BIBBs) (BACnet)

A BIBB is a collection of one or more BACnet services intended to define a higher level of interoperability. BIBBs are combined to build the BACnet functional requirements for a device in a specification. Some BIBBs define additional requirements (beyond requiring support for specific services) in order to achieve a level of interoperability. For example, the BIBB DS-V-A (Data Sharing-View-A), which would typically be used by an M&C client, not only requires the client to support the ReadProperty Service, but also provides a list of data types (Object / Properties) which the client must be able to interpret and display for the user.

1.3.7 BACnet Testing Laboratories (BTL)(BACnet)

Established by BACnet International to support compliance testing and interoperability testing activities and consists of BTL Manager and the BTL Working Group (BTL-WG). BTL also publishes Implementation Guidelines.

1.3.8 BACnet Testing Laboratories (BTL) Listed (BACnet)

A device that has been certified by BACnet® Testing Laboratory. Devices may be certified to a specific device profile, in which case the certification indicates that the device supports the required capabilities for that profile, or may be certified as "other".

1.3.9 Binary

A two-state system or signal; for example one where an "ON" condition is represented by a high signal level and an "OFF" condition is represented by a low signal level. 'Digital' is sometimes used interchangeably with 'binary'.

1.3.10 Binding (LonWorks)

The act of establishing communications between CEA-709.1-D devices by associating the output of a device to the input of another so that information is automatically (and regularly) sent without being requested by the recipient.

1.3.11 Broadcast

Unlike most messages, which are intended for a specific recipient device, a broadcast message is intended for all devices on the network.

1.3.12 Building Control Network (BCN)

The network used by the Building Control System. Typically the BCN is a BACnet ASHRAE 135 or LonWorks CEA-709.1-D network installed by the building control system contractor.

1.3.13 Building Control System (BCS)

One type of Field Control System. A control system for building electrical and mechanical systems, typically HVAC (including central plants) and lighting. A BCS generally uses Direct Digital Control (DDC) Hardware and generally does NOT include its own local front end.

1.3.14 Building Point of Connection (BPOC)

A FPOC for a Building Control System. (This term is being phased out of use in preference for FPOC but is still used in some specifications and criteria.)

1.3.15 Clearance

Security Clearance

1.3.16 Control Logic Diagram

A graphical representation of control logic for multiple processes that make up a system.

1.3.17 Facility Point Of Connection (FPOC)

The FPOC is the point of connection between the UMCS IP Network and the field control network (either an IP network, a non-IP network, or both). The hardware at this location which provides the connection is generally one of a control protocol router, a control protocol gateway, or an IT device such as a switch, IP router, or firewall.

In general, the term "FPOC Location" means the place where this connection occurs, and "FPOC Hardware" means the device that provides the connection. Sometimes the term "FPOC" is used to mean either and its actual meaning (i.e. location or hardware) is determined by the context in which it is used.

1.3.18 Field Control Network

The network used by a field control system.

1.3.19 Field Control System (FCS)

A building control system or utility control system.

1.3.20 Fox Protocol (Niagara Framework)

The protocol used for communication between components in the Niagara Framework. By default, Fox uses TCP port 1911

1.3.21 Gateway

A device that translates from one protocol to another. Devices that change only the transport mechanism of the protocol - "translating" from LonWorks over TP/FT-10 to LonWorks over IP for example - are not gateways as the underlying protocol (data format) does not change. Gateways are also called Communications Bridges or Protocol Translators.

1.3.22 Control System (CS or now moving to calling it "UMCS")

The NAVFAC NW Control System (CS) is an integration of SCADA (Supervisory Control And Data Acquisition - for Utility System control) and DDC (Direct Digital Control - for Facility mechanical and electrical control) devices and the individual control systems, networks, field equipment, sensors and actuators that provide monitoring and control function for mechanical and electrical systems, and Advanced Metering Infrastructure. All control systems are part of the UMCS, whether part of a utility or a facility. Advanced Metering Infrastructure (AMI) is part of the CS program, but is not covered by this guide specification.

1.3.23 JACE (Niagara Framework)

Java Application Control Engine. See "Niagara Framework Supervisory Gateway". Note: The Niagara Framework parent corporation Tridium's product line of supervisory controllers are called "JACE" so the term "JACE" should be avoided when discussing supervisory controllers/gateways generally as it appears to refer to a proprietary product.

1.3.24 LDAP

Lightweight Directory Access Protocol. LDAP is used to authenticate supervisory controllers and computers to the NAVFAC CS Windows Domain.

1.3.25 LonMark Object (LonWorks)

A collection of network variables, configuration properties, and associated behavior defined by LonMark International and described by a Functional Profile. It defines how information is exchanged between devices on a network (inputs from and outputs to the network).

1.3.26 LNS Plug-in (LonWorks)

Software which runs in an LNS compatible software tool, typically a network configuration tool. Device configuration plug-ins provide a 'user friendly' method to edit a device's configuration properties.

1.3.27 LonMark (LonWorks)

See LonMark International. Also, a certification issued by LonMark International to CEA-709.1-D devices.

1.3.28 LonMark International (LonWorks)

Standards committee consisting of independent product developers, system integrators and end users dedicated to determining and maintaining the interoperability guidelines for LonWorks. Maintains guidelines for the interoperability of CEA-709.1-D devices and issues the LonMark Certification for CEA-709.1-D devices.

1.3.29 LonWorks (LonWorks)

The term used to refer to the overall technology related to the CEA-709.1-D protocol (sometimes called "LonTalk"), including the protocol itself, network management, interoperability guidelines and products.

1.3.30 LonWorks Network Services (LNS) (LonWorks)

A network management and database standard for CEA-709.1-D devices.

1.3.31 LonWorks Network Services (LNS) Database (LonWorks)

The standard database created and used by LonWorks Network Services (LNS) compatible tools, such as LNS Network Configuration tools.

1.3.32 Modbus

A basic protocol for control network communications generally used in utility control systems. The Modbus protocol standard is maintained by The Modbus Organization.

1.3.33 Master-Slave/Token Passing (MS/TP)(BACnet)

Data link protocol as defined by the BACnet standard. Multiple speeds (data rates) are permitted by the BACnet MS/TP standard.

1.3.34 Monitoring and Control (M&C) Software

The UMCS 'front end' software which performs supervisory functions such as alarm handling, scheduling and data logging and provides a user interface for monitoring the system and configuring these functions.

1.3.35 NAVFAC NW CIO (CIO)

NAVFAC NW CIO (CIO) is the authority having jurisdiction over all CS IT (Information Technology) and OT (Operational Technology).

1.3.36 Network or CS Network

The CS is composed of Ethernet TCP/IP router-switch-and-cable network running over copper and fiber media, and serial networks running over a variety of media.

1.3.37 Network Variable (LonWorks)

See 'Standard Network Variable Type (SNVT)'.

1.3.38 Niagara AX (Also called "Niagara")

A version (release) of the Niagara Framework used by NAVFAC NW. While it is often used to refer to just the front end, it includes all components of the Niagara Framework. NAVFAC NW (along with the Navy enterprise-wide) is moving to Niagara 4 via inclusion in the enterprise Authority to Operate.

1.3.39 Niagara Framework (Niagara Framework)

A set of hardware and software specifications for building and utility control owned by Tridium Inc. and licensed to multiple vendors. The

Framework consists of front end (M&C) software, web based clients, field level control hardware, and engineering tools. While the Niagara Framework is not adopted by a recognized standards body and does not use an open licensing model, it is sufficiently well-supported by multiple HVAC vendors to be considered a de-facto Open Standard.

1.3.40 Niagara Framework Supervisory Gateway (Niagara Framework)

DDC Hardware component of the Niagara Framework. A typical Niagara architecture has Niagara specific supervisory gateways at the IP level and other (non-Niagara specific) controllers on field networks (TP/FT-10, MS/TP, etc.) beneath the Niagara supervisory gateways. The Niagara specific controllers function as a gateway between the Niagara framework protocol (Fox) and the field network beneath. These supervisory gateways may also be used as general purpose controllers and also have the capability to provide a web-based user interface. NAVFAC NW has called these devices "Supervisory Controllers" in the past, but is aligning with enterprise-wide terminology and will now use the term "gateway".

1.3.41 Override

To change the value of a point outside of the normal sequence of operation where this change has priority over the sequence. An override can be accomplished in one of two ways: the point itself may be Commandable and written to with a priority or there may be a separate point on the controller for the express purpose of implementing the override.

Typically this override is from the Utilities Monitoring and Control System (UMCS) Monitoring and Control (M&C) Software. Note that this definition is not standard throughout industry.

1.3.42 Point, Calculated

A value within the M&C Software that is not a network point but has been calculated by logic within the software based on the value of network points or other calculated points. Calculated points are sometimes called virtual points or internal points.

1.3.43 Point, Network

A value that the M&C Software reads from or writes to a field control network.

1.3.44 Polling

A requested transmission of data between devices, rather than an unrequested transmission such as Change-Of-Value (COV) or Binding where data is automatically transmitted under certain conditions.

1.3.45 Property (BACnet)

A BACnet Property - a data element associated with an Object. Different Objects have different Properties, for example an Analog Input Object has a Present_Value Property (which provides the value of the underlying hardware analog input), a High_Limit Property (which contains a high limit for alarming), as well as other properties.

1.3.46   Protocol Implementation Conformance Statement (PICS)(BACnet)

A document, created by the manufacturer of a device, which describes which potions of the BACnet standard are implemented by a given device.

1.3.47   Repeater

A device that connects two control network segments and retransmits all information received on one side onto the other.

1.3.48   Router(LonWorks)

A device that connects two channels and controls traffic between the channels by retransmitting signals received from one subnet onto the other based on the signal destination. Routers are used to subdivide a control network and to control bandwidth usage.

1.3.49   Router (BACnet)

A device that connects two or more BACnet networks and controls traffic between the networks by retransmitting signals received from one network onto another based on the signal destination. Routers are used to subdivide an internetwork and to control bandwidth usage.

1.3.50   SAAR-N Form (SAAR)

A System Authorization Access Request - Navy form and any required addendums. These forms are used to request UMCS access and validate that an individual has the appropriate security clearance in place prior to performing any work related to the UMCS. A SAAR form is also used to request a domain account for a new user.

1.3.51   Segment

A 'single' section of a control network that contains no repeaters or routers. There is generally a limit on the number of devices on a segment, and this limit is dependent on the topology/media and device type. For example, a TP/FT-10 segment with locally powered devices is limited to 64 devices, and a BACnet MS/TP segment is limited to 32 devices.

1.3.52   Service (BACnet)

A BACnet Service. A defined method for sending a specific type of data between devices. Services are always defined in a Client-Server manner, with a Client initiating a Service request and a Server Executing the Service. Some examples are ReadProperty (a client requests a data value from a server), WriteProperty (a client writes a data value to a server), and CreateObject (a client requests that a server create a new object within the server device).

1.3.53   Service Pin (LonWorks)

A hardware push-button on a device which causes the device to broadcast a message containing its Node ID and Program ID. This broadcast can also be initiated via software.

1.3.54   Standard BACnet Object/Property/Service (BACnet)

BACnet Objects, Properties, or Services that are standard Objects, Properties, or Services enumerated and defined in ASHRAE 135. Clause 23 of ASHRAE 135 defines methods to extend ASHRAE 135 to non-standard or proprietary information. Standard BACnet Objects/Properties/Services specifically exclude any vendor specific extensions.

1.3.55 Standard Network Variable Type (SNVT) (LonWorks)

Pronounced 'snivet'. A standard format type (maintained by LonMark International) used to define data information transmitted and received by the individual nodes. The term SNVT is used in two ways. Technically it is the acronym for Standard Network Variable Type, and is sometimes used in this manner. However, it is often used to indicate the network variable itself (i.e. it can mean "a network variable of a standard network variable type"). In general, the intended meaning should be clear from the context.

1.3.56 Supervisory Controller (also called "SC")

A controller implementing a combination of supervisory logic (global control strategies or optimization strategies), scheduling, alarming, event management, trending, web services or network management. Note this is defined by use; many supervisory controllers have the capability to also directly control equipment. Supervisory controllers can also be gateways and typically are in a Niagara Framework-based UMCS. See "Niagara Framework Supervisory Gateway" definitiona above. NAVFAC NW is moving away from the term "supervisory controller" to describe the controller that contains the Niagara Framework and using "gateway" instead.

1.3.57 Supervisory Gateway

A device that is both a supervisory controller and a gateway, such as a Niagara Framework Supervisory Gateway.

1.3.58 Transport Switch

Switch with more than two trunk port connections and acts as WAN (wide area network) connectivity.

1.3.59 TP/FT-10 (LonWorks)

A Free Topology Twisted Pair network (at 78 kbps) defined by CEA-709.3. This is the most common media type for a CEA-709.1-D control network.

1.3.60 TP/XF-1250 (LonWorks)

A high speed (1.25 Mbps) twisted pair, doubly-terminated bus network defined by the LonMark Interoperability Guidelines. This media is typically used only as a backbone media to connect multiple TP/FT-10 networks.

1.3.61 Trunk Port Connection

A port that is assigned to carry traffic for all the VLANs that are accessible by a specific switch, a process known as trunking. This is typically a switch-to-switch connection.

1.3.62 VLAN

A virtual LAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. The UMCS IP network is divided into multiple VLANs, which include Administration, Utility systems, Facility systems and metering systems, printers, each type of server, workstations internal to the Operations Center, workstation external to Operations Center and more. Multiple VLANs are in use, and are subject to change by CIO.

1.4 SUBMITTALS

****

NOTE: Review Submittal Description (SD) definitions in Section 01 33 00 SUBMITTAL PROCEDURES and edit the following list to reflect only the submittals required for the project.

The Guide Specification technical editors have designated those items that require Government approval, due to their complexity or criticality, with a "G." Generally, other submittal items can be reviewed by the Contractor's Quality Control System. Only add a "G" to an item, if the submittal is sufficiently important or complex in context of the project.

The "S" following a submittal item indicates that the submittal is required for the Sustainability eNotebook to fulfill federally mandated sustainable requirements in accordance with Section 01 33 29 SUSTAINABILITY REPORTING. Locate the "S" submittal under the SD number that best describes the submittal item.

****

****

NOTE: Coordinate the review of all submittals with the NAVFAC NW CIO as they have review authority on all products and graphic user interfaces.

****

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. Submittal with a "G-CIO" designation shall be routed to NAVFAC NW CIO for approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES Section 01 33 00.05 20 CONSTRUCTION SUBMITTAL PROCEDURES and TABLE 1: PROJECT SEQUENCING

Provide one copy of required paper and electronic submittals.

Limit submittal information to only that required by this specification. Do not package product data, design drawings, wiring/network diagrams, or other submittals required by building automation field control systems into the UMCS submittals. Doing so could result in immediate rejection.

Drawings:
Provide review drawings as PDF compatible files e-mail and optical disk and each drawing on 11" x 17" paper.

Where existing systems are being modified, shop drawings shall consist of edits to existing record drawings.

****

NOTE: The submittals included in this guide specification are critical and require Government review. Any added submittals normally should be for information only and reviewed through the Contractor Quality Control system.

****

SD-02 Shop Drawings

CS Contractor Design Drawings; G-CIO

CS Contractor Design Drawings on optical disk in PDF and AutoCAD format.

Draft As-Built Drawings; G-CIO

Draft As-Built Drawings on optical disk in PDF and AutoCAD v2010 format.

Final As-Built Drawings; G-CIO

Final As-Built Drawings in hard copy and on optical disk in PDF and AutoCAD v2010 format.

Graphics; G-CIO

Provide graphics pages for the project at actual graphics resolution and format, including all common pieces of equipment, page backgrounds, and menu structures.

Also provide the entire station copy (including images, px pages, and the *.bog file) of the graphical user interface along with the administrative credentials.

SD-03 Product Data

Product Data Sheets; G-CIO

Copies of all manufacturer catalog cuts and specification sheets for all products (equipment) specified in PART 2 and supplied under this contract. When manufacturer's product data sheets apply to a product series rather than a specific product, clearly indicate applicable model selected and options selected by highlighting or by other means.

Include in the product data sheet submittal a single page with the list price value for each product (do not provide a single lump sum amount) in PART 2 supplied on this project. The itemized list must include all switches, supervisory controllers, data cabling/wiring, software (including drivers or other software added to the switches and supervisory controllers), UPS, and locked rack or enclosure (including intrusion detection). Provide only material costs (not labor) and provide a total sum for the project at the bottom of the list.

Software; G-CIO

Manufacturer OEM support (includes license).

Network UMCS Hardware and Software Inventory; G-CIO

Managed Ethernet Switch; G-CIO

Submit approved switches to NAVFAC NW CIO for configuration.

SD-05 Design Data

Project UMCS Plan; G-CIO

SD-06 Test Reports

****

NOTE: Keep the Existing Conditions Report for CS projects in existing buildings and using existing network infrastructure.

****

Existing Conditions Report; G-CIO

One electronic copy of the Existing Conditions Report.

Password Logs; G-CIO

Provide a preliminary list of all passwords created in executing the work of this contract.

FPT Report; G

One electronic copy of the FPT Report.

SD-10 Operation and Maintenance Data

Operation and Maintenance (O&M) Instructions; G

Only provide O&M information for the supervisory controller.

SD-11 Closeout Submittals

Password Log; G-CIO

Provide a final, complete list of all passwords (and associated software, device or system) created in executing the work of this contract.

Warranty (ethernet switch); G-CIO

Key(s) to Locked Enclosure; G-CIO

Final Supervisory Controller Station; G-CIO

Programming Code Files; G

1.5 PROJECT SEQUENCING

TABLE I: PROJECT SEQUENCING specifies the sequencing of submittals as specified in paragraph SUBMITTALS (denoted by an 'S' in the 'TYPE' column) and activities as specified in PART 3: EXECUTION (denoted by an 'E' in the 'TYPE' column).

a. Sequencing for submittals: The sequencing specified for submittals is the deadline by which the submittal must be initially submitted to the Government. Following submission there will be a Government review period as specified in Section 01 33 00 SUBMITTAL PROCEDURES. If the submittal is not accepted by the Government, revise the submittal and resubmit it to the Government within [14] [_____] working days of notification that the submittal has been rejected. Upon re-submittal there will be an additional Government review period. If the submittal is not accepted, the process repeats until the submittal is accepted by the Government.

b. Sequencing for Activities: The sequencing specified for activities indicates the earliest the activity may begin.

c. Abbreviations: In TABLE I the abbreviation AAO is used for 'after approval of' and 'ACO' is used for 'after completion of'.

d. The Cybersecurity Hygiene Checklist submittal referenced in Table I below is from 25 50 00.00 20 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS. It is included here for clarity regarding the overall process of connecting to the UMCS IP network.

e. The Network UMCS Hardware and Software Inventory form is detailed in 25 50 00.00 20 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS, but is a submittal in this specification.

****

NOTE: Complete TABLE I by entering the appropriate number of days in the spaces provided in the SEQUENCING column.

****

****

NOTE: The PROJECT SEQUENCING table may not display properly in SpecsIntact. If it appears empty right-click on the table and select "Make All Rows Same Height" to make the entire table appear and then adjust row heights as needed (such as reducing row height for rows with less text).

****

TABLE I. PROJECT SEQUENCING

ITEM	TYPE	DESCRIPTION	SEQUENCING
1		[Notice to proceed][_____]	

TABLE I. PROJECT SEQUENCING

ITEM	TYPE	DESCRIPTION	SEQUENCING
2	E	Contractor requests existing network topology. Allow 15 working days for NAVFAC NW CIO response.	
3	S	CS Contractor Design Drawings and Existing Conditions Report; Project UMCS Plan	[_____][60] days after #1
4	S	Product Data Sheets	[_____][30] days AAO #3
5	S	Network Hardware and Software Inventory; Contractor shall deliver to NAVFAC NW CIO all transport and access switches to be installed.	AAO #4
6	E	Contractor picks up submitted switches.	[___][15] days AAO #5
7	S	Graphics	AAO #3
8	E	Install CS	AAO #6
9	S	Cybersecurity Hygiene Checklist turned into CIO; Computer Software; Draft As-Built Drawings; Preliminary Password Log; Building Control System Performance Verification Testing [and Commissioning]	ACO #8
10	S	Request physical connection; Close-out Password Log	10 days after Government AAO #9 (iterative process)
11	E	Government authorized personnel will make physical connection.	14 days after #10
12	E	UMCS IP NetworkFunctional Performance Testing	AAO #10 and #11
13	S	Functional Performance Testing Report	[_____] days ACO #12

TABLE I. PROJECT SEQUENCING

ITEM	TYPE	DESCRIPTION	SEQUENCING
14	S	O&M Instructions	AAO #13

1.6 QUALITY CONTROL (QC)

1.6.1 Contractor's Qualifications

The Contractor or subcontractor that will perform the work shall have completed at least three systems installations of the same type and design specified and that have successfully operated the required sequence of operation for at least one year. The installer shall be a Niagara AX Contractor-Partner.

Control System Integrator shall exclusively be in the regular and customary business of design, installation and service of networked, computerized building controls systems similar in size and complexity to this project. The Control System Integrator shall be the manufacturer of the primary system components or shall have been the authorized representative for the primary DDC components manufacturer for at least 5 years.

The programmer responsible for programming the gateways shall have a minimum of 2 years of experience in programming gateways for similar systems of the same manufacturer. Programmer shall have successfully completed the Niagara AX Certification Training Course (or more current) and be certified. The programmer shall also have attended a NAVFAC NW Front-End Integration Training since this version of the Front-End Integration specification was issued. Contact NAVFAC_NW_PW_ICS_OPS@navy.mil for upcoming training dates and times. (Note: The date (MM/YY) that this specification was issued can be found immediately under the specification title header at the beginning of this Section.)

1.6.2 Support

Certified local technical support shall exist within 50 miles of the site.

[1.6.3 Commissioning

****

NOTE: Commissioning is required by UFC 01-200-02 for all "complex" systems. If the project this specification is being used for is generating a Sequence of Operation or new control logic, it is recommended that this paragraph is retained.

For smaller projects, having the contractor provide the commissioning agent (first paragraph option below) is acceptable. For larger projects only choose third party commissioning if job will have third party commissioning agent of the DDC or SCADA

system. LEED certified building projects would have this and so would other larger ECIPS, MCONS, etc.
****

****
NOTE: Choose the next paragraph if the Contractor is providing the Commissioning Agent and this is a smaller project without a Division 01 Commissioning specification.
****

[The Contractor shall provide commissioning of the Utility Monitoring and Control System (UMCS) installed by this project and the Commissioning Agent shall create testing requirements as necessary to verify the installed CS system meets the contract requirements.
]
****
NOTE: Choose the next paragraph if the Contractor is providing the Commissioning Agent and this is a larger project WITH a Division 01 Commissioning specification.
****

[The Contractor shall provide a Commissioning Authority to commission the UMCS and other systems as specified in 01 91 00.15 TOTAL BUILDING COMMISSIONING.
]
****
NOTE: Choose the next paragraph if the Government is providing the Commissioning Agent and there is a Division 01 Commissioning specification. Request the NW version of the Commissioning UFGS from someone in the mechanical group in NAVFAC NW Capital Improvements Design Product Line, specifically Dan O'Neal or Kimberly Paulson. It can also be found on the CI4 Mechanical portal page.
****

[The Government has retained the services of a Commissioning Authority to commission the UMCS and other systems as specified in 01 91 00.15 24 TOTAL BUILDING COMMISSIONING.

]]1.7 DELIVERY, STORAGE, AND HANDLING

Stored products shall be protected from the weather, humidity and temperature variations, dirt and dust, and other contaminants, within the storage condition limits published by the equipment manufacturer.

1.8 OPERATION AND MAINTENANCE (O&M) INSTRUCTIONS

The UMCS Operation and Maintenance Instructions shall include:

a. Procedures for the CS system start-up, operation and shut-down.

b. Final As-Built drawings.

c. Routine maintenance checklist. The routine maintenance checklist shall be arranged in a columnar format. The first column shall list all installed devices, the second column shall state the maintenance activity or state no maintenance required, the third column shall state the frequency of the maintenance activity, and the fourth column for additional comments or reference.

d. Qualified service organization list including points of contact with phone numbers.

e. Start-Up and Start-Up Testing Report.

f. Functional Performance Test (FPT) Procedures and Reports.

[1.9 RECOMMENDED DIVISION OF WORK

****

NOTE: Include the "Division of Work" paragraph if the project includes DDC or electrical system work intending to report to the UMCS. If this RGS is only to be used to integrate an existing BLC into the UMCS, then this paragraph is unnecessary. If in doubt, leave this paragraph.

****

The Division 23, 26, and 33 contractors (when separate from the UMCS contractor) shall be responsible for all controllers, control devices, control panels, controller programming, controller programming software, controller input/output and power wiring and controller network wiring. The design and installation of these systems are covered in Parts 3 and 4 of this RFP Division 23, 26 and 33 UFGS'.

The UMCS contractor shall be responsible for the SC, software and programming of the SC, the graphical user interface, development of all graphical screens, Web browser pages, setup of schedules, alarms, LonWorks network management and connection of the gateway into the UMCS IP network. The UMCS contractor shall integrate all data, monitoring and control provided by the Division 23, 26 and 33 contractor devices and make it available onto the UMCS IP network.

]PART 2 PRODUCTS

2.1 EQUIPMENT REQUIREMENTS

2.1.1 Standard Products

Provide components and equipment that are "standard products" of a manufacturer regularly engaged in the manufacturing of products that are of a similar material, design and workmanship. "Standard products" is defined as being in satisfactory commercial or industrial use for 2 years before bid opening, including applications of components and equipment under similar circumstances and of similar size, satisfactorily completed by a product that is sold on the commercial market through advertisements, manufacturers' catalogs, or brochures. Products having less than a 2-year field service record are acceptable if a certified record of satisfactory field operation, for not less than 6000 hours exclusive of the manufacturer's factory tests, can be shown. Provide equipment items that are supported by a service organization.

2.1.2 Product Certifications

Computing devices, as defined in FCC Part 15, supplied as part of the UMCS shall be certified to comply with the requirements of Class B computing devices.

2.1.3 Product Sourcing

Contractor supplied units of the same type of equipment shall be products of a single manufacturer. Each major component of equipment shall have the manufacturer's name and the model and serial number in a conspicuous place. Materials and equipment shall be new standard unmodified products of a manufacturer regularly engaged in the manufacturing of such products.

The Contractor shall select software, materials and equipment that are compatible with the existing UMCS system. If the Contractor incorporates equipment or devices which require software and programming tools different than those currently in use, the Contractor shall provide compatible software for every server, laptop and desktop workstation in the existing UMCS, any specialized training, and all UMCS modifications or specialized programming needed to support the unique equipment.

Contractor shall utilize as few unique pieces of equipment as possible. Wherever possible, the Contractor shall utilize a typical piece of equipment in numerous locations.

2.1.4 Ownership of Proprietary Material

Project-specific software and documentation shall become the Government's property. This includes, but is not limited to: software, graphics, record drawings, database(s), application of programming code, station copies, and documentation.

2.1.5 General Requirements

Provide components that meet the following requirements:

a. Portions of the data communications equipment system installed in unconditioned spaces shall operate properly in an environment with ambient temperatures between [0 and +49]degrees C [+32 and 120] degrees F and ambient relative humidity between 10 percent and 90 percent noncondensing. Special temperature and/or humidity requirements for specific equipment is provided in Part 2 of this Specification.

b. Components shall accept 100 to 125 volts AC (Vac), 60 Hz, single phase, three wire with a three-pronged, dedicated circuit outlet or be provided with a transformer to meet the component's power requirements. The only exception to this are products in a SCADA or substation environment in which power can be supplied at direct current. The requirement for devices to unplug remains.

c. The equipment shall meet the requirements of NFPA 70, UL 60950, NFPA 262, FCC EMC, and FCC Part 15.

2.1.6 Nameplates

Nameplates shall be laminated plastic and shall identify the function, network address, if applicable, and identifier of the device. Laminated plastic shall be at least 3 mm 0.125 inch thick, white with black center core. Nameplates shall be a minimum of 25 by 75 mm 1 by 3 inch with minimum 6 mm 0.25 inch high engraved block lettering.

2.1.7 Product Data Sheets

For all products (equipment) specified in PART 2 and supplied under this contract, submit copies of all manufacturer catalog cuts and specification sheets to indicate conformance to product requirements.

2.2 MANAGED UMCS ETHERNET SWITCH

****

NOTE: Always keep this switch section (next paragraph) in the project unless the designer knows that an existing switch should not be upgraded. The switch product info would only be deleted if the facility is already on UMCS IP network. In that case the existing switch may remain, but check with CIO to make sure the existing switch meets current criteria. If it doesn't, project documentation should state to replace the existing switch and this paragraph should remain.

****

2.2.1 General

Provide managed ethernet switch(es). Consult with NAVFAC NW Command Information Office (CIO) to obtain the salient characteristics of the managed switch(es) allowed on the UMCS Authority to Operate currently in use throughout the NW Region. In general, expect to provide a managed switch with the following features:

a. Configurable session timeouts for each service such as (but not limited to) SSH, Telnet, TFTP, and Web console sessions
b. Multi-level user passwords; support authentication for console access
c. SSH version2/SSL (128-bit encryption) connections
d. Support SNMPv3 with SHA Authentication Protocol and AES Privacy
e. Support SNMPv3 with SHA Authentication Protocol and AES Privacy
f. Support enabling/disabling of ports
g. Support MAC based port security
h. Support VLAN (802.1Q) to segregate and secure network traffic
i. Support RADIUS centralized password management utilizing AAA authentication
j. Console timeout must be configurable
k. FIPS 140-2 compliant (all four levels)
l. Support multiple NTP server to synchronize time
m. Compatible with network performance monitoring; can tie into a security incident event management system (SIEM)
n. Configurable login banner
o. 56-bit encryption
p. Ability to create and rename local accounts
q. Create SNMP accounts separate from local accounts
r. Have integral power plug and cord.

SOHO or SMB class switches are prohibited.

Provide five year manufacturer's warranty (ethernet switch).

2.2.2 Software

Operating System Software shall allow plug and play operation and have automatic learning, negotiation and crossover detection and shall support MSTP 902.1Q-2005, RSTP (802.1w) and Enhanced Rapid Spanning Tree network fault recover (<5ms), SNMPv3 SHA Authentication Protocol, AES Privacy Protocol, Quality of Service (802.1p) for real time traffic, VLAN (802.1Q) with double tagging and GVRP support, Link aggregation (802.3ad), IGMP Snooping for multicast filtering, and provide port configuration, status, statistics, mirroring, and security.

2.2.3 Ports

Ports shall be non-blocking, store and forward switching, with long haul optics allow Gigabit distance up to 70km and multiple connector types. Gigabit fiber ports shall be configured for small form-factor pluggable (SFP), and the Contractor shall provide an SFP transceiver for each SFP port.

Fiber ports for all planned connections can be in a fixed configuration.

2.2.4 Types of Managed UMCS Switches

[2.2.4.1 Switches serving a Substation

Switch shall be ruggedized to support immunity to EMI and heavy electrical surges and the temperature and humidity environment commonly found in substation installations. Specifically switches shall comply with the following industry standards: IEEE 1613 Class 2 (electric utility substations) and IEC 61850-3 (electric utility substations).

]2.2.4.2 Switches Located in Unconditioned Enclosures in Ambient Conditions

Switch shall be ruggedized to withstand minus 40 degrees Celsius to 85 degrees Celsius -40 to 125 degrees Fahrenheit operating temperatures.

2.2.4.3 UMCS Transport Switch

Switch shall have trunk port connections at 1000 megabits per second (MPS) or greater.

Spare ports:

a. Provide enough ports to support a total of 25% of the ports to be unused, or "spare", at the conclusion of the project.

b. Two of the spare ports provided above shall be RJ-45 copper connections capable of speeds 100 MPS or greater, one of which is to be dedicated to technician laptop access.

c. The remaining spare ports must be a user-replaceable SFP module that supports fiber and copper transceivers capable of 1000 MPS or greater. If the prevailing fiber media to the location is limited to slower speeds, due to distance or other conditions, 100 MPS are permissible with prior approval of NAVFAC NW CIO.

d. At least two of the remaining spare ports in "c" above shall be populated with the appropriate SFP transceiver for use with 1000LX SMF LC.

2.2.4.4 UMCS Access Switch

Switch shall have trunk port connections at 1000 megabits per second (MPS) or greater.

Switch shall have minimum of six (6) RJ-45 copper ports capable of speeds 100 MPS or greater.

Spare ports:

a. Provide enough ports to support a total of 20% of the ports to be unused, or "spare", at the conclusion of the project.

b. Two of the spare ports provided above shall be RJ-45 copper connections capable of speeds 100 MPS or greater, one of which is to be dedicated to technician laptop access.

2.3 CONTROL HARDWARE

2.3.1 Control Protocol Gateways

The Control Protocol Gateway shall perform bi-directional protocol translation between Fox protocol and one of the following protocols: CEA-709.1-D, ASHRAE 135, Modbus, and OPC DA.

a. All software required for gateway configuration shall be provided and licensed to the Government.

b. Gateways shall retain their configuration after a power loss of an indefinite time, and shall automatically return to their pre-power loss state once power is restored.

c. Gateways shall, in addition, meet all requirements specified (in the following subparagraphs) for each of the two protocols it translates.

2.3.1.1 Gateway for CEA-709.1

In addition to the requirements for all gateways, Gateways that use CEA-709.1-D shall meet the following requirements:

a. It shall allow bi-directional mapping of data in the Gateway to Standard Network Variable Types (SNVTs) according to the LonMark SNVT List.

b. Gateways shall not communicate CEA-709.1-D over an IP network.

c. It shall allow of its standard network variables (SNVTs) and support transmitting data using the "min, max, and delta" (throttling and heartbeat) methodology.

d. It shall provide the ability to label SNVTs.

e. It shall supply a LonMark external interface file (XIF) as defined in the LonMark XIF Guide for use with LNS tools and utilities.

f. It shall provide a configurable self-documenting string.

2.3.1.2   Gateway for ASHRAE 135

In addition to the requirements for all gateways, Gateways that use ASHRAE 135 shall meet the following requirements:

a. It shall allow bi-directional mapping of data in the Gateway to Standard Objects as defined in ASHRAE 135.

b. All ASHRAE 135 Objects shall have a configurable Object_Name Property.

c. It shall be BTL Listed.

d. Gateways shall not communicate ASHRAE 135 over an IP network.

e. Gateways communicating ASHRAE 135 to a field control systems shall support the DS-RP-A (Data Sharing–Read Property–A) BIBB and the DS-WP-A (Data Sharing–Write Property–A) BIBB.

2.3.1.3   Gateway for Modbus

In addition to the requirements for all gateways, Gateways that use Modbus shall allow bi-directional mapping of data in the Gateway to Modbus registers using the four standard Modbus register types (Discrete Input, Coil, Input Register, and Holding Register). Gateways communicating Modbus to the M&C Software shall communicate via Modbus over TCP/IP.

2.3.1.4   Gateway for OPC

In addition to the requirements for all gateways, Gateways that use OPC DA shall allow bi-directional mapping of data in the Gateway using OPC DA tags and shall communicate over an IP network in accordance with OPC DA.

2.3.1.5   Gateway for DNP3

In addition to the requirements for all gateways, Gateways that use DNP3 shall allow bi-directional mapping of data in the Gateway to DNP3 object groups and variations as defined by IEEE 1815. Gateways communicating DNP3 over an IP network shall communicate in accordance with the LAN/WAN Networking volume of IEEE 1815.

2.3.1.6   Niagara Framework Supervisory Controller (Gateway)

****

NOTE: FYI - The Niagara Framework Supervisory Gateway is known by many names within industry, and this specification uses the name "Niagara Framework Supervisory Gateway" in order to remain vendor neutral. Probably the most common term used for this device in industry is a "Java Application Control Engine", or JACE, but please do NOT use that term as it is proprietary to Tridium products.

****

Niagara Framework Supervisory Controller Hardware shall:

a. be direct digital control hardware.

b. have an unrestricted interoperability license and its Niagara Compatibility Statement (NiCS) shall follow the Tridium Open NiCS

Specification.

c. manage communications between a field control network and the Niagara Framework Monitoring and Control Software and between itself and other Niagara Framework Supervisory Controller. Niagara Framework Supervisory Controller Hardware shall use Fox protocol for communication with other Niagara Framework Components.

d. be fully programmable using the Niagara Framework Engineering Tool and shall support the following:

(1) Time synchronization, Calendar, and Scheduling using Niagara Scheduling Objects

(2) Alarm generation and routing using the Niagara Alarm Service

(3) Trending using the Niagara History Service and Niagara Trend Log Objects

(4) Integration of field control networks using the Niagara Framework Engineering Tool

(5) Configuration of integrated field control system using the Niagara Framework Engineering Tool

e. meet the following minimum hardware requirements:

(1) Two 10/100 Mbps Ethernet Ports

(2) One port compatible with the field control system to be integrated using this product.

(3) Central Processing Unit of 1000 Mhz or higher.

(4) Embedded QNX operating system.

(5) 1 GB of SDRAM.

(6) Capacity: Under normal working conditions the gateway's central processing unit processor usage percentage shall not exceed 80% and memory usage should not exceed 85% of total memory.

(7) Two RS-485 serial ports.

(8) One RS-232 serial port

(9) One NDIO port

(10) Two communication card option slots

(11) Niagara 4.1 (or later) compatible with current Niagara Supervisor version on NW regional servers.

(12) One LonWorks Interface Port - 78KB FTT-10A

f. provide access to field control network data and supervisory functions via web interface and support a minimum of 16 simultaneous users

g. Required Data Storage

****

NOTE: Retain the 36 hour option for a facility planned in a robust, dense area of the UMCS IP network since the Supervisory Controller is supposed to archive data to the central network storage every 24 hours. Choose two weeks for either a) active building managers who want to look at trend data, or b) more remote locations where network coverage may be more prone to outage.

****

(1) Store data at 15 minute intervals for all hardware input data and output commands for digital outputs for a minimum of 14 days. See Appendix E for trending data specifics.

(2) All stored data shall be automatically submitted to the head-end server each day at a set time.

h. Software, Protocols, and Drivers:

All software used to access the programming of managed devices shall have open licensing, actively supported by the original manufacturer, and not be restricted to only the installing vendor or manufacturer.

The following software is required on all SC's:

(1) Niagara/Fox Protocol

(2) Embedded operating system.

(3) DDC and Facility control systems only (not applicable to SCADA and utility infrastructure systems): Tunnel service to allow programming of device level controllers by a person on a remote computer on the Ethernet network using Niagara Framework Engineering Tool.

(4) LDAP Support

The following software must be provided as necessary on SC's: LonWorks, BACnet, Modbus, Other protocol drivers as needed, oBix, Java Virtual Machine, web services, database services.

2.3.1.7 Wireless Communication

Gateway or controller shall be shipped with wireless communication disabled at the operating system level. NOTE: This is also known as "32300323-003 Wireless Disabled". Wireless communication disabling must be done at the factory and NAVFAC NW will not accept this disabling if done in the field.

2.4 UMCS NETWORK

Wiring between transport switches and buried in conduit shall be optical fiber. Other wiring between IP addressable devices can be optical fiber or copper. All UMCS IP network wiring (for any location) shall support 802.3 Ethernet and minimum speeds of 1 Gbps. All copper cable or wiring used for control network wiring shall be purple (Pantone 269C).

Plenum grade cabling and fire blocking must be used when applicable to the installation location.

2.4.1 Data Cable/Wiring

2.4.1.1 Copper Wiring

Copper wiring is limited to less than 100 meters between active devices. Receive Government approval prior to using media extenders.

Copper wiring shall:

a. Support the 1000BASE-T standard. The use of CAT6 cable is encouraged.

b. Shall follow the T586B standard for pin assignments.

2.4.1.2 Fiber Optic Cabling

Fiber optic cabling provided for the UMCS IP network shall be one of the following:

a. 62.5/125 µm multi-mode fiber (MMF)

b. 9/125 µm single-mode fiber (SMF)

Single-mode fiber shall always be provided unless it cannot meet the speed requirement. Receive Government approval prior to proposing to install multi-mode fiber. Hybrid cabling is allowed.

Unless noted otherwise in the project documents, provide a minimum of 12 fiber pairs.

Terminations: All fiber strands must be terminated in patch panels using LC connectors.

2.5 SOFTWARE

2.5.1 Niagara Framework Engineering Tool

The Niagara Framework Engineering Tool shall be Niagara Workbench or an equivalent Niagara Framework engineering tool software and shall:

a. have an unrestricted interoperability license and its Niagara Compatibility Statement (NiCS) shall follow the Tridium Open NiCS Specification.

b. be capable of performing network configuration for Niagara Framework Supervisory Controllers and Niagara Framework Monitoring and Control Software.

c. be capable of programming and configuring for Niagara Framework Supervisory Controllers and Niagara Framework Monitoring and Control Software.

d. be capable of discovery of Niagara Framework Supervisory Controllers and all points mapped into each Niagara Framework Supervisory Controller and making these points accessible to Niagara Framework Monitoring and Control Software.

e. Niagara Framework Engineering Tool version provided by the Contractor must be compatible with the version of the Niagara Operations Server at the time of commissioning.

2.5.2 Monitoring and Control (M&C) Software

NAVFAC NW is currently using Niagara Framework AX Web Supervisor and communicates with Niagara Framework field control systems using the Fox protocol. Niagara AX version provided by the Contractor must be compatible with the version of the Niagara Operations Server at the time of commissioning.

NAVFAC NW is also currently using SkySpark by SkyFoundry energy analytics software for continuous commissioning activities. See Part 3 of this specification for integration of point data generated by this project into the analytic rules run by SkySpark.

2.5.2.1 Alarms

NAVFAC NW is currently using Niagara Framework AX Web Supervisor in conjunction with Niagara Framework Alarm Portal to handle alarms generated by supervisory controllers and supports the use of Niagara Framework Alarm Classes. See Appendix E of this specification for alarm priority levels (classes) that should be assigned as part of this project.

2.5.2.2 Trending

NAVFAC NW is currently storing trend data on the UMCS servers. See Appendix E for details regarding what and how often to trend certain data points.

2.6 UNINTERRUPTIBLE POWER SUPPLY (UPS)

A UPS or backup source of power is a cybersecurity requirement.

****

NOTE: CIO will provide the UPS time duration. Use 15 minutes if unsure.

****

Where needed, the uninterruptible power supply (UPS) shall be a self-contained device suitable for installation and operation to support the Supervisory Controller and shall be sized to provide a minimum of [15 minutes][_____] of operation of the connected hardware. Equipment connected to the UPS shall not be affected in any manner by a power outage of a duration less than the rated capacity of the UPS. UPS shall be complete with all necessary power supplies, transformers, batteries, and accessories and shall include visual indication of normal power operation, UPS operation, abnormal operation and visual and audible indication of AC input loss and low battery power. The UPS shall be UL 1778 approved.

a. UPS shall have 445 Joules of surge protection.
b. UPS shall be default to a power-on mode following each power outage.
c. UPS shall support the SC and Ethernet switch(es).

2.7 LOCKED RACKS AND ENCLOSURES

2.7.1 Enclosures

A locked enclosure or rack is a cybersecurity requirement. Regardless of whether the locked enclosure is a rack or cabinet-style enclosure, the enclosure must be constructed to secure the interior of the enclosure from all entry except by opening the enclosure using a key to unlock the lock. Enclosures that are not secure from entry or tampering with interior devices on the top, bottom, sides, or rear panel are prohibited.

The enclosure shall be securely attached, and keying of the lock shall match that currently in use at the installation. All doors of the enclosure shall have an intrusion detection sensor, and this sensor shall be integrated into the control system, and shall report alarms on open, and change of state.

Each locked enclosures shall be affixed with a permanent engraved phenolic sign stating the following, all centered within the sign. Signs shall be red with white lettering and 6 inches wide by 5 inches tall. Letters shall be upper case and lower case as written below:

Line 1: Cabinet is Alarmed
Line 2: For Entry Contact UMCS Ops
Line 3: 360-315-7901

Install identification plates using a compatible adhesive.

Enclosures supplied as an integral (pre-packaged) part of another product are acceptable. Keys for lockable enclosures shall be provided to the Government.

2.7.2 Equipment Racks

Equipment racks shall be standard 482 mm 19 inch wall-mount racks compatible with the electronic equipment provided and capable of securing all switches and other Ethernet-connected equipment provided by this project. Racks shall be either aluminum or steel with bolted or welded construction. Steel equipment racks shall be painted with a flame-retardant paint. Guard rails shall be included with each equipment rack and have a copper grounding bar installed and grounded to the earth.

Passive venting shall provide adequate cooling to maintain the manufacturer's maximum thermal limitations for all installed equipment in the cabinet based on calculated total wattages and adequate convective cooling. Top mounted louvers without allowing for a bottom ventilation air circulation path are not allowed.

2.7.3 Enclosure

Device enclosures located outdoors or in wet ambient conditions shall be mounted in rainproof (NEMA 250 3R) enclosures. Device enclosures located outdoors or in wet ambient conditions AND within 100 feet of waterfront shall be mounted in rain-tight corrosion-resistant (NEMA 250 4X) enclosures. Device enclosures used in conditioned space can be mounted in dust-protective (NEMA 250 1) enclosures.

PART 3 EXECUTION

3.1 EXAMINATION

The Contractor shall become familiar with all details of the work, shall verify all dimensions in the field, and shall advise the Contracting Officer of any discrepancy before performing the work.

Designer of Record shall coordinate with NAVFAC NW CIO to confirm design direction provided in contract.

The Contractor shall carefully investigate the mechanical, electrical, and finish conditions that could affect the work to be performed, and shall furnish all work necessary to meet such conditions.

3.1.1 Existing Conditions Report

Perform a field survey, including but not limited to testing and inspection of equipment to be part of the UMCS, and submit an Existing Conditions Report documenting the current status and its impact on the Contractor's ability to meet this specification. For field control systems to be integrated to the CS which are not already connected to the UMCS IP network, verify the availability of the building network backbone at the FPOC location, and verify that FPOCs shown as existing are installed at the FPOC location.

Notify the Government when delivering the Report if existing switch has only one available port or if no ports are available.

3.1.2 Project UMCS Plan

Provide to the Government a summary of the project's control scope including planned UMCS IP network connectivity, desired centralized command and control functionality, systems in the UMCS (HVAC/DDC, SCADA, elevator, etc.), system protocol(s), and the general plan for system control system architecture.[This submittal is required in 23 09 23.02 24 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS (NAVFAC NW). Provide only one submittal.]

3.2 DRAWINGS AND CALCULATIONS

3.2.1 CS Contractor Design Drawings

Provide drawings to include details of the system design and all network hardware components, including contractor provided and Government furnished components. Drawings shall be prepared with AutoCAD v2010 with hard copies on ANSI B (279 by 432 mm11 by 17 inches) sheets. Details to be shown on the Design Drawing include:

a. The logical structure of the network, including but not limited to the location of all Control Hardware (including but not limited to each Control Protocol Gateway, Control Protocol Router, Niagara Framework Supervisory Controller and Monitoring and Control (M&C) Controller). Provide network topology of wiring between an existing UMCS IP network drop and the one proposed for this project. Edit an existing network topology (provided by NAVFAC NW CIO) to show overall network connectivity and routing. Network diagram edit can be done manually, but shall be done clearly enough to be used for record drawing(s) by the BOSC or shop.

b. Manufacturer and model number for each piece of Computer Hardware and Control Hardware.

c. Physical location for each piece of Computer Hardware and Control Hardware.

d. Version and service pack number for all software and for all Control Hardware firmware.

3.2.2 As-Built Drawings

****

NOTE: The Points Schedule is a submittal from Section 23 09 23 LONWORKS DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS contracts and is a contract drawing for this Section. The Contractor updates the Points Schedule and submits it as an as-built.

Where projects require integration to systems not installed under Section 23 09 23 LONWORKS DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS, or where the Points Schedules for the system are not available, create Points Schedules for inclusion in the Contract Drawings.

****

Prepare draft as-built drawings consisting of Points Schedule drawings for the entire UMCS, including Points Schedules for each Gateway, and an updated Design Drawing including details of the actual installed system as it is at the conclusion of Start-Up and Start-Up Testing. As-Built Drawings shall include details of all hardware components, including contractor provided and Government furnished components. In addition to the details shown in the design drawings, the as-built drawing shall include:

a. IP address(es) and Ethernet MAC address(es) as applicable for each piece of Control Hardware (including but not limited to each Niagara Framework Supervisory Controller, Control Protocol Gateway, Control Protocol Router, and Monitoring and Control (M&C) Controller).

b. Niagara Framework Station ID for all Niagara Framework components including but not limited to Niagara Framework Supervisory Controllers and the AX Web Supervisor.

Prepare Draft As-Built Drawings and the Final As-Built Drawings as specified in the Project Sequence in Part 1.

3.3 INSTALLATION REQUIREMENTS

3.3.1 General

****

NOTE: Indicate the location of telecommunications closets on the contract drawings.

****

Install system components as shown and specified and in accordance with the manufacturer's instructions and provide necessary interconnections, services, and adjustments required for a complete and operable system. Communication equipment and cable grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation. Fiber Optic cables and wiring in exposed areas, including low voltage wiring but not including network cable in telecommunication closets, shall be installed in metallic raceways or EMT conduit as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Do not install equipment in any space which experiences temperatures or humidity outside of the rated operating range of the equipment.

3.3.2 Isolation, Building Penetrations and Equipment Clearance

The UMCS shall be completely installed and ready for operation, as specified and shown. Dielectric isolation shall be provided where dissimilar metals are used for connection and support. Penetrations through and mounting holes in the building exteriors shall be made watertight. Holes in concrete, brick, steel and wood walls shall be drilled or core drilled with proper equipment; conduits installed through openings shall be sealed with materials which are compatible with existing materials. Openings shall be sealed with materials which meet the requirements of NFPA 70 and SECTION 07 84 00 FIRESTOPPING.

3.3.3 Nameplates

Provide Nameplates for all Control Hardware and all Computer Hardware. Attach Nameplates to the device in a conspicuous location.

3.3.4 UMCS Network

3.3.4.1 Network UMCS Hardware and Software Inventory

The Government will provide IP addresses for each Ethernet-addressable device and addresses specific to the control protocol for non-IP (MSTP, etc.) network devices. The Contractor shall submit the Network UMCS Hardware and Software Inventory spreadsheet (see 25 50 00.00 20 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS for information) to CIO with the request for network addresses. The Government will return the spreadsheet to the Contractor with network addresses within 10 business days unless there are five or more switches to be deployed. If multiple switches are to be deployed, allow 3 weeks for a meeting between the Contractor and NAVFAC NW CIO and the follow-on IP addresses to be issued. IP addresses will not be provided electronically. If more than five device IP addresses are requested, Government Construction Manager shall facilitate contacting NAVFAC NW CIO directly.[This submittal is required in 23 09 23.02 24 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS (NAVFAC NW). Provide only one submittal.]

3.3.4.2 Switch Configuration by NAVFAC NW CIO

Contractor to deliver all transport and access switches to NAVFAC NW CIO at NBK-Bangor, WA Building 1101. NAVFAC NW CIO will configure all switches prior to field deployment. See Part 1 Project Sequence for more information.

3.3.5 UMCS Network Connection

The Contractor shall provide all equipment and materials needed to complete the connection to the existing NAVFAC UMCS IP network, however only

Government authorized personnel are allowed to complete the actual physical connection between the Contractor's installation and the Government Control Systems network. The Building Control System shall be fully operational and successfully passed the UMCS Pre-Functional Tests in Appendix A and Performance Verification Testing required by 23 09 23.02 24 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS (NAVFAC NW)prior to requesting connection (see Table 1, "Project Sequencing"). Once connected to the UMCS IP network, all contractor laptops will no longer be permitted to be connected to the Building Control System. Provide two weeks' notice to the Contracting Officer when scheduling this connection and include it in the project's schedule.

****

NOTE: Contact NAVFAC NW CIO3 (see portal) for help figuring out what spare ports exist on the switch that this project will make its connection to existing infrastructure.

****

Connectivity to the existing UMCS IP network shall be made in Room [_____] of Building [_____]. The available port characteristics are as follows: [_____].

****

NOTE: Use the next paragraph to describe additional switch capacity or other infrastructure issues that this Contractor and project are required to solve that are not shown on the drawings.

****

[The existing network infrastructure requires additional work to provide the [capacity][connectivity] required by this project. Contractor is required to [_____].

]3.4 INSTALLATION OF EQUIPMENT

3.4.1 Wire and Cable Installation

System components and appurtenances shall be installed in accordance with NFPA 70, manufacturer's instructions and approved network topology. Necessary interconnections, services, and adjustments required for a complete and operable signal distribution system shall be provided. Components shall be labeled in accordance with TIA-606. Penetrations in fire-rated construction shall be firestopped in accordance with Section 07 84 00 FIRESTOPPING. Conduits, outlets and raceways shall be installed in accordance with Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Wiring shall be installed in accordance with TIA-568-C.1 and as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Wiring, and terminal blocks and outlets shall be marked in accordance with TIA-606. Non fiber-optic cables shall not be installed in the same cable tray, utility pole compartment, or floor trench compartment with power cables. Cables not installed in conduit or raceways shall be properly secured and neat in appearance.

3.4.2 Grounding

Signal distribution system ground shall be installed in accordance with TIA-607 and Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Equipment racks shall be connected to the electrical safety ground.

3.4.3 Power-Line Surge Protection

Equipment connected to ac circuits shall be protected against or withstand power-line surges. Equipment protection shall meet the requirements of IEEE C62.41. Fuses shall not be used for surge protection.

3.4.4 Control Hardware and Software

Control Hardware (network switch(es), supervisory controller and UPS) shall be installed a locked cabinet (see Part 2 for options). All power and network connections to the control hardware within the cabinet shall be within the cabinet also and not accessible outside the locked cabinet. This requirement is waived if the room containing the locked cabinet has restricted access. Deliver all key(s) to locked enclosure to the Government. Locked cabinet locations shall comply with standoff distance requirements in UFC 4-010-01 *DoD Minimum Antiterrorism Standards for Buildings*. Configure Control Hardware as specified, as required to meet the functions for which the hardware used and as follows:

a. Disable all ports, protocols, and network services other than those required or specifically permitted by this Section. Services to be disabled include but are not limited to: FTP, Telnet, and HTTP. HTTP may be enabled for Niagara Framework Supervisory Controllers only if HTTPS is unavailable. Products unable to support disabling of ports are prohibited.

3.4.4.1 Ethernet Switches

****

NOTE: Check with NAVFAC NW CIO about critical, uninterrupted or redundant power needs for any of the installed switches. They will define the type of power required (power distribution units, multiple UPS', another panel, local generator (if planned), etc.

****

If more than one switch will be installed in the same location, each switch shall be linked by two 1,000 Mb connections utilizing link aggregation. Switches linking substations or to the Operations Centers shall be configured with dedicated dual 10 GB fiber connections utilizing link aggregation on two separate fiber paths into and out of each of the primary substations, capable of and configured to provide 20 GB service and automatic failover.[The UMCS Transport Switch[es] planned for this project require a redundant power supply.][The second source of power shall [_____].]

Only the Supervisory Controller(s) shall be connected to the access switch. No other lower controller(s) shall be provided an IP-address and/or connected to the switch in order to publish data on the UMCS IP network.

Installation of switches in series at the same location ("daisy-chaining") is prohibited.

Ethernet switches located in Substations and water system buildings shall be tiered so that in the event one switch fails, the system will still share data through an alternate switch and data path, and connections shall be fault tolerant with dual path to each device including switches, relays and similar equipment that are available with 2 Ethernet ports.

3.4.4.2 Supervisory Controller(SC)

Provide one or more SC's as part of this contract. Number of controllers required is dependent on the type and quantity of devices installed. Separate building controls systems from utility systems and vice versa on separate SC's; do not co-mingle on one SC.

****

NOTE: Keep the following paragraph if this is a facility that would be harmed by single point of failure in the control system.

****

[Supervisory controllers shall not be programmed to handle functionality of subordinate device controllers. Subordinate controllers shall be programmed such that the loss of the supervisory controller does not inhibit normal operations.

] Power supply shall be fused or current limiting and shall be rated at a minimum of 125% of SC power consumption.

Do not divide control of a single mechanical system such as an air handling unit, boiler, chiller, pump system, or terminal equipment between two or more controllers. A single controller shall manage control functions for a single mechanical system. It is permissible, however, to manage more than one mechanical system with a single controller.

Unnecessary data transmission above the SC and across the CS Network shall be limited. Only one port of the SC shall be connected to the upstream network switch.

Multiplexing of points is not allowed.

****

NOTE: Keep the following paragraph if the project if the supervisory controller being replaced used to be networked in so as to report through an SC in another building. If this communication pathway is not broken, it will result in a mess of data on the network. This situation is most commonly found on NBK-Bangor on old copper connections.

****

[Remove existing data communication and reporting through other "upstream" supervisory controllers that result in the data and/or alarms of this project's supervisory controller being duplicated on the UMCS IP network.

]3.5 COORDINATION

Contractor shall keep Operations Center UMCS personnel apprised of on-going activities and any expected impacts to normal operation. Impacts to normal operation are required to be requested and coordinated in advance.

3.5.1 Coordination With Division 23, 26 And 33 Contractors

Coordinate with Division 23, 26, and 33 Contractors (when separate from

UMCS contractor) supplying products or systems in order to integrate their work into the UMCS. Specifically:

+ Coordinate type and quantity of SC's required for a complete installation.
+ Coordinate all UMCS IP network schematic diagrams that include Division 23 or 26 work.
+ Coordinate all monitoring and control functions including scheduling, alarms, and the level of device/equipment controllability.
+ Coordinate and integrate all factory-installed controllers furnished with equipment (e.g., boiler control panels, chillers, packaged air-handling units) into the UMCS communication architecture.
+ Coordinate compatibility of factory-installed controllers prior to shipment.
+ Coordinate specific maintenance timeframes and alarms for all new equipment requiring maintenance.

3.6   PROGRAMMING

Provide graphics as specified in Appendix B and Appendix C. Display on each equipment's graphic page all of the associated input and output points and relevant calculated points. Point information on graphics shall dynamically update.

In addition to providing a graphical user interface specific to this project installation, update the existing Niagara Framework Supervisor-generated UMCS graphical user interface pages to incorporate the new work associated with this project. This shall include: 1-line diagrams corresponding to those already in the system, updating the values on graphical screens where there is now new data (or improved data), show amps/watts/kVA and other relevant data into and out of each substation or utility site, control of devices previously just monitored, and update data to be added to unit summary screens, utility screens, and all other aspects of the UMCS system that are impacted by this project. See Appendix C for examples of existing screens.

System shall generate maintenance alarms when equipment exceeds adjustable runtime, equipment starts, or performance limits.

Programming code files shall contain the programming code installed on each individual control device including documentation stating which system and/or device the code file applies to.

3.6.1   Supervisory Controller

Supervisory controllers ("station") will operate using Niagara-AX modules sanctioned by NAVFAC NW. Customized or altered Niagara-AX modules are prohibited, including copying modules existing on an existing supervisory controller. Submit a request to the Government Contracting Officer through the submittal process if a customized module is desired. The request will be reviewed and approved by the Government prior to its use on the supervisory controller.

Provide a copy of the final supervisory controller station to be retained by the Government.

Synchronize controller time clocks daily from the Windows domain servers where capable or from the Niagara servers in the Operations Center.

Monitor controller and I/O point operation. System shall annunciate controller failure and I/O point locking (manual overriding to a fixed value).

3.6.2   Generators

Design an appropriate graphical user interface in the Operations Center graphical user interface to support quickly and easily selecting which generator systems to bring online during an outage, and automatically select which circuit breakers or sectionalizing switches to open or close to best support the customers.

3.7   INTEGRATION OF FIELD CONTROL SYSTEMS

****

NOTE: For complete integration the contract package must include the following:

1. Points Schedule - make sure Points Schedule includes:

- **points to be displayed by the M&C Software**
- **points that can be overridden by the M&C Software**
- **trend points.**
- **Alarm routing (also make sure to include the Alarm Routing Schedule)**

2. Alarm Routing Schedule drawings. Identify and assign priorities.

3. Control System Schematics for each field control system (This may be an as-built drawing from the field control system specification.)

5. Occupancy Schedules for each field control system. (This may be an as-built drawing from the field control system specification - such as Section 23 09 23)

While integration *may* be able to be performed without the other drawings, the Points Schedule is required for successful integration of any system and must be provided.

Note that the necessary Points Schedule drawing should be part of the as-built submittal for building control systems. If a points schedule for the system is not available one must be created and included in the contract package. Alternatively, a requirement can be manually added here (along with appropriate edits to the submittals and project sequencing paragraphs) to include a site survey of the system prior to integration, the results of which the Government must then use to provide actual integration requirements such as identifying points to be displayed, overridden, trended etc (thus creating a Points Schedule as part of the project).

****

****

NOTE: FPOCs may have been installed with the field control system. Contract drawings must indicate the FPOC locations for each field control network and whether or not a FPOC already exists at that location.

****

Install, initialize, start up, and troubleshoot operator interface software and functions (including operating system software, operator interface database, and third-party software installation and integration required for successful operator interface operation).

Contractor to integrate all control points including those associated with the sequence of operation, alarms and other data generated by field devices (whether controlling or reporting) that were specifically listed or named in the final approved shop drawings so that it is available on the UMCS IP network.

Fully integrate the field control systems in accordance with the following three step sequence and as specified and shown.

STEP 1: Install and configure Control Hardware as necessary to provide a Field Point of Connection to connect the field control system to the UMCCS IP network and, when necessary, to provide control protocol translation and supervisory functionality.

STEP 2: Add Field Control System to M&C Software: Perform system discovery, system database merges, or any other actions necessary to allow M&C Software access to the field control system.

STEP 3: Configure M&C Software to provide monitoring and control of the field control system, including but not limited to the creation of system displays and the configuration of scheduling, alarming, and trending. See Appendix E for Trending Requirements.

3.7.1 Integration Step 1: Install Control Hardware

Install Control Hardware as specified at the FPOC location to connect the field control system to the UMCS IP network and, if necessary, to provide control protocol translation and supervisory functionality. Depending on the field control system media and protocol this shall be accomplished through one of the following:

a. Connect the existing field control network FPOC to the UMCS IP network. (Note: The existing FPOC will generally be a network switch.)

b. Install Niagara Framework Supervisory Controller/Gateway connected to both the field control network and the UMCS IP network.

3.7.1.1 Installation of Niagara Framework Supervisory Controller/Gateway

Install Niagara Framework Supervisory Controller hardware to connect the field control network to the UMCS IP network. Install additional field control system network media and hardware as needed to connect the Niagara Framework Supervisory Controller to the field control system.

****

NOTE: Retain the following paragraph if the supervisory controller provided on this project is being installed to take over communication for a facility that was daisy-chained or connected to another building and data was passed through that connection. Provide information to the contractor about which existing supervisory controller needs to be cleaned up.

****

[Existing control data and programming for this project is currently being communicated to the Control System network through the existing supervisory controller located [_____]. Remove all programming and communication installed on this project's supervisory controller from the existing supervisory controller so there is no duplication after project closeout.

]3.7.1.2 Installation of Control Protocol Router

If there is not an existing connection between the CS IP Network and the field control network, install a switch to connect the field control system to the UMCS IP network. Install additional field control system network media as needed to connect the field control system to the Supervisory Controller.

3.7.2 Integration Step 2: Add Field Control System to M&C Software

Perform system discovery, system database merges, or any other actions necessary to allow M&C Software access to points and data in the field control system.

3.7.2.1 Integration of Field Control Systems Via Niagara Framework

For each Niagara Framework Supervisory Controller installed in integration step 1 for this project do both of the following:

a. Use the Niagara Framework Engineering Tool to fully discover the field control system and make all field control system information available to the Niagara Framework Supervisory Controller.

b. Create and configure points and establish network communication between the Niagara Framework Supervisory Controller and the field control system to provide points from the field control system to the M&C software and to provide support for supervisory functions, including but not limited to schedule objects, trend logs and alarming.

For each Niagara Framework Supervisory Controller to be integrated as part of this project, make all information in the Niagara Framework Supervisory Controller available to the M&C Software.

3.7.3 Integration Step 3: Configure M&C Software

Configure M&C Software to provide monitoring and control of the field control system, including but not limited to the creation of system displays and the configuration of scheduling, alarming, and trending.

3.7.3.1   Configure M&C Software Communication

Create and configure points and establish network communication between M&C Software and Field Control Systems as specified to support M&C Software functionality:

a. Points on currently active displays shall be updated via polling as necessary to meet M&C Software display refresh requirements.

b. Points used for overrides shall be sent to the device receiving the override as shown on the Points Schedule.

3.7.3.2   Configure M&C Software Functionality

Configure M&C Software functionality as specified:

a. Create System Displays using the standards described in Appendices B and C. Label all points on displays with the approved point name acronyms from Appendix D. Configure user permissions for access to and executions of action using graphic pages. Coordinate user permissions with UMCS shop supervisor.

b. Configure alarm handling such that all alarms are routed to the installation operations server and all critical alarms (as listed in Appendix E) are also routed to the NW Region operations server.

c. Create M&C Software trends for required points as shown on the Points Schedule and as specified in Appendix E. Create and configure displays for creation and configuration of trends and for display of all trended points.

d. Configure all field devices to routinely send their data to the SQL server via the historical data archiving server.

3.8   FIELD QUALITY CONTROL

Demonstrate compliance of the installed UMCS components with the contract documents. Furnish personnel, equipment, instrumentation, and supplies necessary to perform testing. Ensure that tests are performed by competent employees of the system installer or the system manufacturer regularly employed in the testing and calibration of Control System. All points shall work end-to-end. The Government may choose to witness the working of any and all points.

Contractor shall keep and maintain a Password log for all devices (supervisory controllers only) and submit to the Government. Password Logs shall be transmitted as required in Part 1.

3.9   FUNCTIONAL PERFORMANCE TESTS (FPT)

3.9.1   Network Switch FPT

Upon completion of FPT and as specified, prepare and submit the FPT Report documenting all tests performed during the FPT and their results. Failures and repairs shall be documented with test results.

3.9.2   M&C Software Integration FPT

Test compliance of the M&C supervisory software for:

a. The ability to demonstrate seamless communications with the existing UMCS servers at the Operations Center as well as direct connect via the Supervisory controller in the facility where the work is being accomplished.

b. Editing Control programs: Demonstrate the ability to edit the control program off line.

c. Reporting of alarm conditions: Cause alarm conditions for each alarm, and ensure that workstations receive the alarms.

d. Reporting trend and status reports: Demonstrate ability of software to receive and save trend and status reports.

e. Successful execution of Skyspark analytic processes against trend data archived from the supervisory controller.

Complete the checklists in Appendix A for both Pre-Functional Tests and Functional Performance Tests.

3.9.3 Work Coordination

Schedule and arrange work to cause the least interference with the normal Government business and mission. In those cases where some interference may be essentially unavoidable, coordinate with the Government to minimize the impact of the interference, inconvenience, equipment downtime, interrupted service and personnel discomfort.

-- End of Section --