SECTION 25 1219
INTEGRATION PROTOCOLS

PART 1 - GENERAL

1.1 SUMMARY
A. Section includes Network protocols for all DDC Systems.
B. Related Sections:
   1. 25 1223 Client-Server Information Database Integration
   2. 25 1313 Building Level Controller

1.2 REFERENCES
A. ANSI/CEA Standard 709.C LonTalk protocol

1.3 DEFINITIONS
A. LONWORKS®: The generic technology that incorporates LONMARK® certified products that communicate using LonTalk Communications protocol. The technology employs routers, gateways, bridges, and multimedia transceivers, permitting topology and media independent control solutions.
B. LonTalk® Protocol: Protocol implemented on LONWORKS® networks to standardize communications. It defines a standard way for devices to exchange information. The LonTalk protocol is an openly published non-proprietary protocol.
C. LONMARK® International Association: An organization dedicated to issuing guidelines to ensure that devices from different vendors can coexist and operate on a single LONWORKS® network. The organization establishes functional profiles and LONMARK® certification to devices in order to ensure interoperability between vendors.
D. Modbus Serial communication protocol developed by Modicon. Modbus protocol utilizes 3 frame formats:
   1. Modbus RTU Used to connect a supervisory computer with a remote terminal unit (RTU) for supervisory control and data acquisition.
   2. Modbus TCP/IP (More commonly Modbus TCP) is Modbus protocol encapsulated in a TCP frame.
   3. Modbus ASCII Not used for Stanford control systems.
E. IP Internet Protocol
F. TCP Transmission Control Protocol
G. TCP/IP Transmission Control Protocol / Internet Protocol
H. PICS Protocol Implementation Conformance Statement
I. SNMP Simple Network Management Protocol is a network-management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance and security on a network. SNMP uses a distributed architecture consisting of entities called "managers" and "agents".
J. oBIX Open Building Information Xchange
K. FOX   Fox is the TCP/IP protocol which is used for all network communication between Stations as well as between Workbench and stations. Fox is a multiplexed peer to peer protocol which sits on top of a TCP connection.

L. FOXS   Secure Fox SSL. The Fox protocol run over an SSL encrypted connection following certificate based server authentication. The Niagara implementation of the industry-standard Secure Socket Layer (SSLv3) and Transport Layer Security (TLSv1) protocols provides server authentication and encryption/decryption of data transmitted between client and server.

M. Workbench    Tridium's brand name for the Niagara configuration tool, a Java VM which hosts Niagara plugin components. The Distech-specific brand name for Workbench is EC-NetAX Pro.

N. BAJA   Building Automation Java Architecture. The core framework that the Niagara framework is built upon is published as an open standard. This standard is being developed through Java Community Process JSR 60.

O. HTTP  Hypertext Transfer Protocol is an application-level protocol for distributed, collaborative, hypermedia information systems. HTTP is the standard protocol used by web browsers to access web pages from a station.

P. HTTPS  Hypertext Transfer Protocol Secure is a communications protocol for secure communication over a network. It is the result of layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

Q. HTML  HyperText Markup Language is the standard markup language used to create web pages. Web browsers can read HTML files and compose them into visible web pages.

R. XML  Extensible Markup Language is a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable. XML code is similar to Hypertext Markup Language (HTML). XML is a text-based format that allows for the structuring of electronic documents and is not limited to a set of labels. XML is used to describe data. The XML standard is a flexible way to create information formats and electronically share structured data via the public Internet, as well as via corporate networks. Both XML and HTML contain markup symbols to describe page or file contents. HTML code describes Web page content (mainly text and graphic images) only in terms of how it is to be displayed and interacted with.

S. PX   Presentation XML. A PX file is a special XML file, used by Niagara, to display webpages. PX describes the components in a database and can be any collection of components, up to a complete database. A PX view can be used to provide a complete variety of options in the development of dynamic user interfaces.

T. Niagara Framework    The Niagara Framework is a system designed to manage and control information. Its primary application is for control systems because of its powerful and flexible integration capabilities. The system is made up of Stations that run the components of the Niagara Framework and views that provide the ability to view and command these components.

U. Niagarad    The protocol used for workbench-to-daemon communication.

V. Daemon   Typically refers to the Niagara platform daemon, a native daemon server process required by a Niagara host to run a station. The daemon is used to boot stations and to manage platform configuration such as IP settings.

W. Normalization   In Niagara, this term is used to indicate “data normalization”. This is the process of making data and features from various different communications protocols work together so that they can be integrated. The Niagara framework provides a way to normalize data across various protocols so that it may be viewed and controlled from a single user interface.

X. Host   This is a term for a hardware system (or platform) that provides the operating environment for a Niagara application. In a navigation tree, the host node is used to depict the platform,
which is the first level of the navigation tree. Hosts always represent a physical piece of hardware. Localhost is a term used to indicate the local machine.

Y. **Platform**  The name for everything that is installed on a Niagara host that is not part of a Niagara station. The platform interface provides a way to address all the support tasks that allow you to setup, support and troubleshoot a Niagara host.

Z. **Station**  A station is the main unit of server processing in the Niagara architecture. A station runs the components of the Niagara Framework and provides the access for client browsers to view and control these components. The primary parts of a station include components and services. It is the combination of a database, a web server, and a control engine. The station either runs on a Web Supervisor PC or a JACE controller.

AA. **Supervisor**  In Niagara, the Supervisor or Supervisor PC is a flexible network server used in applications where multiple Niagara-based stations are networked together. The Niagara Supervisor serves real time graphical information displays to standard web-browser clients and also provides server-level functions such as centralized data logging, archiving, alarming, real time graphical displays, master scheduling, and integration with enterprise software applications. Optional SQL and Oracle drivers enable seamless data transfer to these industry standard databases. In addition, the Niagara Supervisor provides a comprehensive, graphical engineering toolset for application development. On the Stanford Building Controls Network Architecture drawing, the Supervisor PC is designated as Building Controls System Server. Common industry generic terms for the Supervisor PC include: Operator Workstation, Front End Computer, Head End Computer, Host PC etc.

BB. **Supervisor Station**  The station that is running on the Supervisor PC

CC. **JACE**  JAVA Application Control Engine. A variety of headless embedded platforms. Typically a Jace runs on a Flash file system and provides battery backup or other means of orderly shutdown upon sudden power loss. Jaces usually host a Station and a Niagara Daemon process, but not Workbench. Jaces typically run QNX as their operating system. The Distech-specific brand name for a JACE is EC-Bos.

DD. **Thin Client**  A thin client (sometimes also called a lean, zero or slim client) is a computer program that depends heavily on another computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself.

EE. **NAT**  Network Address Translation. A methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. Used extensively by Stanford University.

FF. **NAT-T**  NAT Traversal is a general term for techniques that establish and maintain Internet protocol connections traversing network address translation (NAT) gateways, which break end-to-end connectivity. Intercepting and modifying traffic can only be performed transparently in the absence of secure encryption and authentication. Use of any NAT traversal technique is prohibited on any Stanford Control network.

GG. **BACnet**  Building Automation and Control Network communication protocol.

HH. **BTL**  BACnet Testing Laboratory

II. **BBMD**  BACnet broadcast management device. Use of BBMDs on BACnet/IP networks, is not permitted. Use of any other device or software that facilitates global message broadcasts across multiple IP subnets, is not permitted on any Stanford control network.

JJ. **Protocol**  An agreed-upon format for transmitting data between two devices.

**Note:** Edit list to meet project requirements.

### 1.4 SYSTEM DESCRIPTION

A. Refer to Stanford Network Architecture diagrams (MC-01) for additional details.
1.5 SUBMITTALS

A. Integration Plan

1. Network architecture diagram. Network architecture includes but is not limited to:

- Nodes. Each TCP/IP node shall include:
  1) Device Description
  2) Device Name
  3) IP Address
  4) Domain Name (if applicable)
  5) Physical Location (Room Number or Location Description)

- Switches and Routers

- Integrated systems and/or sub-systems

- Dedicated I/O locations

2. Coordination of vendor protocol and point list submission. Include an integration matrix detailing systems and protocols to be used.

3. Workflow processes to integrate systems

4. Include communication hardware, software, and protocols to implement full systems integration.

5. Identify proposed enhancements or deviations from project documents. Include specific drawings or specifications impacted.

6. Include latest version of LonMark Functional Profiles used for each type of controller and operator interface included in the submittal.

7. Include latest version of protocol profiles used: BACnet Protocol Implementation Conformance Statement (PICS) for each type of controller and operator interface included in the submittal.

8. Modbus registry list for each Modbus device. Include:

- Name (Name should convey meaningful description of point)

- Type i.e. Analog Input, Digital Output, etc., (Define whether Master or Slave perspective)

- Modbus Register

- Comment Field.

  - For digital points indicate numeric relation to Binary State, i.e., 0=Alarm, 1=Normal.
  
  - For analog points, indicate embellished description i.e., # Cooling Requests.
  
  - For analog points representing Enumerated States indicate numeric relation, i.e. 0=Occ, 1=UnOcc, 3=Standby

- Logic i.e. Summation, High Select, Modbus points stale > 5 min, etc.

- Master Side Scaling Factor of each analog point

- Slave Side Scaling Factor of each analog point

- Read/Write Indicate Read or Write (Define whether Master or Slave perspective)

9. For each typical system/device that will be integrated, provide point list matrix of available points for integration that includes: Point name, descriptor device ID, object ID and point type.

1.6 QUALITY ASSURANCE

A. BACnet products shall be BTL compliant.

B. Lon products shall be LonMark compliant

C. Coordinate other system requirements with owner.

Note: Section specific quality requirements should be defined here but not repeated from other sections.

1.7 WARRANTY

A. Include protocol fixes and version upgrades during warranty period.
PART 2 - PRODUCTS

2.1 – Not Used

Note: Consultant to consider adding the following language into equipment specifications (VFDs, Chillers, Boilers, CRAC units, Lighting Controls, Lab Controls, etc):

DDC Systems Integration

Comply with 25 1219 for protocol and product certifications and listings.

Provide point list matrix of available points for integration that includes: Point name, descriptor device ID, object ID and point type

Include latest versions of protocol profiles used. Provide BACnet Protocol Implementation Conformance Statement (PICS) for each type of controller and operator interface. Include complete set of BACnet Implementation Building Blocks.

Coordinate polling rate requirements to minimize traffic of integrated equipment.

Provide support and coordination for Integration Automation System specified in division 25. Assist in system setup (addressing, naming, etc).

PART 3 - EXECUTION

3.1 CAMPUS CONTROLS TCP/IP NETWORK COMMUNICATION

A. Niagarad protocol is permitted on Campus Controls Network.
B. FOX/FOXS protocols are permitted on Campus Controls Network.
C. HTTP/HTTPS protocols are permitted on Campus Controls Network.
D. BACnet IP protocol is not permitted on Campus Controls Network.
E. Modbus TCP protocol is not permitted on Campus Controls Network.

3.2 BUILDING LEVEL CONTROLS TCP/IP NETWORK COMMUNICATION

A. Building level controls network is a private TCP/IP network.
B. Niagarad protocol is permitted on Building Level Controls Network with no restriction.
C. FOX/FOXS protocols are permitted on Building Level Controls Network with no restriction.
D. HTTP/HTTPS protocols are permitted on Building Level Controls Network with no restriction.
E. BACnet IP protocol is not permitted on Building Level Controls Network.
F. Modbus TCP protocol is permitted on Building Level Controls Network under limited conditions.

3.3 FLOOR LEVEL NETWORK COMMUNICATION

A. LonTalk protocol over LON TP-FT10 network is the preferred protocol of the Floor Level Network.
B. BACnet MS/TP protocol is permitted on the Floor Level Network, under limited conditions, specifically:
   1. Only if necessary to integrate a third party controller that does not have an equivalent controller available from Distech. Equivalency shall be determined by Owner.
   2. And, only if a LON solution is not available from vendor.
   3. Only controllers/devices from one single manufacturer are permitted on any MS/TP network. Additional controllers/devices from another manufacturer require a separate MS/TP network.
C. BACnet IP protocol is permitted on the Floor Level Network, under limited conditions, specifically:
   1. Only if necessary to integrate a third party controller that does not have an equivalent controller available from Distech. Equivalency shall be determined by Owner.
   2. And, only if a LON solution is not available from vendor.

D. If project requires, Building Level Controllers shall communicate with Delta V Controller via MODBUS RTU.

END OF SECTION