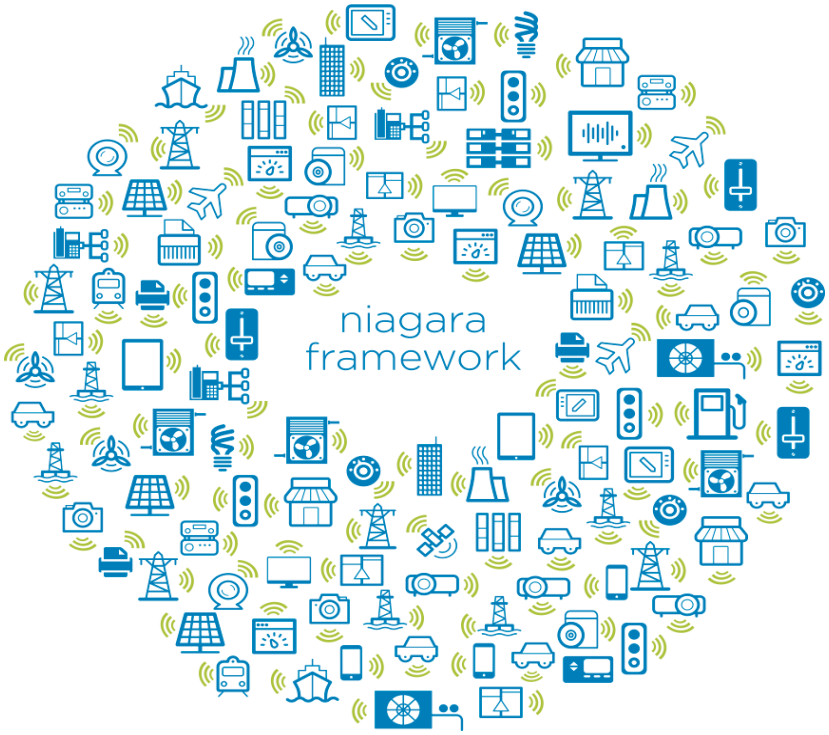
TRIDIUM NIAGARA FRAMEWORK®
SMART BUILDINGS
GUIDE SPECIFICATION



Prepared by:

Tridium Europe Limited

1 The Grainstore,
Brooks Green Road
COOLHAM
West Sussex
RH13 8GR

Telephone: +44 1403 740290
Email: ordersemea@tridium.com
www.tridium.com

REVISION STATUS

Document Control

CONTROLLED DOCUMENT				
Name:	Niagara Framework® Guide Specification			
Document:	E0090			
Status:	Final			
REVISION HISTORY				
Rev	Date	Summary of Changes	Written By	Checked By
1.0	05.06.17	Released		P.Warnes

INDEX

DEFINITIONS 5
2 INTRODUCTION 6
2.1 PURPOSE & TARGET AUDIENCE 6
2.2 USE OF THIS GUIDE SPECIFICATION 6
3 SCOPE 6
3.1 NIAGARA FRAMEWORK® IOT DATA STACK 8
3.2 NIAGARA FUNCTIONS & FEATURES 9
3.2.1 The Niagara Framework® s Architecture supports: 9
3.2.2 Niagara N4 Features 9
3.3 MARKET PLACES 9
3.4 SMART BUILDING BENEFITS 10
3.4.1 On the Cloud Services 10
4 MIDDLEWARE 12
4.1 NETWORKS & FRAMEWORK INFRASTRUCTURE SCOPE 12
4.1.1 Niagara Platform Connectivity 12
4.1.2 Niagara Integration 12
4.2 OPEN PROTOCOL & DATA SECURITY 13
5 GENERAL SYSTEM DESCRIPTION 14
5.1 MIDDLEWARE REQUIRMENTS 14
5.2 MIDDLEWARE INTERFACING 14
6 SMART BUILDING NIAGARA FRAMEWORK® OVERVIEW 15
6.1 GENERAL 15
6.2 ARCHITECTURE 15
6.2.1 Systems Integration 15
6.2.2 Software Components 17
6.2.3 Enterprise Connectivity 19
6.3 FRAMEWORK ARCHITECTURE OVERVIEW 19
6.3.1 Network Infrastructure 20
6.3.2 Middleware Platforms & Management Level 20
6.4 NIAGARA FRAMEWORK® OPERATIONAL REQUIREMENTS 20
6.4.1 Operating System & Security 20
6.4.2 Ports and Protocol Control 21
6.5 ACCESS AND PERMISSIONS 22
6.5.1 User Groups 22
6.5.2 Categories 23
6.5.3 Permissions 23
6.5.4 Authentication 23
6.6 SECURITY & DOMAIN INTERFACING 23
6.6.1 Domain Considerations 24
6.7 SOFTWARE & DATABASE BACKUP 24

7 NIAGARA MANAGEMENT LEVEL REQUIREMENTS 26
7.1 GRAPHICS USER INTERFACE 26
7.1.1 General 26
7.1.2 Graphic Browser Navigation 26
7.2 USER INTERFACE (UI) 27
7.2.1 User Logon 27
7.2.2 SPoG Landing Page 27
7.2.3 Navigation Task Bar 27
7.3 SYSTEM GRAPHICS DEVELOPEMENT 28
7.3.1 Specific Graphical Requirements 28
7.4 APPLICATION REQUIREMENTS 28
7.4.1 Schedules 28
7.4.2 Alarm Handling, Notification and Management 30
7.4.3 Histories 32
7.4.4 Reporting 33
7.5 ENTERPRISE SERVER & WEB BROWSER GUI 34
7.5.1 System Overview 34
7.5.2 Niagara Middleware Server & Network Storage 34

1 DEFINITIONS

Acronym	Description
Tridium	The Company
Niagara Framework®	The Framework Architecture for Edge to Cloud technology
JACE	JAVA Application Control Engine
API	Application Programme Interface
BaaS	Backup as a Service
ES	Enterprise Services
FM	Facilities Management
Fox	Unencrypted Niagara Framework intra-JACE communications
Foxs	Encrypted Niagara Framework intra-JACE communications
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input Output
ICT	Information Communications Technologies
IoT	Internet of Things
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
M&E	Mechanical & Electrical
NAS	Network Attached Storage
NICS	Niagara Information Conformance Statement
OEM	Original Equipment Manufacturer
OSA	Open Systems Architecture
PaaS	Platform as a Service
PICS	BACnet Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
SaaS	Software as a Service
SI's	Systems Integrators
SCADA	Supervisory Control and Data Acquisition
SPoG	Single Pain of Glass
SSL	Secure Socket Layer
SVG	Scalable Vector Graphics
TCP	Tridium Certified Program
TLS	Transport Layer Security
UI	User Interface
UPS	Uninterruptable Power Supply
VLAN	Virtual Local Area Network
VRV	Variable Refrigerant Volume
VSD	Variable Speed Drive

2 INTRODUCTION

2.1 PURPOSE & TARGET AUDIENCE

This guide specification is aimed at Consultants, Developers and Interested Specifying parties such as:

- Consultants
- Design & Build Contractors
- Developers
- Direct End Client / Users
- Middleware Specialists
- System Integrators

This specification serves as a guide to defining project specific requirements and becomes an outline to the deployment of the Niagara Framework® Architecture, equipment and solutions

The aim is for specifying parties to create their own Smart Buildings specification from the outline of this Guide specification which provides information and guidance on the Niagara Framework® components and how to deploy the Niagara Framework® over multi protocoled systems and IoT Edge devices.

The output specification will need to incorporate the client's specific requirements and systems to be integrated, the target of this output should be Niagara Framework® OEM, Resellers and SI's who have the capability to deploy the required solution(s).

This output specification should also be read in conjunction with other services system specifications and their requirements such as BMS, Electrical, Lighting, Mechanical, Fire, Security, FM Systems & Enterprise Systems

2.2 USE OF THIS GUIDE SPECIFICATION

This Guide specification is offered in good faith and without prejudice; the responsibility remains with the system designers to ensure that their project design intent is met. Any Interested specifying partner can use this Guide Specification and relevant clauses in conjunction with their own specification and standards specification sections.

3 SCOPE

This Smart Buildings Guide specification outlines the Functions and Features of the Niagara Framework® which can be deployed across any network connected systems, locally and remotely and accessible via the Internet via WEB Browsers over the IoT(Internet of Things).

A Smart Building approach differs from a traditional building systems and services approach where each M&E, Facilities and Enterprise systems are connected via their own infrastructures, a Smart Building facilitates connectivity of any system over common communications Infrastructure (Cabling, Network Infrastructure) using industry standard open protocols and Application Programme Interfaces (API's) allowing data to be shared and manipulated to provide cause and effects between systems.

Communications infrastructures can include client's server environments (Server Farms) which are designed, supplied and installed by an Information and Communications Technology (ICT) and Cloud Specialist and includes/considers deployment of the following components parts which require separate scoping:

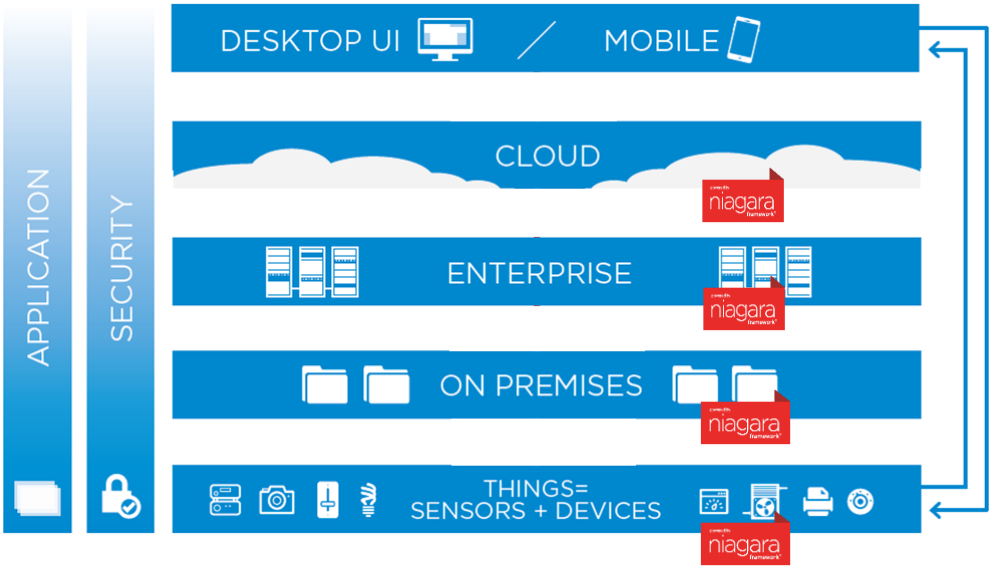
- Data Centres and Cloud Infrastructure
- Building Level Network Backbone Fibre/CAT6 cabling Infrastructure
- Active Network / Switch Infrastructure
- Direct Connectivity of Sub-Systems via IP
- Connectivity of Building, Corporate or Internet Software Services (SaaS) on the same infrastructure Data via "Middleware" platforms to allow data connectivity
- Logical Separation of Data Services (Building / Clients Services) via Firewalls / Virtual Local area Networks (VLAN's)
- Implementation of common Network Security / Management in line with Client Policies
- Virtualised Server \ Cloud Environments onto which all applications and services are deployed from
- Common User Interfaces and Facilities Management Operation

This guide specification mentions the above but does not detail any design or deployment requirements, it will be the responsibility of the designer to ensure that the above are considered as part of an overall Smart Building delivery.

3.1 NIAGARA FRAMEWORK® IoT DATA STACK

Building Services Technologies and Systems Data Integration can provide many possibilities and benefits for system data to be connected to allow inter-process control and interaction as well as providing common management level visualisation and operation via Desktops and Mobile devices.

There are different levels of integration available depending on the various systems, services and applications, the Niagara Framework® is architected around the IoT and takes the form of the following:



This is a representation of a typical IoT solution with the many layers required to get data from many disparate systems and IoT devices to either a Desktop User Interface (UI) I or Mobile device through the IoT Layer Stack.

The Niagara Framework® supports device and data connectivity across all layers of the Niagara Framework® Tridium are developing Niagara down to the Edge with Micro and Lite versions to facilitate applications at the Edge of the IoT layer stack.

3.2 NIAGARA FEATURES & FUNCTIONS

The Niagara Framework® facilitates an Open, no lock-in framework architecture allowing multi-vendor systems and solutions to be connected and supported by a community of Systems Integrators and Developers, allowing clients freedom of choice to either retain existing systems and infrastructures or to upgrade in the future using the latest technologies and infrastructures. The Niagara Framework® was designed to allow integrators and developers to connect, manage, and control any device, regardless of manufacturer, using any protocol.

3.2.1 The Niagara Framework® s Architecture supports:

- Cloud Deployment
- Enterprise Systems & Services
- Facilities & Asset Management Services
- Visualisation, Alarming, History, Reporting Applications
- On-Premises Deployment
- IoT and Connectivity of Edge Devices
- IoT Apps
- Customizable Security Controls to meet Organization Security Policies
-

3.2.2 Niagara N4 Features

- Structured / Relational Tagging
- Templating
- Analytics
- User Interfaces
- IT Compliance
- Built-in Cyber Security Controls for Confidentiality, Integrity, Authentication, Authorization, Auditing, and Malware prevention.

3.3 MARKET PLACES

The Niagara Framework® is a flexible and extensible IoT framework that can support many business domains, it facilitates multi-disciplined Systems connectivity, and can provide solutions in the following sectors:

- BMS / HVAC (Plant Level)
- Security (CCTV/ACCESS)
- Lighting / Blinds
- AV
- Fire
- Elevators
- Home Automation
- Energy Management
- Electrical Management
- Building Performance and Monitoring

- Facilities Management
- Data Centres (DCIM)
- Renewables
- Demand Side Response
- Bureau Management
- Smart Devices

3.4 SMART BUILDING BENEFITS

Benefits when adopting a "Smart Building" approach on the Niagara Framework® could include any of the following value propositions:

- Open, no lock in to a specific manufacturer, freedom of choice in future system upgrades
- Backup as a Service (Baas) included.
- Extensible and flexible – can be extended to support any device and protocol, allowing owners to adjust as technology changes
- Browser Based User Interface and visualisation using HTML 5, no Browser Plugin required
- All open protocols included as standard e.g. BACnet, KNX, LON, M-Bus, Modbus, oBiX, SNMP etc.
- Can be used with Multiple Protocols on one platform, e.g. JACE or Server, either open and/or legacy types providing cost effective integration
- JACE 8000 can be supplied with or without Wi-Fi on Board option.
- Native built in Analytics at Platform and Supervisor Levels
- Many different Protocol Drivers are available, refer to latest drivers list: https://www.tridium.com/~/media/tridium/common/documents/tridium%20and%203rd%20party%20drivers.ashx?la=en
- One WEB Based Software engineering tool for Integration, Visualisation, Cyber Security, Enterprise data exchange and analytics.

3.4.1 On the Cloud Services

The Niagara Framework® also facilitates following:

- Browser based engineering

  Flexible secure access either locally and/or remotely
- Cyber Security capabilities that provide strong authentication, role-based authorisation, encrypted communications, encrypted sensitive information at rest, digitally-signed code validated at run-time, and auditing – customisable for meeting the Cyber Security policies of any organization
- Real time Cloud Based information for better business decisions

- Lower total cost of ownership
- Opportunity to improve business processes
- Savings in Operational management

Automation and Optimisation of Systems and Processes

4 MIDDLEWARE

4.1 NETWORKS & FRAMEWORK INFRASTRUCTURE SCOPE

The section outlines the Niagara Framework® and Middleware JACE platform infrastructure concept required to connect and gather date from multiple data sources and services to handle and manage data across multi-disciplined systems.

4.1.1 Niagara Platform Connectivity

Where systems and application require serial data and/or TCP/IP connectivity, these can be accommodated concurrently via the JACE Platform.

- BACnet / RS485 / TCP/IP
- Dali / RS485 / TCP/IP
- LON / TCP/IP
- KNX / RS485 / TCP/IP
- M-Bus / RS232 / TCP/IP
- Modbus / RS485 / TCP/IP
- oBIX / TCP/IP
- SNMP /TCP/IP

4.1.2 Niagara Integration

Building Services Systems Data can be “Integrated” at many levels:

- Hardwired between different systems Input/Outputs to provide C&E functionality
- High Level Integration at the Automation Level using Manufactures own developed Gateways and Protocols
- High Level Integration at the Automation Level using 3rd Party Integration Platforms
- High Level Integration between Automation and Management Levels using Gateways
- Management Level via SQL / oBIX Data Exchange (Many Systems still use File Transfer)
- Integrated Data may then be used to display data on the SPoG via Graphical User Interfaces and automated control interaction between Systems (Cause & Effect)
- It should also be mentioned that the Niagara Framework® is a completely extensible open platform. Using our open APIs, any Niagara developer can write a software module to support any new protocol or device, providing flexibility in enterprise integration.

4.2 OPEN PROTOCOL & DATA SECURITY

To facilitate secure deployment of Software Services (SaaS) utilising Niagara Framework® during Smart Building deployment and as part of any future IoT deployment requirements, all connected systems and services shall comply with the following interfacing & security requirements:

- Support of IT / Networking Industry Standard Open Protocols and IP Connectivity at all levels of each System / Product Architecture including Enterprise Level licensing and SQL / Enterprise interfacing.
- Support of Windows / Linux RHEL Operating Systems
- Support of Open Standard Services Protocols over Ethernet/IP or Serial Networks for Middleware deployment.
- Support of Object data types over Niagara Framework® such as Analogue and Binary Input/Outputs, Internal Calculated Values, Set points, Alarms (Including Acknowledgements and Resets), Time Schedule Objects and Trend Log Objects which shall all be available for Middleware Platform data Integration and automation as well as Management Level Visualisation and Operation
- Where BACnet Systems are deployed either at the Platform or Supervisor levels, the Protocol Implementation Conformance Statement (PICS) Statements for each connecting system shall be used to verify compliance.
- Where other industry standard and Open protocols (Modbus, KNX, LON, SNMP) are utilised for integration with the Niagara Framework®, then each connecting party shall produce a generic interfacing compliance statement with a full list of all available data objects and supported functionality, including whether they are Read and/or Write, and a detail description of there addressing schemes.
- All Niagara systems shall be configured in accordance to the Niagara 4 Hardening Guide. Niagara Framework® comes with a significant number of configurable Cyber Security capabilities, such as strong authentication, Role-Based Access Control, encrypted communications, encryption at rest, security auditing, and provides the ability for integrators to customize security based on their security policies. It is critical that all integrators use the Niagara Hardening Guide to protect Niagara systems. For more information, please see: https://www.tridium.com/~/media/tridium/library/documents/niagara%204%20hardening%20guide.ashx?la=en
- Role-Based Access Control (RBAC) shall be deployed, making user permissions easy to configure and less error-prone. All user actions and security-related events shall be recorded in Niagara's audit log for traceability.
- Any 3rd Party system to be connecting into the Niagara Framework® onto a Smart Building solution, must have an End of Life (EoL) statement outlining the long term life cycle plan, and ongoing product support plan.

5 GENERAL SYSTEM DESCRIPTION

5.1 MIDDLEWARE REQUIRMENTS

A physical Middleware comprising of Niagara Framework® Platforms shall be deployed providing an interfacing data layer between any 3rd-party systems which shall provide distributed processing as well as normalised data into Niagara Objects, the middleware shall comprise of:

- Platforms which shall be housed within dedicated enclosures or racks as required by the project requirements
- Deployment of Overarching Management Level using Niagara N4 Server with overarching Single Pain of Glass (SPoG) to provide a Graphical User Interface, Multi System Navigation from Landing Page with ability to simply navigate and individual system/plant page graphics using N4 Navigation
- Setup and configuration of stations in accordance with the Niagara Hardening Guide.
- Structured Tagging, Templating, Analytics and "Cause & Effect" functionality as required to provide SPoG design requirements. The middleware shall comprise of:
- Multi System Alarm Management, Handling and Reporting

5.2 MIDDLEWARE INTERFACING

The Middleware and its associated Management Systems shall comprise of a number Niagara Platforms distributed throughout the facility to suit interfacing requirements to:

- Access Control Systems
- Automated Demand Response (ADR)
- Audio Visual (AV)
- Combined Heat & Power (CHP)
- Building Management Systems (BMS / HVAC)
- Closed Circuit Television (CCTV)
- Elevators
- Energy Monitoring & Management Systems (EMS)
- Escalators
- Enterprise
- Facility Management
- Fire Alarm
- Heat Pumps
- Lighting
- Pumps
- Renewable Power Systems (e.g. Solar PV, Wind Turbines, Battery Storage)
- SCADA/PLC (Electrical HV/LV Switching)
- Signage

- Uninterruptable Power Supplies (UPS)
- Variable Speed Drives (Inverters)
- Variable Refrigerant Volume Systems (VRV)

6 SMART BUILDING NIAGARA FRAMEWORK® OVERVIEW

6.1 GENERAL

The Smart Building system shall be based on a design for an Open Systems Architecture (OSA) within a multi-user, multi-tasking environments allowing for simultaneous access by multiple users and distributed network interfacing to provide connectivity to multiple sub-systems via the Internet / cloud.

Data exchange shall be facilitated by utilising the Niagara Framework® as a "Middleware" to interface with Open and proprietary 3rd party systems over the Common Network Infrastructures and to present data into an overarching Management Level System via HTML 5 and Visualisation using Niagara N4

The N4 architecture shall be based on a scalable framework to accommodate any changes in data usage and connectivity within the buildings and their systems to meet with any future requirements, thus future proofing client's investment into Smart Buildings Systems, infrastructures and services.

6.2 ARCHITECTURE

6.2.1 Systems Integration

The Smart Building Middleware system shall be based on the Niagara N4 Framework architecture, designed around open and secure communications standards using HTML5 WEB technology.

The Middleware shall have the capability to communicate via multiple industry open protocols running over Building Network Infrastructures and computer networks, the Niagara Framework® provides support for the following protocols as standard:

- BACnet
- LonWorks
- KNX/EIB
- Modbus
- M-Bus
- oBIX
- OPC
- SNMP
- HTTP (HTML 5 / XML Mark-up Languages)
- Niagara (FOXS)

Once any subsystem are integrated into the Niagara Framework® via JACE Platforms to form a distributed middleware layer, the associated system data point objects shall then be normalised into the Niagara Framework® objects for data manipulation, alarming and visualisation requirements.

The Middleware shall provide the capability to allow Open development of specific solutions or any 3rd Party drivers or Applications (Apps) to meet current or future requirements and to connect to IoT Services, subject to meeting Tridium's Certification Programme (TCP) Niagara Certified Training (N4, Analytics and Development).

Where communications with 3rd Party systems do not conform to any of the Industry Open communication standards and utilise proprietary protocols and networks, they shall be integrated via Niagara Platforms using 3rd party communications drivers if available (Refer to Latest Tridium Driver List), or a 3rd Party drivers developed specifically to meet requirements.

The Middleware Server shall provide access to the 3rd Party systems via HTML5 compatible Browsers over the Network Infrastructures using Niagara N4 Graphics which shall require no special software, e.g. ActiveX components or JAVA Plugins to be installed on to the Client PC's or any other user interfaces (UI's).

Niagara stations shall be configured in accordance with the Niagara Hardening Guide.

Communication between the HTML Web Browser UI's and Middleware Server shall be secured via encryption using 128-bit encryption technology within Secure Socket Layers / Transport Layer Security (TLS/SSL) over HTTPS.

In order to protect the Cyber Security of all connected systems, Niagara Systems shall not be directly exposed on the Internet. If remote access to these systems is required, Niagara systems can be protected by a VPN gateway, providing security protection. Keeping stations behind a properly configured VPN ensures that they are not exposed, reducing the system's attack surface. For more information, see "Using a VPN with Niagara Systems" available from the Niagara Framework Software Security Resource Center on Niagara Community.

As part of the Middleware deployment requirements Niagara N4 Server Software shall be setup to operate on its own dedicated Server environment but shall have the capability to operate under a Virtual server environment if required.

The Niagara framework architecture shall provide Operator(s) complete access to the Middleware system via HTML5 WEB browsers, both operationally and also for engineering requirements via Niagara Software Engineering Tools (Workbench).

The functionality provided through the HTML5 Browser interface shall be not altered, or restricted, based on the location, or type of device used to access the system, the only applicable restrictions shall be those associated with each individual Roll based Access based on their Login credentials.

Niagara Information and Conformance Statement (NICS)

The Niagara Compatibility Statement (NICS) for all Niagara Software shall allow open access and be set as follows: accept.station.in="*" accept.station.out="*" accept.wb.out="*" accept.wb.in="*". In any case, the End User shall maintain the right to instruct the contractor to modify any software license, regardless of supplier, as desired by the End User. The Contractor shall not install any "brand specific" software, applications or utilities on Niagara Framework based devices.

All hardware and field level devices installed, shall not be limited in their ability to communicate with a specific brand of Niagara Framework JACE. They shall also be constructed in a modular fashion to permit the next generation and support components to be installed in replace of or in parallel with existing components.

At the completion of the project the owner shall be given all existing platform and station log in credentials to include; Super User (Admin) user names; passwords and passphrases.

The HTML5 WEB browser User Interface (UI) shall be completely interactive and provide the following functionality as a minimum:

- Single Pain of Glass (SPoG) Visualisation and access to all Systems
- Alarm / Event information
- Real-Time Graphics
- Browser Based Navigation of Systems & Graphics
- Trending (Data Historian)
- Time Scheduling
- Analytics
- Control Logic Definitions (Wire Sheets)
- Parameter/Setpoints and Override Adjustment
- Client Alarm Popup and Annunciation
- Single Tool for Live Software & Graphics Engineering
- Platform / Station Configuration & Maintenance

6.2.2 Software Components

The Niagara Framework® architecture shall provide a Middleware layer which is fully extensible and scalable to meet any future expansion or enhancement requirements. The Middleware shall also facilitate Enhanced Cause and Effect between systems which can be designed, delivered and commissioned via TCP Trained Niagara Specialists.

All components of the Middleware software shall be configured, setup and completed in accordance with the required specifications, software components shall include:

- Server Software including latest Operating System (Windows or Linux RHEL)
- Niagara N4 Core Software and Licenses
- Single WEB based Application & Tools (Workbench)
- Graphical Programming Tool
- Control Logic Software Tool
- Application Software (Alarming, Trending, Time Scheduling, Logging)
- Analytics

6.2.3 Enterprise Connectivity

Subject to licensing and requirements, the Enterprise Management Level shall allow real time Connectivity of data via any of the following accepted methods:

- SQL (Structured Query Language)
- OPC (Object Link Embedding for Process Control)
- oBIX (Open Building Information eXchange)
- SNMP (Simple Network Management Protocol)
- API (Application Programme Interface)

Whilst still employed a common means of transferring data, Simple Text file transfer e.g. Comma Separated Value (CSV) mechanisms are not recommended as part of the Open System Architecture requirements as this are inherently prone to failure and data loss, oBIX (XML) and API based data transferred are the recommended data transfer methods into Niagara.

6.3 FRAMEWORK ARCHITECTURE OVERVIEW

The Framework shall be based on a distributed architecture with real time data access via open industry protocols providing WEB based engineering capability and System monitoring and management of the connected subsystems data at multiple levels over secured networks and infrastructures:

- Cloud
- Enterprise
- Edge

The Tridium JAVA Application Control Engine (JACE) shall be deployed to provide peer-to-peer connection and Edge device connectivity, allowing subsystem devices to continue operating without loss of data in the event of network or Server failure.

A Middleware formed of multiple distributed JACE's shall be deployed to provide a Smart Building System, with the capability to allow any data objects to be connected to facilitate future Enhanced Cause & Effect (EC&E) requirements.

The Network Infrastructure shall be designed to consider speed, latency, performance, traffic flow, network security requirements and data separation via VLAN's for all connected sub-systems.

The Middleware Platform shall be the latest Niagara N4 JACE together with Niagara N4 Server / Supervisor which shall provide a Framework of data Management to reduce the traffic flow to improve speed performance between subsystems between the Middleware Platform and Overarching Management Levels.

Middleware JACE Platforms shall be deployed using TLS and data security between the Network Infrastructure and Connected Subsystems.

The JACE Middleware Platforms shall provide distributed processing of data and reduce the Management Level Server processing and network throughput requirements. Where High Availability and Fault Tolerance is required within critical environments, 3rd Party solutions can be deployed to provide critical backup, e.g. Stratus EverRun.

As the Middleware system scales, the data traffic loads shall be managed at the Middleware Platform Level (JACE), network traffic, data visualisation, alarm management, reporting and data logging shall be managed at the Management level.

6.3.1 Network Infrastructure

To ensure data separation of subsystem services, VLAN's shall be deployed to separate each subsystem service with VLAN Routing to connect systems and data where required into a separate Middleware VLAN to provide an "Open" Data Connectivity layer across connected systems.

6.3.2 Middleware Platforms & Management Level

All Middleware subsystem communications shall be managed via dedicated Niagara N4 JACE platforms to provide distributed processing with reporting to a N4 Management Level Framework Architecture.

JACE Hardware Platforms shall be connected to their respective sub systems via High Level Protocols (Refer to Table 1 for details of Ports, Protocols and Services) over IP or RS232/485 serial connections.

6.4 NIAGARA FRAMEWORK® OPERATIONAL REQUIREMENTS

6.4.1 Operating System & Security

The embedded JACE hardware uses a QNX Operating System at the Platform level together with JAVA at the N4 Supervisory level using the "Foxs" protocol to communicate with Web Services

To ensure Niagara is deployed using the strongest security levels possible at all levels (Edge, Enterprise and Cloud), all communications shall be encrypted using a minimum of TLS V1.2, additionally each JACE Platform Middleware, shall have User Level Access and Authentication

Niagara hardware platforms together with their operating system shall be configured with a common "Strong" password for access, the local user password must meet this minimum requirement.

All messages shall be encrypted, including the usernames and passwords used to access the system either as a browser GUI user, or for Niagara Workbench development engineering use.

6.4.2 Ports and Protocol Control

Access from the Tridium Niagara Platform (Station) over network Infrastructures shall also require following Ports and Protocols to be permitted for each respective service, unused Ports shall be disabled to prevent any unauthorised access:

Services	TCP Port	UDP Port	IP Protocols	Notes
Niagara V4				
Secured Fox Service (Workbench)	3911	—	FoxS	Default port for a Station's Secure Fox Service Used for Workbench To Station and also Station To Station communications
Secured Web Service	443	—	HTTPS	Default port for a Station's Web Service and used for browser access
Secured Platform daemon	5011	—	HTTPS	Default ports for Platform connection for access / administration via the Workbench engineering tool.
Optional Services				
Client Connection to Mail Server for e-mail Notifications	25	—	SMTP	Mail Service
Internet Time Protocol service	37	—	—	
DHCP	—	67, 68	—	Static IP Address's to be assigned to all Middleware Devices
Niagara Drivers *				
SNMP	—	161	SNMP	SNMP protocol
SNMP Trap	—	162	SNMP	
Modbus TCP	502	—	—	
BACnet Ethernet	—	—	—	(Not used)
BACnet/IP	—	47808	—	
OPC Client (Uses DCOM)	135	135		DCOM, using RPC (See below).
KNX				

Services	TCP Port	UDP Port	IP Protocols	Notes
LON				
Others				
RPC, used by NetBIOS (Browsing, File Shares, etc.) and also Windows Update, Browser, OPC client & server	137, 138, 139	137, 138, 139	—	Required for JACE to appear in browser lists and for Network Shares. Required by OPC client driver.
PING	—	—	ICMP	Basic "Ping" Test of connection.
DCOM	135	135	—	See Requirements for OPC Client
Microsoft SQL Server	1433	1433	—	
Network Time Protocol	—	123	—	Sync with Time Server.

Table 1: Niagara Ports and Protocols

*Note: Protocols & Ports required by each particular driver must be unlocked and specified within the configuration of the corresponding Niagara driver as well as within the Network Routers for Cloud access.

NOTE: FOR DETAILED GUIDANCE AND SECURITY CONFIGURATION OF PORTS, PLEASE SEE THE NIAGARA HARDENING GUIDE

6.5 ACCESS AND PERMISSIONS

Niagara Framework® Access and Permissions shall be based on Role-Based Access Control (RBAC) whereby User Groups, Categories and Permissions are defined by User Roles.

Each User Group shall be granted a set of permissions in each category. This combination of categories and permissions shall define exactly what each User Group can do with each object defined within the system, the following sections outline the Niagara "Station" Security requirements:

6.5.1 User Groups

A set of pre-defined Roles based on User Groups" shall be defined across all Stations and every User of the system shall be given a unique "Username" and "Password" Login to provide audit logs.

- "Admin" - Shall always be a Super User, having all permissions in every Category and can thus access everything in a Station that cannot be deleted or renamed.
- "Engineers" - Shall provide Station access from the Web browser with Individual User Accounts and Login Authentication having Read / Write permissions to all Categories and to be able to undertake all Engineering and Graphics configuration including Project Backup and Restore.

- "Operator" - Shall provide Station access from the Web browser and shall have the ability to navigate to following assigned objects:
  i) "Read" Permission (All Objects)
  ii) "Write" permission (Alarms)

- "Guest" - Shall provide Station access from the Web browser with no authentication (User is not prompted to login) and shall have the ability to navigate to any object that has been assigned "Read only" permission.

Groups and Users shall be stored in the Station's local database by default and verified by the Station's "User Service".

6.5.2 Categories

Categories shall be defined for logical grouping of items or components. Categories shall be typically named to reflect each Grouping, as a minimum the following Categories shall be defined for each 3rd Party Subsystem:

Objects requiring further protection with individual security rules shall also be assigned to additional categories as required.

6.5.3 Permissions

Permissions shall be used to define the rights a User has within each of the Categories in the station.

Within each account level, Separate user rights shall be applied to "Read Access" and "Write Access"

Every "User" defined in the Station shall be configured with a "Permissions Map" which shall be used to grants the "User" permissions for each Category defined in the Station

6.5.4 Authentication

There are three authentication points in the Niagara Framework®

- Workbench To Station via the FOXS Protocol
- Station To Station via FOXS Protocol
- Web Browser-to-Station (HTTPs)

Whenever a Station connection attempt is made, the User's login credentials shall be authenticated in accordance with the Niagara Hardening Guide.

6.6 SECURITY & DOMAIN INTERFACING

This section outlines the Security and Domain Services which if required which shall require full co-ordination, design and development prior to being deployed over a Clients Network infrastructure:

6.6.1 Domain Considerations

The following Domain requirements shall be fully ascertained and agreed before any deployment:

- Network Administrator access to Middleware Server / Workstation for the updating of profiles, adding/removing of machines, user account password management.

  No Active Directory security policies shall be "Pushed" down to the Smart Building Server / Workstations without review and agreement as certain policies may conflict with Middleware applications and platform security functions

  If any applicable security policies are required, these shall only be deployed in full consultation with the respective suppliers of the subsystems and undertaking of connectivity/functionality testing to determine any impact on the Middleware system architecture and performance.
- All Testing and implementation of User Account Groups and Profiles together with the Rights of these User Accounts shall be co-ordinated with the Client IT
- A single Domain Logon for Middleware Platforms, Servers and Workstation to facilitate future Enhanced Cause & Effect and middleware data object access.
- Where Email Services are required, these shall be co-ordinated with the Clients IT to provide an Exchange Account if required.

- Time synchronization of Middleware Server, Workstation and JACE platforms to a NTP Server which shall be available across the clients IT Network Infrastructure.

  The NTP server shall be synchronized with other systems to within 1 second to ensure that logging of data and events is accurate. Any Time disparity in time clocks between subsystem server processors shall cause an alarm to be generated.

6.7 SOFTWARE & DATABASE BACKUP

Application software/operating system software shall be backed up onto suitable digital media such as a Network Attached Storage (NAS).

The N4 System Supervisor shall be automatically configured to backup any Historical Trend, Logging, Alarm and System/User Event databases according to user configurable periods to ensure databases are consistently and automatically maintained and Databases regularly compacted to ensure maximum performance at all times.

Back-up of the entire N4 Management Level systems, including configuration and setup data shall be automatically performed on a weekly basis or any time a change is made to the system configuration to ensure that even in the most catastrophic of events the system can be fully restored from the back-up files and, at worst, only one week of data would be lost.

In the case where system changes are carried out, a backup copy shall be taken prior to commencement of any software changes, each version shall be version controlled and date/time stamped, in the event of any failure the system can be reverted to previous backup version.

From Niagara version 4.3, Backup as a Service (Baas) is included with every installation of Niagara.

Niagara BaaS allows any N4 station to be securely backed up to the cloud whereby should any hardware failure or corruption happen, the latest or historical can be traced tracked and downloaded 24/7/365 by authorised individuals from a secure cloud login, and then manually installed on the jace®.

This facility includes the following features:

Initiate backups with 1GB of storage

•Automated/scheduled backups

•View, delete backups

•Add, edit and delete notes

•Notifications

•Geo-located backup service

•Soft backup limits

7 NIAGARA MANAGEMENT LEVEL REQUIREMENTS

7.1 GRAPHICS USER INTERFACE

7.1.1 General

This section outlines the Niagara Middleware HTML5 WEB based Graphics User Interface (GUI) as well as the Single Pain of Glass (SPoG) deployment philosophy which shall be to unify the display of multiple sub systems to present a single operational view of data in a way that's easier to interpret and manage.

Each of the connected subsystems has their own Management Level Operator Workstations and different graphical user interface standards. The Middleware requirements are to bring a common set of Graphics that shall provide Operators with intuitive and instant overview / status information across these systems and where required detailed system graphics.

The WEB based GUI standard shall detail the visual layout and design of graphics, static and dynamic symbols and their representation on graphic pages for the systems covered by these works along with site plan and hierarchy/navigational requirements. The Trade Contractor shall develop a 2/3D dynamic/active graphics library for each subsystem discipline covered by these works along with Landing Page, System Overview Status and Graphical hierarchy/navigation for future expansion.

Active 2/3D colour graphics shall be provided depicting the connected Middleware systems monitored by the Middleware system.

The Graphics shall be designed to be intuitive and operated either from a Workstation which shall be mouse / keyboard driven or via Smart Devices using Touch screens and be intuitive.

All Graphic Pages shall be submitted to the clients engineer for comment as part of each system design requirement, together with all necessary overviews and navigational requirements.

7.1.2 Graphic Browser Navigation

The Graphics Browsing shall be designed to facilitate operation via:

- Middleware Operator Work Station
- Smart / Mobile devices such as Smart phones and/or tablet computers

The Client UI shall provide a comprehensive user interface using a collection of pages to provide a seamless link to all applications and subsystem data.

It shall be possible to navigate through the system using a browser to accomplish the functionality detailed within this specification without the need for any mouse or keyboard. The Graphics Browser Interface shall as a minimum provide:

- A Landing Page with an Overview of Systems and overall Alarm Status Information
- A Navigation area with Navigation tree
- A Common Navigation bar with shall be used on all graphical displays

- Action area for display and operation of graphics
- Access to Applications such as Alarms and Events & Histories, Time Scheduling
- Live Graphic Programming
- Administration Configuration
- Reports and Reporting actions for Alarms and Events.

The "Look and Feel" for the UI pages representing each of the above applications shall be developed in a consistent manner and the WEB Application shall fully utilise the same developed graphics and standards.

7.2 USER INTERFACE (UI)

7.2.1 User Logon

On launching the Logon from the Client Workstation or Tablet device and selecting the appropriate entry via SPoG HTML5 WEB Graphics, the operator shall be presented with a login page based on the User Roles that shall require a unique Login Name and Password.

Navigation within the Middleware system shall be wholly dependent on the operator's role, privileges, and geographic area of responsibility.

The Middleware system shall be capable of complete scalability in terms of User Access and Object privileges. This shall apply to, but not be limited to, individual systems access, functionality and subsystem interaction.

7.2.2 SPoG Landing Page

The Landing Page shall provide access for each connected subsystem together with Alarm Overview / Status. An operator shall be able to select the required System and associated Graphics pages by clicking on buttons / hot spots, corresponding to the highlighted system.

7.2.3 Navigation Task Bar

SPoG shall provide the ability for any user to accomplish the following actions by clicking appropriate Button Icons / menu's in a Graphical Navigation Taskbar which shall be common to all Graphic pages:

- Log In / Out
- Navigation Tree
- Alarm Status Display
- Home Page
- Page Forward/Back
- System Topology
- Application Access (Time Scheduling, Trending, Alarming & Event Logging)
- Print
- Help Menu
- Hide / Show Navigation Pane

7.3 SYSTEM GRAPHICS DEVELOPEMENT

7.3.1 Specific Graphical Requirements

The Middleware UI shall make extensive use of 2D / 3D static and dynamic symbols together with iconic representation of system components in the graphic area to communicate information related to Viewing and Operational elements of each subsystem, the Middleware UI shall provide the following:

- Graphical Display Size: The Trade Contractor shall make allowances to fully develop a Graphical Standard to meet the requirements as detailed. The UI shall as a minimum be optimised to graphically display in HD 1080p, True Colour or higher and shall be compatible with High Resolution Touch screens and WEB UI's without Horizontal or Vertical scroll bars.
- Screen Display: Client Workstations shall have 1080p HD Wide Screens suitable for displaying High Resolution Graphics.
- Bitmaps, JPEG's shall be optimised for 1080p HD Resolution screen display following the UI standards as detailed.N4 support Scalable Vector Graphics (SVG)
- Colour Concept: The Graphic backdrop colour shall be a passive colour that shall be non-invasive and consistent across all subsystem disciplines and shall allow dynamic objects to be displayed clearly, the Plant Graphics shall be designed to be clean and non-cluttered and shall use:
- Dynamically Displayed Values and units of any input / output values shall correspond to the quantity it represents throughout all levels of Graphics.

  Analogue values shall be capable of being displayed to 2 decimal places which shall include inputs, outputs and calculated values.

  Digital values shall be represented by either an Icon representation or a full English word that truly and correctly represents the status and type of point being displayed; this shall include inputs, outputs and calculated values.

The Trade Contractor shall submit a Project Specific HMI Standards Document to the engineer, fully detailing all proposed symbols, icons, page layouts and graphic standards to be deployed on this project.

7.4 APPLICATION REQUIREMENTS

As well as the subsystem specific graphic requirements the following WEB based Applications shall be accessible via SPoG:

7.4.1 Schedules

Niagara N4 shall provide time scheduling capability for all connected systems and commandable Niagara Objects.

Utilising the navigation area displayed in the GUI, an operator with password access levels shall be able to define a Normal, Holiday or Override schedule priorities for each individual piece of equipment or zones, or choose to apply a single schedule to part of the system, site or floor area.

For example, a schedule for one floor in the system would be created by selecting the designated floor and entering the relevant schedule at that location.

No further operator intervention would be required and every control module controlling that floor would be automatically downloaded with the data for that newly entered schedule.

The system shall include the option to have an area opt out of the tiered scheduling criteria to allow specific and separate scheduling of that area with minimal intervention.

All schedules that affect the system, area or piece of equipment highlighted in the navigation area shall be shown in a summary schedule table and graph.

- Schedules shall be compatible with BACnet standards and verified using the 3rd Party PIC's Statement, (Schedule Object, Calendar Object, Weekly Schedule property and Exception Schedule property) and shall allow events to be scheduled based on:
  - i) Types of schedule shall be Normal, Holiday or Override
  - ii) A specific date
  - iii) A range of dates
  - iv) Any combination of Month of Year (1-12, any), Week of Month (1-5, last, any), Day of Week (M-Sun, Any)
  - v) Wildcard (example, allow combinations like second Tuesday of every month).

- The system shall allow operators to define and edit scheduling categories, different types of items to be scheduled; for example, lighting, HVAC occupancy, etc. The categories shall include: name, description, icon representation to display in the hierarchy tree when icon option is selected and type of value to be scheduled.
- In addition to a tiered system of scheduling, operators shall be able to define functional Schedule Groups, comprised of an arbitrary group of areas, rooms or equipment scattered throughout the facility and site. For example, the operator shall be able to define "Individual" plant groups to reflect the usage occupancy of the different areas within each of the buildings Floors / Area's.

  Group Schedules, when applied shall automatically be downloaded to control modules associated with the relevant area's spaces.
- The system shall be designed to automatically turn on any supporting equipment needed to control the environment in an occupied space. Demand shall be created at the point of delivery and that demand shall be passed back through to all plant and equipment necessary to achieve the demand at the point of delivery. For example, if an operator schedules an individual rooms / area's served by Re-heaters for occupancy, the system shall automatically enable the respective AHU, Chiller, Boiler, pumps and/or any other equipment required to achieve and maintain the specified comfort and environmental conditions within the room.
- It shall be possible to setup and apply Site Wide as well as local exception Schedules to accommodate a time range specified by the operator (e.g.: Operating Theatres that need to be operated in an Emergency from 6pm to 12pm overrides Normal schedule), including any Bank or Public Holidays.

- The Schedule summary shall clearly show Normal versus Holiday versus Exception Schedules, and the net operating schedule that results from all contributing schedules. Where more than one schedule is applied, it shall be possible to prioritise.
- The system shall be capable of maintaining Master Schedules for reliability and performance, which shall maintain a single schedule in a JACE that writes over the network to notify other devices when a scheduled event occurs.

7.4.2 Alarm Handling, Notification and Management

The Niagara Alarming System shall provide any required Alarm and Event Management setup and configuration for the data points and devices associated with each connected subsystem.

Alarms and Events shall be configured to generate system messages that provide operators with information such as communications failure and subsystem specific alarms such as breaker status monitoring, elevator status etc.

The Alarm Handling and Management System shall have the capability of providing any of the following possible actions:

- Display of the most recent Highest Priority Alarms for each system category in the Landing Page Alarm Banner
- Initiate a Pop-up Window on any designated Alarm Monitoring Workstations
- Operator Acknowledgement and Reset capability subject to object access and privileges
- Routing to Specified Workstations or Receiving devices
- Routing to Help Desk for further action
- Send to key personnel e-mail account with the relevant alarm information

An alarm matrix shall be produced for each system which shall include:

- System
- Categories
- Priorities
- Messages
- Annunciation
- Network Printing, Email, Mobile Devices)

Alarms associated with a specific system, area, or equipment shall have the following capabilities:

- Each currently active alarm shall be displayed using different icons together with date/time of occurrence, current status and a context link to the associated graphic for the selected system, area or equipment.

  An operator shall be able to sort events on any available data field.
- Systems shall be defined for each subsystem type such as BMS/HVAC, SCADA/PLC, EMS, Lighting, Lifts, EMS or Fire. An icon shall be associated with each category, enabling the operator to easily sort through multiple alarm events displayed using a built-in filter capability.

- Alarm Categories shall be defined for different types of alarms types such as Life Safety, Critical, Maintenance and Abnormal together with their associated properties. As a minimum, properties shall include a reference name, Category, Priority, text description at least 256 characters in length, severity of event, Acknowledgement and Reset requirements, high/low limit out of range and reliability information.
- All Alarm shall be Time/Date Stamped, all events shall be generated at the JACE and shall comprise the Time/Date Stamp using the synchronised time and date.
- Operator Actions shall also be logged for each associated Alarm which shall include any Acknowledgement or Reset notification as well as return to Normal status.
- Alarm Summary Counters for each system shall be displayed across the top of each Graphic page. The view shall provide a numeric counter, indicating how many alarm events are active (In Alarm) and require acknowledgement, and total number of events in the Middleware Alarm Server database.
- Alarm Events that have been Acknowledged, Reset (Where Required) and have returned to Normal shall be auto-deleted from the Alarm Banner view and stored in the Server Log database and archived after an operator-defined period.
- Alarm Reporting Actions specified shall be automatically launched under certain conditions on receiving an event request. Operators shall be able to fully define these Reporting Actions using the Navigation Tree and Graphic Area in the WEB Browser GUI.

  Reporting Actions shall be as follows:

  i) Alarms shall be routed and printed to any networked printer and shall print immediately after the previous Alarm.

  ii) Email shall be sent via any Exchange compatible email server. Email messages may be routed to several email accounts.

  iii) The Simple Network Management Protocol (SNMP) shall be used where reporting Network Events and shall send an SNMP trap to the Network Management system (NMS).

- The SPoG Web Browser Interface shall provide an Event Simulator to test assigned Reporting Actions. Any operator with sufficient object access and privilege shall have the option of using current time or scheduling a specific time to generate the Event.
- Utilising the Navigation Tree and drop-down menus in the Graphic Area, the operator shall be able to select any Alarm / Event Type, Category, Status, Notification, Priority, Message, and whether Acknowledgement and Reset is required.

7.4.3 Histories

The system shall be able to Trend and Display graphically via SPoG any analogue, digital or calculated point. A Trend log's properties shall be editable using the Navigation Tree and shall provide the following:

- The operator shall have the ability to view trends by using the Navigation Tree and selecting a Trend button in the Graphic Area. The system shall allow y-axis and x-axis maximum ranges to be specified and shall be able to simultaneously graphically display multiple trends per graph.
- Trend data shall be collected from any connected subsystem and periodically uploaded based on automatic configuration to the N4 Server; Trend data shall be retained in non-volatile module memory and archived after an operator-defined period.
- Sample intervals shall be as small as one second. Each trended point shall have the ability to be trended at a different trend interval. When multiple points are selected for display, which have different trend intervals, the system shall automatically scale the axis.
- Trends shall be able to dynamically update at operator-defined intervals.
- It shall be possible to zoom-in on a particular section of a trend for more detailed examination; the system shall be able to Zoom Out or Reset the Trend view to the standard range.
- It shall be possible to pick any sample on a trend and have the numerical value displayed without moving to a different screen.

The system shall extract information directly from any relevant data within the Middleware JACE's to initiate trend logging facilities, retrieving real time values of any I/O or from process control loops and then display/print the logged data for tuning/diagnostic purposes. The measured value shall be the actual reading at the sensing device.

The capacity of each JACE shall allow all for all points to be logged in the system at 1 minute intervals for a minimum of 24 hours within the same controller that they are connected to. In addition, each controller shall be able to log all calculated points and shall have the capacity to log 75% of these points at 5 minute intervals within the same controller that they are held.

The data collected from a point shall be stored in non-volatile memory. The time periods of data logging shall be variable between a minimum of 1 minute to a maximum of once per day. This shall be selectable at the time of initiation of the logging period.

The Operator shall have the option to specify the start and/or stop time of the trend log period. The logs shall also be capable of being held, overwritten on a first-in first-out basis.

The value stored periodically shall be the average reading since the previous reading. Spot readings at the time of the sample shall not be acceptable. The Operator shall have the option to read the maximum and minimum logged values.

All Trend log data shall be initially stored in memory buffers of the JACE's which shall also support short term (1 Day) logging requirements.

The Middleware JACE's shall archive Trend values to the Middleware Server prior to them being over-written in the JACE. The Middleware Server hardware shall be sized such that one year's worth of archived data may be held for retrieval on an "Instantaneous" basis.

The Middleware system shall have the facility to automatically archive trend data older than one year to the Network Attached Storage (NAS) with the capability of being retrieved for viewing at any time in the future.

System operating Logs shall be configured to log all events during commissioning and samples shall be included within the Trade Contractors system commissioning report. These system operating logs shall contribute towards providing evidence of the satisfactory completion of commissioning.

7.4.4 Reporting

The N4 Middleware Management system shall have the facility to configure to generate the following daily/monthly management and system reports on an ad-hoc and on-line basis:

i) Alarm Console

ii) Energy Usage

iii) Monthly Service Call

iv) Response Time Monitoring

- The Reporting function will allow for the creation of configurable (user-defined) reports via a report builder tool. The Reporting function will provide functionality to ensure that certain types of user-defined reports are made available only to specific user roles.
- The Reporting function will allow for specification of filter conditions to refine the data being displayed in standard and user-defined reports.
- The Reporting function will allow for dynamic analysis on both standard and user-defined reports by providing the following features:
  - i) Changing of row and column orders for different presentation layouts.
  - ii) Grouping/aggregation to view data at a summary as well as detailed level within the same report
  - iii) Slice-and-dice capabilities for advanced analysis
- The Reporting function will allow for exporting of data into Microsoft Excel, comma-separated text (CSV), PDF or other suitable formats.
- The Reporting function will be compatible with standard reporting engines so that new reporting templates can be developed.
- The Reporting function will have facility for the users to select whether to generate a report on-line or in batch mode.

- The Reporting function will allow preview of all reports on screen before it is sent for printing on desktop printers or network printers.
- The Reporting function will allow the user to generate reports in a graphical format, for example, bar chart, pie chart, etc.

7.5 ENTERPRISE SERVER & WEB BROWSER GUI

7.5.1 System Overview

Rack mounted Enterprise Servers shall be deployed in the Clients IT Rack Space and shall be configured to Run the Middleware Application as a "Service" and be capable of multiple client logins.

To allow the users to view the monitored middleware system data, dedicated Client Workstations shall be provided in all required locations.

Additionally, the Middleware Server shall be configured to provide WEB Services to any WEB Client Device such as Tablets or any Client Desktop dependant on network Security and User Access and Privileges.

The Server Manufacture type and model shall be approved by the Clients IT who shall also ensure that the environments comply with their own corporate Security and Management requirements.

Servers shall be of sufficient specification to meet this specification plus 50% expansion in the future with Remote Desktop Access for Administrators.

The Niagara N4 Server shall be supplied to allow a minimum of ten concurrent Client users without any performance degradation.

As detailed above, Servers, NAS and Workstations connected to the Network Infrastructure, shall subject to User Login and any Security Privileges and User Base Roles.

7.5.2 Niagara Middleware Server & Network Storage

Example - The Middleware and Network Storage Servers shall be of minimum specification:

- Intel Xeon E5640 Processor 2.66GHz
- 4GB Memory CPU
- Integrated Level 10 RAID controller with 5 2.5" Disks Hot Plug (1 Hot Standby)
- 16X DVD-ROM Drive SATA
- GB Network Card
- Windows Server 2012 Enterprise SP2 64 bit
- Microsoft SQL2014
- KVM Console with 17" LCD Display Keyboard & Touchpad Mouse

The Network Attached Storage Server NAS shall have RAID Level 5 with 4 2.5" Disks Hot Plug (1 Hot Standby)