Liebert® SiteScan® Web

Critical Facilities Monitoring System

GUIDE SPECIFICATIONS

1.0 GENERAL

1.1 OVERVIEW

This document contains the specification and input/output point summaries for a Critical Facilities Monitoring System (CFMS). The system shall provide the Critical Facilities Monitoring for Computer Room Air Conditioning (CRAC) systems, Uninterruptible Power Supply (UPS) systems, Power Distributions Units (PDU), Static Transfer Switches (STS), Direct Current Power Systems (DC), Branch Circuit Monitors Systems (BCMS), Power Distribution Strips (PDU), Standby Generators, Alber™ Battery Monitoring, Rack Enclosure Monitoring, Leak Detection Systems and other critical infrastructure systems as specified.

1.2 SYSTEM REQUIREMENTS

A. 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, except site-specific software, shall have previously been thoroughly tested and proven in actual use prior to installation on this project.

B. The manufacturer will furnish or supply a site-specific CFMS system based on customer requirements.

C. The CFMS architecture shall be fully modular permitting expansion of application software, system peripherals and field hardware.

D. The CFMS shall utilize a distributed processing architecture so that polling of all points is not dependent on a single processor.

E. The CFMS shall be based on Open Protocols and seamlessly integrate with Emerson Network Power, Aperture® software suite and Building / Network Management Systems.

F. Open protocol support shall include:
- Java
- HTTP(s)
- XML/SOAP
- BACnet PTP / MSTP / IP
- Modbus ASCII / RTU/ via Serial or Network interfaces IP slave only
- SNMP v.1

G. An employee of the manufacturer shall initialize, commission and warrant the CFMS.

H. The CFMS will have the capability of being remotely monitored and managed 24 hours a day, 7 days a week by the manufacturer.

I. The CFMS shall have the ability to be deployed world-wide.

J. The CFMS shall operate as a true Web-based system. Bolt-on Web applications are not permissible.

K. The Web interface shall support all standard Web browsers.

L. The Web interface shall also support Web-enabled devices (WAP) by default; no special programming should be necessary.

M. The CFMS shall support Enterprise Level databases including SQL.

N. The CFMS shall support XML/SOAP Web services to allow data to be remotely accessed.

O. The CFMS shall operate on a server defined by the customer. Specific server brand or function is not permissible.

P. The CFMS shall support virtual server environments, by default.

1.3 APPROVED PRODUCTS

The Critical Facilities Monitoring System (CFMS) shall be Liebert SiteScan Web, 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:

A. Network (LAN) hardware and software required to provide an Ethernet backbone to be used for transport of IP data packets from gateway modules to the CFMS Web Server, and from the CFMS Web Server to the Liebert SiteScan Web 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 CFMS Web Server, CFMS Web workstations, and control modules.

B. Dedicated CFMS Server meeting the following minimum requirements:
- Microsoft® Windows® 2000, 2003, XP or XP Server, Windows Vista®, Windows Server® 2008 or Windows 7 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)
- 10/100 BaseT network port or better
- Monitor, keyboard and mouse port as required for setup
- CD or DVD-ROM drive for software installation (CD/DVD-RW suggested for installation and backup)

C. CFMS Server may be Virtual Environment compatible.

D. CFMS Workstation PCs meeting the following minimum requirements:
- System should meet the minimum requirements for Microsoft Windows 2000, 2003, XP or XP Server, Windows Vista, Windows Server 2008 or Windows 7 operating systems.
- Microsoft Internet Explorer® v6.0 or better
- 1GB RAM
- 10GB hard disk

E. 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
- Drawing and schematics as needed to create the customized graphics pages and configuration
- Provide a person as the nominated system owner for administrator purposes
- Assistance in defining point descriptions, alarm messages and content for customized graphic pages and configuration
- Secure location for hardware and server

1.4.2 Contractor's Responsibilities

In the overall scope of the project, the contractor shall provide one or more of the following CFMS components:

A. Software
- CFMS Server software and license
- Customized graphic pages and software configuration

B. Control Modules
- Liebert SiteLink™-12E, Liebert SiteLink-4E or Liebert SiteLink-2E Interface Modules for Liebert Precision Cooling, Power and UPS units
- Liebert SiteI/O-E™ Universal Input/Output Modules for space, power and cooling sensor monitoring, etc.
- Liebert SiteTPI-E™ Modbus or BACnet Third-Party Interface
- Liebert SiteIP-E™ SNMP to BACnet Interface
- 120-230VAC / 24 VAC transformers for Control Modules listed in this section

C. Control Module Mounting: Mount all control module panels (i.e., Liebert SiteLink, Liebert SiteI/O, Liebert SiteTPI and Liebert SiteIP, etc.) and furnish miscellaneous mounting hardware.
- Provide power wiring and receptacles to power all control panels from UPS circuits. 120-230/24 VAC plug-in transformers will be furnished with the control panels.
  All to be fed by UPS back power supplies.
- Provide 24 VAC wiring from screw terminal on the transformer to screw terminal in each control panel.
- Provide twisted-pair communications wiring and terminate as shown on the drawings.
  Recommended wire is: MAGNUM Cable P/N A3-ARC-156-2
- Provide wiring for all field-mounted sensors and transducers as required and make wiring terminations.
  See cable specifications; wiring must meet plenum and low smoke and zero halogen standards based on local codes.
- Label all wiring runs at both ends and provide as-built termination list to the CFMS vendor facilitate software configuration.
- Provide warranty on contractor-furnished items as specified under General Conditions (see Section 1.6.1).

D. Conduit and Wiring: Conduit and wiring is provided under Division 16. The Contractor is responsible for termination of all wiring used for sequence of operation and alarms.
- **Codes and Regulations** - All electrical equipment and material and its installation shall conform to the current requirements of the following authorities:
  - Occupational Safety and Health Act (OSHA)
  - Underwriters Laboratories (UL)
  - National Electric Code (NEC)
  - National Fire Code
  - IEC 60364 Electrical Installations for Buildings
- **Controllers** - All distributed, stand-alone and unitary controllers supplied shall be in compliance with the following listings and standards:
  - UL916 for Open Energy Management
  - FCC Part 15, Sub-Part B, Class A
  - CE Electro Magnetic Compatibility

E. As-Built Drawings: Provide as-built drawings of system configuration per actual installation.

1.4.3 CFMS Vendor Responsibilities

Provide hardware and software as listed.

- Create site-specific software configuration and graphic screens based on information provided by the owner or customer.
- Provide system startup, commissioning and operator orientation by factory-employed System Specialist.
- Provide 7 x 24 system application and service support through a toll-free number.
- Provide warranty (parts and labor) per the manufacturer's warranty statement.
- The CFMS 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

Shop Drawings: A minimum of six (6) copies of shop drawings shall be submitted and shall consist of a complete list of equipment and materials, including manufacturer's descriptive and technical literature, catalog cuts and installation instructions.

Shop drawings shall be approved before any equipment is installed. Therefore, shop drawings must be submitted in time for complete review so that all installations can be completed per the project's completion schedule.

1.5.2 Owner's Instructions

The Contractor shall provide full instructions to designated personnel in the operation, maintenance and programming of the system. The training shall be specifically oriented to the system and interfacing equipment installed.

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 commissioning or 18 months from shipment from the manufacturer's location, whichever comes first.

2.0 EQUIPMENT

2.1 SYSTEM OVERVIEW

The CFMS contractor shall provide system software based on a true Web-based architecture, designed around the open standards of Web technology. The CFMS Server shall communicate using ASHRAE's BACnet/IP protocol. The CFMS Server shall be accessed using a Web browser over the owner's intranet.

At a minimum the CFMS shall provide:

- Unlimited simultaneous users
- Multiple operating systems and databases
- Built-in alarming, trending and report writing capabilities
- Support simultaneous international languages
- Support third-party integration
- WAP-enabled devices without special programming
- Secure server access using TLS/SSL
- Enterprise integration via Web services (XML / SOAP)
- Advance security policy to meet 21 CFR 11

2.2 INTENT OF WEB ARCHITECTURE

The intent of the Web architecture is to provide the operator(s) complete access to the CFMS via a Web browser. The workstation Graphical User Interface (GUI) shall support Microsoft Internet Explorer version 6.0 or greater as well as non-Windows operating systems.

2.3 OPERATING SYSTEM SUPPORT

The CFMS Server software must support Microsoft Windows 2000, 2003, XP or XP Server, Windows Vista, Windows Server 2008 or Windows 7 platforms. (See Section 1.4.1, item B for minimum requirements.)

2.4 WEB BROWSER GRAPHICAL USER INTERFACE

A. **Web Browser Navigation:** The Client Web browser GUI shall provide a comprehensive user interface. Using a collection of Web pages, it shall be constructed to function like a single application and provide a complete and intuitive mouse- or menu-driven operator interface. It shall be possible to navigate through the system using a Web browser. The Web browser GUI shall (as a minimum) provide a Navigation pane for navigation, and a Action pane for display of graphics, schedules, alarms/events, live graphic programs, active graphic setpoint controls, configuration menus for operator access, reports and reporting actions for events.

B. **Color Graphics:** The Web browser GUI shall make extensive use of color in the graphic pane to communicate information about the equipment being monitored.

C. **Display Size:** The GUI workstation software shall graphically display in 1024 by 768 pixels and 24 bit True Color.

D. **General Graphic:** General area maps shall show locations of controlled buildings in relation to local landmarks.

E. **Mechanical and Electrical Components:** Mechanical and electrical system graphics shall show the type of mechanical and electrical system components serving any zone through the use of a pictorial representation of components. Selected I/O points being controlled or monitored for each piece of equipment shall be displayed with the appropriate engineering units.

F. **Minimum System Color Graphics:** Color graphics shall be selected and displayed via a Web browser.

G. Each piece of equipment monitored or controlled including each terminal unit
- Each building
- Each floor showing equipment monitored

H. Events and Alarms: Events and alarms associated with a specific system, area or equipment selected in the Navigation Tree shall be displayed in the Action pane when an operator selects the Events view. Events, alarms and reporting actions shall have the following capabilities:
- **Events View:** Each event shall display an Event category (using a different icon for each event category), date/time of occurrence, current status, event report and a bold URL link to the associated graphic for the selected system, area or equipment. The URL link shall indicate the system location, address and other pertinent information. An operator shall easily be able to sort events, edit event templates and categories, acknowledge or force a return to normal in the Events view as specified in this section.
- **Event Categories:** The operator shall be able to create, edit or delete event categories such as Electrical, Mechanical, Fire Protection and Generator. An icon shall be associated with each Event category, enabling the operator to easily sort through multiple events displayed.

I. The CFMS shall support international languages simultaneously. Language support shall include:
- English
- Spanish
- French
- Swedish
- Russian
- Korean
- Simplified Chinese
- Traditional Chinese
- Vietnamese

J. System Navigation
- **Navigational Tree:** At a minimum, the user must be able to navigate the system through a navigational tree.
- The system must provide the capability of using links and hot spots to navigate through the viewing pane.
- Setpoint or parameter change of properties
- The user must have the ability to change parameters properties.
- The system will have the ability to define parameter access for users.

K. The CFMS shall have the ability to make configuration changes with interrupting system operation. Through a right-mouse click the user shall be able to:
- Reload a program
- Reset a property value
- Perform a global copy
- Select a different unit icon
- Rename equipment
- Change the navigational tree

L. The CFMS Web browser GUI shall have the ability to auto-scale or resize to best suit the user's environment.

M. Alarm / Event Information: The user shall be able to:
- View events throughout the system.
- Dependent on access level, manage the event through acknowledgements, deletions, sorting rules and viewing short and extended messages.
- Use a direct link or hot spot to automatically navigate to the unit that sent the alarm.
- Configure Alarm / Event notifications:
  - Alarm popup tool
  - File write
  - Parallel print
  - E-mail
  - Numeric / alphanumeric paging or SMS
  - Run external program
  - BACnet write
  - SNMP trap notification
  - Attached report via e-mail action

N. Configuration of operators
- User names and passwords:
  - To access the CFMS, an operator must enter a user name and password. This password requirement can be enhanced by using advanced password policies.
  - When enabled, the Advanced password policy includes:
    - Different users may not have the same user name and password.
    - Passwords must contain special characters.
    - Users may not use previous passwords.
    - User names and passwords must have an expiration date.
- System owner will have the ability to assign combinations of roles and privileges to users that define access levels.
  - System-wide privileges allow an operator to perform functions throughout the entire system, such as accessing system configuration or performing a system shutdown.
  - Local privileges allow an operator to perform functions in a specific area of the system, such as editing setpoints or viewing alarms.

O. Audit Log: A log shall record operator activities and some system activities (such as opening and closing the database or automatic deletions) in a text file.

P. Trends: Trends shall be displayed and user-configurable through the Web browser GUI. Trends shall comprise analog, digital or calculated points simultaneously. A trend log's properties shall be editable using the Navigation Tree and Graphic pane.
- **Viewing Trends:** The operator shall have the ability to view trends by using the Navigation Tree and selecting a Trends button in the Graphic pane. The system shall allow y- and x-axis maximum ranges to be specified and shall be able to simultaneously graphically display multiple trends per graph.
- **Local Trends:** Trend data shall be collected locally by Multi-Equipment/Single-Equipment general-purpose controllers and periodically uploaded to the CFMS Server if historical trending is enabled for the BACnet object. Trend data, including run-time hours and start-time date shall be retained in nonvolatile module memory. Systems that rely on a gateway/router to run trends are NOT acceptable.
- **Resolution:** Sample intervals shall be as small as one second. Each trended point will have the ability to be trended at a different trend interval. When multiple points are selected for display that have different trend intervals, the system will automatically scale the axis.
- **Dynamic Update:** Trends shall be able to dynamically update at operator-defined intervals.
- **Zoom/Pan:** It shall be possible to zoom-in on a particular section of a trend for more detailed examination and pan through historical data by simply scrolling the mouse.

- **Numeric Value Display:** It shall be possible to pick any sample on a trend and have the numerical value displayed.
- Trend data must be held in memory at the interface level, such that monitoring system downtime will not reflect a loss of trend data.
- Trend intervals (captures) can be specified on either a time interval or based on COV (a change of value).
- Any trend point in the system can be evaluated versus any other trend point in the system. Unit or location does not exclusively define trends.
- Trend values can be presented in an owner-definable graphical format. The user must be able to vary the presentation of the graph such that colors and lines can be defined to suit the owner's need.
- The data graph must be able to be copied to a clipboard so that it can interface to owner's spreadsheet software products.
- Customized trend graphs can be saved to the navigational tree so that they can be accessed through a click of a button.
- Data storage size at the hardware level must be changeable by the owner / customer.
- Data must be able to be uploaded from the hardware modules for historical reporting functions. Historical data must be able to be maintained for a minimum of 365 days.

Q. **Report writing:** The CFMS shall allow users to view standard reports as well as create user-defined reports.
- Standard reports include, but are not limited to:
  - Audit log
  - Alarm report
  - Locked parameter values
  - Network usage
- User-defined reports (custom) include, but are not limited to:
  - Equipment summaries (Current Status)
  - Equipment values (Current Status)
  - Trend samples (Historical Data)
- Each report will have the ability to be saved electronically. Standard and user-defined reports can be saved in the following file formats:
  - Microsoft Excel®
  - Adobe® PDF
  - CSV (Comma-Separated Values)

2.5   ADVANCED SECURITY PACKAGE

The CFMS shall provide support for 21 CFR Part 11. With this feature enabled, the CFMS can require an operator to record a reason for changing an equipment property before the CFMS accepts the change. The CFMS Audit Log report shall display the operator's name and the recorded reason for making the change.

2.6   GLOBAL PARAMETER CHANGE

The system will have the ability to execute a global parameter change.

2.7   SOFTWARE INTEGRATION

The CFMS shall support Emerson Network Power Aperture brand software integration.

The CFMS shall integrate seamlessly with Aperture brand software. No additional hardware of software will be necessary for integration.

2.8   DEPLOYMENT AS A SERVICE

The CFMS Server shall have the ability to run as an Operating System Service.

2.9 SECURITY

The CFMS shall also be subject to owner's policies for security without effect on CFMS Server or Client operation.

- The system shall not deploy protocols inherently susceptible to intrusion like Telnet or FTP.
- The system shall strip all unnecessary files and services from the Web service to protect the owner from intrusions (hackers).
- General-purpose Web servers like Microsoft IIS are not permitted.

2.10 WEB SERVICES

The CFMS shall support eXtensible Markup Language (XML) and Simple Object Access Protocol (SOAP) for open data exchange between applications. This function provides a standard method for remote applications to work together for a common purpose.

At a minimum, the owner shall be able to retrieve the following using XML/SOAP Web services:

- Real-time status
- Trend data
- Change setpoints
- Get report

2.11 DATABASE SUPPORT

The CFMS shall support the following databases as a minimum:

- Microsoft Access®
- MSDE™
- Microsoft SQL™
- MySQL™
- Oracle®

2.12 ENTERPRISE DB INTEGRATION

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

2.13 PROGRAMMABLE INTERFACE DEVICES

The interface devices shall be easily customizable by the manufacturer or field service representative.

- The user-defined customization must be able to be downloaded to the field device for autonomous operation and not a manipulation of the application software.
- Graphic programs must have real-time, live data
- The user must be capable of reviewing the live data associated to the downloaded program in the interface device.
- The user must be able to make parameter property changes through the live graphic program viewer.

2.14   SOFTWARE COMPONENTS

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

A. Server software, database and Web browser Graphical User Interface

B. System configuration utilities for future modifications to the system

C. Graphical programming tools

D. Application software

E. Database open connectivity: The CFMS Server database shall be Java Database Connectivity (JDBC) compatible, allowing real-time access of data via the following standard mechanisms:

- Open protocol standard like CORBA or SOAP
- Database import from and export to XML (eXtensible Markup Language)

2.15   STAND-ALONE FIELD PANELS - CONTROL MODULES

Control modules must use BACnet as the native communication protocol between controllers.

2.15.1 General Specification

Control modules must be capable of stand-alone direct digital operation utilizing its own 32-bit processor, nonvolatile flash memory, input/output, 12-bit A to D conversion, hardware clock/calendar and voltage transient and lightning protection devices. A separate co-processor shall be used for communications to the controller network. All nonvolatile flash memory shall have a battery backup of at least five years. Firmware revisions to the module shall be made from the CFMS Server or remotely over the intranet or Internet. Controllers that require component changes to implement firmware revisions are NOT acceptable.

A. **Communications Speed:** Modules shall communicate at a minimum of 156 Kbps using ARCNET implemented over EIA-485 using a shielded twisted pair at the Data Link Layer.

B. **Point Programming:** All point data, algorithms and application software within a controller shall be custom programmable from the operator workstation.

C. **Program Execution:** Each control module shall execute application programs, calculations and commands via a 32-bit microcomputer resident in the controller. All operating parameters for application programs residing in each controller shall be stored in read/writable nonvolatile flash memory within the controller and will be able to be uploaded to and downloaded from the CFMS Server.

D. **Self-Test Diagnostics:** Each controller shall include self-test diagnostics, enabling the controller to report malfunctions to the router and CFMS Server.

2.15.2 Input-Output Processing

A. Digital outputs shall be relays, 24 Volts AC or DC maximum, 3 amp maximum current, each configured as normally open or normally closed using jumpers and provide dry contacts. Each output shall have a manual Hand-Off-Auto switch for local override and an LED to indicate the operating mode. Triac outputs are NOT acceptable.

B. Universal inputs shall be thermistor (BAPI Curve II) 10K Ohms at 77°F (25°C), 0-5VDC, 10K Ohms maximum source impedance, 0-20mA - 24 VDC loop power, 250 Ohms input impedance, dry contact - 0.5mA maximum current.

2.15.3 Control Modules with Gateway Functionality

The following panels shall be provided to monitor data points from the equipment to be monitored:

A. **Liebert SiteLink-2/4/12-E:** Module shall have the capacity to interconnect with any combination of two (2), four (4) or twelve (12) Liebert environmental, Power, UPS, Leak Detection Systems or Contact Closure units. The Liebert SiteLink shall communicate directly with the Liebert units via EIA-422 communication cable.

   The Liebert SiteLink-2/4/12E module will have the ability to communicate to other BMS vendors via:

   - Modbus ASCII or RTU Slave via EIA-232, EIA-485
   - BACnet PTP, MSTP or IP
   - LonWorks serial (SLTA required for connectivity to LonTalk network)

B. **Liebert SiteIP-E:** Module shall have the ability to interconnect SNMP v.1 devices. The module shall connect to the monitored devices via the customer's network or private network connection. The modules shall have the ability to support 25 IP addresses or 2000 data points, whichever comes first.

   End user is responsible to supply IP address and read/write community strings and/or access to SNMP device configuration.

C. **Liebert SiteTPI-E:** Module shall integrate third-party equipment into the CFMS via the following open protocols:

   - BACnet PTP, MSTP or IP
   - Modbus ASCII or RTU via EIA-485 or IP

   Module may be configured for Master or Slave communications.

D. **Liebert SiteI/O-E:** The Liebert SiteI/O-E Module shall have the capability to monitor any combination of ten (10) universal outputs for the following:

   - Digital inputs (0.5mA maximum current sense)
   - Thermistor inputs (10K Ohms @ 77°F or 25°C - Precon Type 2)
   - Analog input (4-20mA - 24VDC loop power, 250 Ohms impedance; 0-5VDC or 0-10VDC - 10K Ohms maximum source impedance).
   - RTD sensor supported
   - The Liebert SiteI/O-E will also have four (4) universal outputs. Digital outputs are to 24VDC relay driver so an external relay must be provided.
   - Analog outputs: 4-20mA - 0-5VDC or 0-10VDC (minimum resistance to ground must be 500 Ohms) or 0-20mA (maximum resistance to ground must be 800 Ohms).
   - Device must share same ground as the control module; total output current from all outputs and Aux Power Out connection must not exceed 400mA at 125°F (52°C) or 300mA at 140°F (60°C).

E. **Liebert Information Gathering Modules (IGMs) External:** The external Liebert IGMs shall connect directly to the Liebert SiteScan System with an EIA-422 data link and shall consist of the following IGMs:

   - LPS0240, LPL1150, LPL2300 Direct Read Liquid Detection
   - Liebert Distribution Monitoring LDM™
   - Liebert Universal Monitor
   - Liebert AC8™

3.0 EXECUTION

3.1   GENERAL

Contractor, unless specified in other sections of the specifications, shall install all equipment and devices furnished under this section of these specifications. Contractor shall 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.

NOTE: These Guide Specifications comply with the format outlined by the Construction Specifications Institute per CSI MP-2-1 and CSI MP-2-2. In correspondence, reference Liebert document SL-27100_REV02_04-10.