Vertiv™ Liebert® Nform Software
Critical Infrastructure Management System
GUIDE SPECIFICATIONS

1.0 GENERAL

1.1 Overview

The Critical Infrastructure Management software centrally monitors and manages distributed equipment using the customer's existing network infrastructure. The system provides the Critical Infrastructure Management and Monitoring for Air Conditioning (CRAC) systems, Uninterruptible Power Supply (UPS) systems, Power Distributions Units (PDU), Static Transfer Switches (STS), Direct Current Power Systems (DC), Power Distribution Strips (PDU), Vertiv™ Liebert® Alber™ Battery Monitoring, Rack Enclosure Intrusion Monitoring, Leak Detection Systems and other critical infrastructure systems as specified. The system has an architecture that allows up to 10,000 managed devices, including Liebert and third-party devices, in a single-server installation.

1.2 System Requirements

1. All material and equipment used shall be standard components, regularly manufactured and available and not custom-designed especially for this project. All systems and components shall have previously been thoroughly tested and proven in actual use prior to installation on this project.
2. The manufacturer will furnish or supply a site-specific Critical Infrastructure Management software system based on customer requirements. The system must be a software-only solution; no substitutions will be accepted.
3. The system architecture may consist of network interface cards that will be installed in all critical infrastructures that at a minimum support HTTP and SNMP simultaneously.
4. The system shall receive SNMP traps from managed equipment and display the alarm notification in a graphical user interface.
5. The system shall be based on SNMP Open Protocols and integrate seamlessly with Emerson Network Power, Vertiv™ Liebert® Aperture™ software suite and Network Management Systems.
6. Open protocol support shall include:
    - HTTP(s)
    - TCP/IP/v4, TCP/IP/v6
    - SNMP v.1, SNMP v.2

7. The system will have the capability of being remotely monitored and managed 24 hours a day, 7 days a week by the manufacturer.
8. The system shall have the ability to be deployed world-wide.
9. The system will operate as a client-to-server application.
10. The Web interface of each managed device shall integrate directly into the system.
11. The system will support Enterprise level databases including Microsoft SQL.
12. The system shall support exporting of all recorded parametric trend data.
13. The system will operate on a server defined by the customer. Specific server brand or function is not permissible.
14. The system will support virtual server environments by default.
15. The system will include at no additional cost one (1) year of Software Assurance.

1.3 Approved Products

The Critical Infrastructure Monitoring System shall be Vertiv™ Liebert® Nform as manufactured by Emerson Network Power, Liebert Corporation. No substitutions will be accepted.

1.4 Scope of Work

1.4.1 Owner-Supplied Items

The owner will furnish the following system components:

1. Network (LAN) hardware and software required to provide an Ethernet backbone to be used for transport of IP data packets from network interface cards installed in all equipment to the Critical Infrastructure server and to the Liebert® Nform workstations. These components may include hubs, routers, cabling, network operating systems, firewalls, IP addresses, Virtual Private Network (VPN) and other components as required. The owner will supply network drops for the Critical Infrastructure server, workstation clients and all network-interfaced equipment.
2. **Dedicated Critical Infrastructure Server meeting the following minimum requirements:**
    - Microsoft Windows 7, Windows 8/8.1 Enterprise, Windows Server 2003, Windows Server 2008 (R2) or Windows Server 2012 (R2) operating system
    - Pentium 3.0GHz single processor or better (1.8 GHz dual processor or better recommended)
    - 4 GB of RAM (memory) or better
    - 40 GB hard drive (SCSI recommended) or better
    - 10/100 BaseT network port or better
    - Monitor / keyboard and mouse port as required for setup
    - Standard USB ports
    - CD or DVD-ROM drive for software installation (CD/DVD-RW suggested for installation and backup)
3. Critical Infrastructure server may be Virtual Environment compatible

4. **Critical Infrastructure Workstation PCs (clients) meeting the following minimum requirements:**
    - System should meet the minimum requirements for Microsoft Windows 7, XP, 2003, Windows Vista, Windows 8/8.1 Enterprise, Windows Server 2008 (R2) or Windows Server 2012 (R2) operating system Microsoft Internet Explorer v9.0 or better
    - 2 GB RAM (or the minimum operating system requirement)
    - 20 GB hard disk (or the minimum operating system requirement)
5. **The owner will supply the following information to facilitate system implementation:**
    - IP addresses and subnet masks and other information as required to configure network devices
    - Provide a person as the nominated system owner for administrator purposes
    - Secure location for hardware and server

1.4.2 Critical Infrastructure System Vendor Responsibilities

Provide hardware and software as listed.

- Critical Infrastructure software and licenses for server and workstation (client) installations.
- Provide Software Assurance for the first year at no additional cost.
- Provide 24 x 7 system application and service support via a toll-free number.
- Provide warranty (parts and labor) per the manufacturer's warranty statement.
- Vendor shall be ISO9001 listed for design and manufacture of environmental control systems for Critical Monitoring and Control applications.

1.5 Submittals, Documentation and Acceptance

1.5.1 Submittals

1.5.2 Owner's Instructions

The Contractor shall provide full instructions to designated personnel in the operation, maintenance and programming of the system.

1.6 General Conditions

1.6.1 Warranty

The Contractor shall warrant that all systems, subsystems, component parts and software are fully free from defective design, materials and workmanship for a period of one (1) year from the date of software license registration or 15 months from shipment from the manufacturer's location, whichever comes first.

2.0 EQUIPMENT

2.1 System Overview

The Critical Infrastructure Contractor shall provide system software based on a server-to-client architecture. The system shall communicate using SNMP UDP/IP protocol. The server shall be accessed using a secured client over the owner's intranet.

At a minimum the system shall provide:

- Unlimited simultaneous users
- Built-in alarming, trending and notification capabilities
- Support simultaneous international languages
- Support third-party integration

2.2 Server-To-Client Architecture

The intent of the server-to-client architecture is to provide operators complete access to the Critical Infrastructure server system via a secured workstation. The workstation Graphical User Interface (GUI) must be an installable application.

2.3 SNMP Support

The Critical Infrastructure software server will utilize the SNMP Services installed with the base operating system. No proprietary SNMP service will be accepted or allowed on the server.

2.4 Operating System Support

The Server software must support Internet Explorer 9 or greater, Microsoft Windows 7, Windows 8, and Windows Server 2008, Windows Server 2012 R2 platforms. (See Section 1.4.2 for minimum requirements.)

2.5 Client Viewer Graphical User Interface

1. **Detachable Windows:** The Client GUI will provide the ability to detach the Dashboard, Alarm Management and Navigation windows to be displayed on multiple monitors, which will enable the user to take advantage of Network Operation Centers with multiple desktop monitors and/or LCD displays.
2. **Dashboard:** The Client GUI will provide a dashboard interface, which will enable the user to define gadgets that provide a quick summary of the status of the system, device types or specific devices managed by the system. The dashboard will have the following capabilities:
    - **Equipment Status:** The dashboard will enable the user to centrally view the distributed status of all critical infrastructure providing a summary of devices in an alarm state, not responding or returned to normal.
    - **Alarm Gadget:** The Alarm gadget will allow the user to display a 2D/3D pie chart that dynamically shows the total number of alarms in various states: unacknowledged, user-acknowledged or system-acknowledged. The gadget can be configured to filter this data by device category, device type and/or manufacturer.
    - **Communication Gadget:** The Communication gadget will allow the user to display a 2D/3D pie chart that dynamically shows the total number of devices in various states of communication: normal, alarms present or not responding. The gadget can be configured to filter this data by device category, device type and/or manufacturer.

3. **Navigation:** The Client GUI will provide a navigational interface, which will enable the user to logically define the layout of the critical equipment by area, floor plan and/or rack location. This Navigation interface will allow the user to connect to equipment directly and view status, summary reports and alarm event conditions. The Navigation view will have the following capabilities:

    - **Web View:** The Web view will allow the user to connect directly to the equipment. The Web interface with the equipment will be integrated directly into the Client GUI. Viewing the Web page of the device in an external browser will not be acceptable.
    - **Parametrics:** The Parametrics view will allow the user to query the telemetry data available for the device. The Parametrics view will allow users with device-editing permission the ability to change setpoints and configuration values of the equipment.
    - **Alarms:** The Alarms view will allow the user to filter alarm history data to display only the alarms for a selected device or devices in a selected area group. All capabilities of the Alarm view will be allowed at this level.
    - **Trends:** The Trends view will allow the user to set up trendable data points in a graph. The Trends view will be capable of displaying a minimum of eight (8) data points in a single line graph.
    - **Info Links:** The Info Links view will allow the user to access online documentation for the selected equipment. Online documentation will include user manuals, installation guides and operator manuals. The user will be able to configure additional links to online documentation.
    - **Device Status Propagation:** The user will be able to customize the navigation tree, creating a hierarchy of areas and groups that contain other areas or devices and will propagate device status up through the tree and the area groups. This allows the user to view the location of areas and devices that have alarm conditions that need to be resolved.
    - **Rack PDU Receptacle Grouping:** The user will be able to customize a navigation tree that contains customized groupings of Rack PDU receptacles. These groups will summarize the parametric data of all the group receptacles. The user will be able to execute command and control signals on these groupings. Only Liebert Rack PDUs will be accepted.

4. **Alarms:** Alarms associated with a specific system, area or equipment selected in the Navigation Tree, will be displayed in the Action Pane by selecting an Alarm view. Event alarms will have the following capabilities:

    - **Alarm View:** Each alarm will be displayed with level of severity (using a different icon for each severity level), date/time of occurrence, current status and a source URL link to the associated graphic for the selected system, area or equipment. The URL link will indicate the system location, address and other pertinent information. An operator will easily be able to sort alarms, edit alarms and severity, acknowledge or add a comment to the alarms in the Alarm View as specified in this section.
    - **Severity:** The operator will be able to edit or assign alarm severities such as Critical, Warning or Informational. An icon will be associated with each severity, enabling the operator to easily sort through multiple alarms displayed.
    - The user will have the ability to view events throughout the system.
    - Dependent on access level, the user will be able to manage events through acknowledgements, deletions, sorting rules and viewing short and extended messages.
    - **Auto-Acknowledge:** The system will be capable of automatically acknowledging new alarms as they are received with a specific severity level.

- **Alarm Storage:** The user will be able to configure the system to automatically manage the alarm database by maximum storage days or maximum database size. The system will automatically archive older alarm records out of the database.

2.6 Remote Notifications

The system will be capable of sending notifications to users with information about alarms and selected details such as date/time of occurrence, affected equipment, type of alarm and level of severity. All notifications and their configurations must be stored and executed from a centralized server. Decentralizing and management of notifications will not be accepted

The following remote notifications will be supported:

- **E-Mail:** The system will be capable of sending e-mail notifications to users. These e-mails can be configured to contain the details of the alarm event, links to online documentation and a URL link to the equipment with the alarm condition.
- **SMS:** The system will be capable of sending SMS notifications to users' mobile devices. These messages can be configured to contain the details of the alarm condition.
- **SNMP Trap Forwarding:** The system will be capable of sending specific SNMP traps to a Network Management System (NMS). These SNMP traps can be filtered to each NMS allowing the system to receive notifications of the most critical alarm events. Systems that support only all-or-nothing SNMP trap forwarding will not be acceptable.

2.7 Automated Actions

The system will be capable of performing automated actions as configured by the user. These actions can be triggered by new alarms that are received by the system. The following actions will be supported:

- **Run Command:** The system will be capable of running external executable programs or scripts. This allows the user to customize the system to perform tasks that are not supported by the system, such as file batch process or integration to other IT-based systems.
- **Write File:** The system will be capable of writing to a file when an alarm is received. These files may contain specific alarms or a set of work directions that can be used by an operator to manage the system.
- **Read Data:** The system will be capable of recording parametric data from equipment at a minimum interval of 10 seconds for a maximum duration of 99 minutes. This parametric data can be viewed in a graph from the specific alarm event. This action can be triggered by multiple alarms in the system.
- **Write Data:** The system will be capable of sending control commands or setpoint changes to equipment being managed. This action can be set up to be performed automatically when a new alarm is received by the system.

2.8 Automated Shutdown

The system will be capable of sending automated shutdown commands to Vertiv™ Liebert® MultiLink 1.5 shutdown clients. These shutdown commands can be triggered on any and all alarm events that can be received by the system. This includes power and cooling alarm events.

2.9 Security

The Client GUI will provide authenticated user access, presenting a user with a login screen from which the user must authenticate before gaining access to any product functionality. The security settings will have the following capabilities:

1. **Authenticated Access:** The Client GUI shall support authenticated access for a default of three (3) user groups (more user groups can be added):
   - Administrator
   - Power User
   - User
2. **User Properties:** The user settings will allow the assignment of a customized navigation tree to be used by a specific operator to navigate the system. This navigation view can be limited to manage specific equipment or areas per their assignment.
3. **User Notifications:** The user settings will allow the assignment of the following methods of receiving local notifications: Bring Application to Foreground, Flash Taskbar Button and Display System Tray Popup Message. Each method may also be specified to activate only for alarms with a minimum alarm severity level.
4. **Local Audible Alert:** The user settings will allow the assignment of local audible alerts that can be played when an alarm event is received by the system. Each severity can be assigned a specific audible alert.
5. **Account Disabled:** The user settings will provide the administrator the ability to disable any valid user account without deleting it. This will prevent a user from accessing the system.
6. **Audit Log:** The system will record operator activities and some system activities (such as opening and closing the database or automatic deletions) in a text file to allow the administrator to monitor changes that are submitted to the Vertiv™ Liebert® Nform server.

2.10 Trends

Trends will be both displayed and user-configurable through the Client Viewer GUI. Trends will comprise analog, digital and setpoints simultaneously. A trend log's properties will be editable using the Navigation Tree and Graphic Pane.

- **Viewing Trends:** The operator will have the ability to view trends by using the Navigation Tree and selecting a Trends button in the Graphic Pane. The system will allow y- and x-axis maximum ranges to be specified and will be able to simultaneously graphically display multiple trends per graph.
- **Resolution:** Sample intervals will be as small as one minute. Each trended point will have the ability to be trended at a different trend interval. When multiple points are selected for display and have different trend intervals, the system will automatically scale the axis.
- **Dynamic Update:** Trends will be able to dynamically update at operator-defined intervals.
- **Zoom/Pan:** Users will be able to zoom in on a particular section of a trend for more detailed examination and pan through historical data by simply scrolling the mouse.
- **Numeric Value Display:** Users will be able to pick any sample on a trend graph and have the numerical value displayed.
- Users will be able to copy a data graph to a clipboard to interface with their spreadsheet software products.

2.11 Language Support

The Critical Infrastructure system will support international languages simultaneously. Language support will include:

- English
- Spanish
- French
- German
- Italian
- Japanese
- Simplified Chinese

2.12 Software Integration

The Critical Infrastructure system will integrate seamlessly with Vertiv™ Liebert® Aperture™ brand software. No additional hardware will be necessary for integration.

2.13 Data Exporting

The system will support the ability to export data that can be used for integration into other systems and/or for the purpose of creating custom reports.

At a minimum, the owner will be able to retrieve the following:

- Alarm Event History
- Trend Data
- Notification and Action History

2.14 Database Support

The system will support the following databases as a minimum:

- Embedded Database
- Microsoft SQL
  - SQL Server 2008
  - SQL Server 2008 R2
  - SQL Server 2012
  - SQL Server Compact Edition v3.5 SP2

2.15 Enterprise Db Integration

The system will have the ability to locate the operating database(s) on the owner's Enterprise class database server.

2.16 Software Components

All software components of the system software shall be installed and completed in accordance with the specification. System components will include:

- Server Software, Database and NT-based service
- System Configuration Utilities for importing of additional devices, which include third-party equipment
- Client Application Viewer

2.17 Software Assurance

The Critical Infrastructure System Software will include one (1) year free subscription to the Vertiv™ Liebert® Nform Software Assurance Online Portal.

Software Assurance includes the following:

- Technical resources
- Software support site access
- Around-the-clock phone support
- Latest software updates
- Tools for device deployment
- Third-party device support

3.0 EXECUTION

3.1 General

Contractor, unless specified in other sections of these specifications, will install all equipment and devices furnished under this section of these specifications. Contractor will install all other equipment, appurtenances, devices and auxiliaries thereto that are required to make the system complete and operative.

Terminate all power and control wiring required to complete the installation.

- Installation of all wiring and conduit is accomplished under Division 16. The term “wiring” includes wire, conduit, miscellaneous materials and labor as required to install all wiring for a total working system.
- Install trunk signal cables as continuous runs from the control center to remote panels and from remote panel to remote panel, without splices or intermediate junction boxes. Terminate all conductors at terminal strips.
- Install software in control units and operator workstation. Implement all features of programs to specified requirements and appropriate to sequence of operation.
- Connect and configure equipment and software to achieve the sequence of operation specified.

3.2 Professional Services - Software Integration Services Startup (Sis Startup)

If a factory SIS Startup is purchased/requested, a factory-trained Infrastructure Management Technician will perform the following installation, activation, configuration, verification and on-site training:

1. Installation

- Full server and client installation of Critical Infrastructure Management Software on customer-designated servers and workstations.
- Verification of installation per manufacturer’s instructions.

2. Activation

- Set up access to the online software assurance portal with full activation and registration.
- Set up Administrator account.
- Register all license keys.

3. Configuration

- Install license keys.
- Discover and configure managed devices.
- Set up notifications and actions.

4. Verification

- Test communication with managed devices.
- Generate test alarms from managed devices.
- Test notifications to active e-mail accounts and mobile devices.

5. On-Site Training

Comprehensive training on the Critical Infrastructure Management system that includes the following:

- User account administration
- Device operation and management
- Event management
- Real-time monitoring and trend analysis
- Troubleshooting and diagnostics