APC by Schneider Electric

InfraStruxure Central v6.2

Datacenter Infrastructure Management System Specification

SECTION [27 60 00]

DATACENTER INFRASTRUCTURE MANAGEMENT SYSTEM

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General Conditions, [Division 01 - GENERAL REQUIREMENTS] [Division 1 - GENERAL REQUIREMENTS], and other applicable specification sections in the Project Manual apply to the work specified in this Section.

1.2 SUMMARY

A. **Scope:** This specification describes the operation and functionality of a Datacenter Infrastructure Management system (DCIM) hereafter referred to as the DCIM. The DCIM shall be a centralized server appliance with a client console. The system shall have an architecture that allows for increasing the number of devices it manages up to 4025 devices. The system shall have the ability to manage 4025 devices on the public Local Area Network (LAN) or have the ability to manage 4025 devices on a private Local Area Network (LAN). The System shall operate in a manner allowing for management of a total of 4025 devices that can reside on both the public LAN and the private APC LAN. The System shall also be of an architecture that allows for monitoring of Multi-Vendor Simple Network Management Protocol (SNMP) devices, Modbus TCP devices, and Modbus RTU devices that are connected to a Modbus RTU-to-Modbus TCP gateway. The Basic system shall be a 1U rack mountable design, the Standard system shall be a 1U rack mountable design, and the Enterprise System shall be 2U in design and fault tolerant.

B. **Section Includes:** This specification shall provide infrastructure management of the Uninterruptible Power System (UPS); Power Distribution Unit (PDU); Rack PDU (rPDU); Computer Room Air Conditioning (CRAC); In-row Cooling; Environmental Sensors; Automatic Transfer Switch (ATS) with supplied Generator; Surveillance Cameras (all the above supplied by the DCIM vendor); SNMP devices from multiple vendors (ex. UPS, PDU, CRAC, and rPDU); Modbus devices; and other infrastructure systems as specified.

C. The DCIM and associated equipment shall operate in conjunction with an existing network infrastructure to provide system management of the systems described above.

1.3 APPROVED PRODUCTS

A. The Datacenter Infrastructure Management system (DCIM) shall be InfraStruxure Central, manufactured by APC by Schneider Electric. Substitutions shall only be permitted subject to 2.1, below.

1.4 REFERENCES

A. FCC Part 15, Sub-Part B, Class A
B. CE EMC Directive, CTICK, Industry Canada
C. EN60950-1
D. CE Safety (Directives 73/23/EEC&89/336/EEC), VDE Safety Approval
E. Where applicable, the DCIM shall also be designed in accordance with publications from the following organizations and committees:
   1. NFPA – National Fire protection Associations
   2. NEMA – National Electrical Manufacturers Association
   3. OSHA – Occupational Safety and Health Administration
F. ISO 9001
G. ISO 14001

1.5 SYSTEM DESCRIPTION

A. **Design Requirements:**
   1. All material and equipment used shall be standard components, regularly manufactured, available and not custom designed especially for this project. The datacenter infrastructure system, including the DCIM, shall previously be thoroughly tested as a system, and proven in actual use prior to installation on this project.
   2. The DCIM shall be a server appliance, with a specified HTTP or HTTPS connection to access the user interface, and standard TCP protocol connections for notifications.
   3. The Basic and Standard systems shall be a 1U rack mountable design. The Enterprise System shall be a 2U rack mountable design, with dual processors, redundant power supplies, and a fault tolerant RAID-5 design.
   4. The Basic system shall be scalable up to 525 managed/monitored devices and support up to 15 NetBotz Appliances.
   5. The Standard system shall be scalable up to 2025 managed/monitored devices and support up to 125 NetBotz Appliances.
   6. The Enterprise system shall be scalable up to 4025 managed/monitored devices and support up to 250 NetBotz Appliances.
   7. The manufacturer will supply an off the shelf management system that will require no factory customization to meet customer requirements.
   8. The system architecture shall be scalable, allowing for future enhancements.
   9. The DCIM shall manage/monitor devices both on a public LAN and on a private LAN created by the management system.
   10. The DCIM shall be capable of managing a total of 4025 devices on a public LAN or a private LAN.
   11. The DCIM shall be capable of hosting additional add-on modules that support a Building Management System (BMS), Power Management System, and Mobile Applications, and allow a user to perform Physical Threat and Environment Management, Surveillance, Energy Efficiency and Energy Cost Management, Inventory Management, Power and Cooling Capacity Management, and Change Management.
   12. The DCIM shall be capable of integrating with additional plug-ins that support Cisco EnergyWise (network management systems), Schneider Electric PowerLogic ION Enterprise (power management systems), Microsoft System Center Operations Manager and System Center Essentials, HP Operations Manager for Windows, and IBM Tivoli (enterprise management systems).

B. **System Characteristics:**
   1. The (LAN) hardware needed to provide an Ethernet gateway used for communication between the DCIM and the managed devices as well as providing the communication link between the DCIM and the remote client accessing it. The components needed may include switches, routers, hubs, Category 5/Category 6/Fiber cables, IP addresses, firewalls, client workstations/servers, and any miscellaneous components that may be determined to be required. The owner of the location the DCIM is installed in, the managed devices, and the client workstation/server accessing the DCIM shall provide 10/100/1000 base T network drops.

2. The DCIM shall meet the following server appliance requirements:
   a. The Basic and Standard system shall be a 1U rack mountable design, and the Enterprise System shall be a 2U rack mountable design.
   b. The Enterprise system shall have dual processors, redundant power supplies, and a fault tolerant RAID-5 design.
   c. Public LAN and Private LAN (10/100/1000 base T) network ports.
   d. USB ports for future use.
   e. Fedora Core 9 as the server operating system
   f. Architecture to schedule discovery of devices connected on the Public LAN and assign IP addresses to devices connected to the private LAN.
   g. Architecture to monitor multi-vendor SNMP devices (UPS, PDU, Rack PDU, CRAC, or other SNMP devices specified) and Modbus devices.
   h. Monitor / keyboard port for field service diagnostic purposes only.

3. The DCIM client workstation/server shall have the following minimum requirements:
   a. Microsoft Windows 2003 Server (SP2), Microsoft Windows XP (SP3), Microsoft Vista, or Microsoft Windows 7
   b. Red Hat Enterprise Linux v5.0 or higher
   c. Java Plug-in (JRE) version 1.6.0_22

4. The owner will supply the following information to facilitate system implementation:
   a. Network configuration settings (IP addresses, subnet mask) necessary for the DCIM and any device to reside on the owner’s public or private network.
   b. E-mail addresses and SMTP settings for e-mail notification.
   c. Device group structure
   d. Network Management System (NMS) IP address and community names to accept SNMP traps.
   e. Building Management System, Building Control System, or Building Automation System to accept Modbus TCP data and events from managed/monitored devices

C. **Contractor’s Responsibilities:** The contractor shall perform the following, if the listed equipment is not purchased by the owner from the DCIM Vendor:
   1. Provide the Category 5, Category 6, or fiber network connection to DCIM.
   2. Provide the Category 5, Category 6, or fiber network connection to the devices managed/monitored by DCIM.
   3. Provide control wiring to optional Environmental Sensors for monitoring of dry contact points and or 4-20milliamp signals.

D. **Management System Vendor Responsibilities**
   1. Provide the hardware and software pre-installed and tested on a 1U or 2U rack mountable server.
   2. Provide system start-up, commissioning, and operator orientation by factory employed Field Service Engineer. This shall include discovery of devices and creation of the customer defined grouping structure for devices.
   3. Provide 7 x 24 technical support through a toll free number per the Software Support Contract.
   4. Provide Parts & Labor warranty and Technical Support per the manufacturer’s warranty and Software Support Contract.
   5. If purchased by the owner, termination of all Category 5, Category 6, and other 0-5V connections, Modbus connections, or Fiber connections to the DCIM and the managed/monitored devices.

E. **Conduit and Wiring:** Conduit and wiring is provided under Division 16. The Contractor is responsible for termination of all control wiring used for connection to optional Environmental Sensors for monitoring of dry contact points and or 4-20milliamp signals.

1.6 SUBMITTALS

A. **Proposal Submittals:**

1. As bid system bill of materials
2. Product catalog sheets or equipment brochures
3. Product guide specifications
4. Network single-line operation diagram
5. Installation information, including requirements
6. Information about terminal locations for network connectivity and control wiring connections
7. Drawings and details for requested optional accessories

B. **Delivery Submittals:**

1. Installation manual, which includes instructions for storage, handling, examination, preparation, installation, and start-up of DCIM
2. CD, which includes an Installation Guide and a Users Manual, which shall be translated from English into the following languages:
    1. Japanese
    2. Simplified Chinese
    3. Russian
    4. French
    5. Italian
    6. German
    7. Korean
    8. Brazilian Portuguese
    9. Spanish
3. As built equipment drawings
4. InfraStruxure™ Welcome Package

1.7 QUALITY ASSURANCE

A. **Qualifications:**

1. **Manufacturer Qualifications:** Manufacturer shall be a firm engaged in the manufacture of datacenter infrastructure management systems of types and sizes required, and whose products have been in satisfactory use in similar service for a minimum of 10 years.
    a. The manufacturer shall be ISO 9001 certified and shall be designed to internationally accepted standards.
2. **Installer Qualifications:** Installer shall be a firm that shall have a minimum of five years of successful installation experience with projects utilizing datacenter infrastructure management systems similar in type and scope to that required of this Project.

B. **Regulatory Requirements:** Comply with applicable requirements of the laws, codes, ordinances, and regulations of Federal, State, and local authorities having jurisdiction. Obtain necessary approvals from such authorities.

1. Where applicable, the DCIM shall also be designed in accordance with publications from the following organizations and committees:
    a. FCC Part 15, Sub-Part B, Class A
    b. CE EMC Directive, CTICK, Industry Canada
    c. EN60950-1
    d. CE Safety (Directives 73/23/EEC&89/336/EEC), VDE Safety Approval
    e. Where applicable, the DCIM shall also be designed in accordance with publications from the following organizations and committees:
        i. NFPA - National Fire Protection Associations

ii. NEMA - National Electrical Manufacturers Association
iii. OSHA - Occupational Safety and Health Administration
f. ISO 9001
g. ISO 14001

C. **Pre-Installation Conference:** Conduct pre-installation conference in accordance with [Section 01 31 19 - PROJECT MEETINGS] [Section 01200 - PROJECT MEETINGS]. Prior to commencing the installation, meet at the Project site to review the material selections, installation procedures, and coordination with other trades. Pre-installation conference shall include, but shall not be limited to, the Contractor, the Installer, and any trade that requires coordination with the work. Date and time of the pre-installation conference shall be acceptable to the Owner and the Architect/Engineer.

1.8 DELIVERY, STORAGE, AND HANDLING

A. Deliver materials to the Project site in supplier’s or manufacturer’s original wrappings and containers, labeled with supplier’s or manufacturer’s name, material or product brand name, and lot number, if any.

B. Store materials in their original, undamaged packages and containers, inside a well-ventilated area protected from weather, moisture, soiling, extreme temperatures, and humidity.

1.9 PROJECT CONDITIONS

A. **Environmental Requirements:** Do not install datacenter infrastructure management system until space is enclosed and weatherproof, wet work in space is completed and nominally dry, work above ceilings is complete, and ambient temperature and humidity conditions are and will be continuously maintained at values near those indicated for final occupancy.

1. **Environmental:**
   a. **Storage Ambient Temperature:** -58 °F (-50 °C) to 131 °F (55 °C)
   b. **Operating Ambient Temperature:** 32 °F (0 °C) to 104 °F (40 °C) (77 °F [25 °C] is ideal for most battery types)
   c. **Relative Humidity:** 0 percent to 95 percent non-condensing.
   d. **Altitude:** Maximum installation with no derating of the UPS output shall be 3280 feet (1000 m) above sea level. At higher altitudes the following derating shall apply:
      1) 4921 feet (1500 m) derating factor of 0.95.
      2) 6562 feet (2000 m) derating factor of 0.91.
      3) 8202 feet (2500 m) derating factor of 0.86.

1.10 WARRANTY

A. **General:** See [Section 01 77 00 - CLOSEOUT PROCEDURES] [Section 01770 - CLOSEOUT PROCEDURES].

B. **Special Warranty:** The Contractor shall warrant the work of this Section to be in accordance with the Contract Documents and free from faults and defects in materials and workmanship for period indicated below. This special warranty shall extend the one year period of limitations contained in the General Conditions. The special warranty shall be countersigned by the Installer and the manufacturer.

1. **Datacenter Infrastructure Management System:** The DCIM shall be covered by a full parts and labor warranty from the manufacturer for a period of 24 months from the date of installation or acceptance by the Owner or 18 months from the date of shipment from the manufacturer, whichever occurs first.

C. **Additional Owner Rights:** The warranty shall not deprive the Owner of other rights the Owner may have under other provisions of the Contract Documents and shall be in addition to and run concurrent with other warranties made by the Contractor under requirements of the Contract Documents.

1.11 MAINTENANCE

A. A complete offering of software support contracts and node licenses for the DCIM shall be available from the manufacturer, and shall be required to provide ongoing technical support and allow future software updates. Contract work shall be performed by factory-trained service personnel.

PART 2 - EQUIPMENT

2.1 MANUFACTURERS

A. **Basis of Design:** Product specified is “APC InfraStruxure Central v6.2” as manufactured by APC by Schneider Electric. Items specified are to establish a standard of quality for design, function, materials, and appearance. Equivalent products by other manufacturers are not acceptable. The Architect/Engineer will be the sole judge of the basis of what is equivalent.

2.2 MODES OF OPERATION

A. **System Overview:** The DCIM shall be a centralized server appliance that is accessed remotely from client workstations/servers via a HTTP or HTTPS connection. No client-based services shall be used as a substitute. Microsoft System Center Operations Manager, Microsoft System Center Essentials, IBM Tivoli, HP Operations Manager integration shall be supported. A Web Services Open API guide shall be made available by the DCIM vendor. The DCIM shall send alerts from the devices it manages to a valid e-mail account accessible via PDA or Blackberry®; a web page via HTTP POST; an FTP server; SNMP traps to a Network Management System; and Modbus events to a Building Management System. These shall be a standard part of the DCIM notification architecture.

B. The DCIM server console must support the following:

a. Microsoft Windows Server 2003 (SP2), Microsoft Windows XP (SP3), Microsoft Vista, and Microsoft Windows 7
b. Red Hat Enterprise Linux v5.0 and higher
c. Java Plug-in (JRE) version 1.6.0_22

C. **Modbus:** The DCIM shall provide access to a separately licensed MODBUS TCP Output Module used to support the Building Management System (BMS). The MODBUS TCP Output Module shall communicate with the Building Management System (BMS) on port 502. Devices that use the Modbus TCP protocol, and Modbus RTU devices that are connected to a Modbus RTU–to–Modbus TCP gateway, shall be discovered and monitored.

D. **User Interface:** The DCIM shall provide a Monitoring perspective and Surveillance perspective to display device status, device data, device events, and surveillance video; an Alarm Configuration perspective to provide notification options; a Reports perspective to access reports about monitored devices and provide configuration and graphing/trending options; and a Power Management perspective to access PowerLogic™ ION Enterprise WebReach and WebReports.

1. **Monitoring Perspective**
   A. **Device Groups**

1. The user shall be able to define groups in a tree format. This shall allow a user to add groups by right clicking the All Devices group or on a sub group and select Create Device Group.
2. The user shall have the ability to drag and drop devices into device groups. The user shall also have the ability to multi-select devices and drag them into created groups.
3. The user shall have the ability to right click on a device group and rename or delete the device group.
4. The user shall control access to each of the groups by defining the users that have access to that device group.
5. Devices shall have the ability to reside in multiple groups.
6. The Device Groups window shall have a button icon to run a Graphing/Trending report, and a button icon to minimize or maximize the Device Group view to full screen size.

B. **Device View**

1. The DCIM shall display all discovered devices in a separate window and display device status of normal, warning or critical. This status shall be real time status and updated as events occur, not based on a poll cycle.
2. The Device View shall display the total number of discovered devices and the number of displayed devices.
3. The Device View shall allow the user to sort the displayed columns by clicking each one.
4. The Device view shall allow the user client preferences to highlight a device that is in a critical state.
5. The Device View shall have user selectable columns displaying the following:
    a. Device Type
    b. Status
    c. Location
    d. Label
    e. Model
    f. Hostname
    g. Parent Device
    h. Serial Number
    i. IP Address
    j. Application Version
    k. Groups
    l. MAC Address
    m. Maintenance Mode
6. The user shall have the ability to right click in the Device View and perform the following actions:
    a. Add Devices
    b. Delete Devices
    c. Remove from Device Group
    d. View Device Sensors
    e. Request Device Scan
    f. Launch to Device
    g. Show Alarm History
    h. Generate Sensor History Report, including graphing
    i. Create Thresholds
    j. SNMP Device Configuration
    k. NetBotz Appliance Configuration
    l. Enter/Exit Maintenance Mode

        m. Change Device Type
        n. Add Custom Property
    7. The Device View pane shall contain a free text field to search for devices.

2. **Surveillance Perspective**
    A. The DCIM shall have the ability to display camera images in central pane by selecting the Surveillance tab within the user interface. This tab shall have the following functionality:
        1. Thumbnails:
            a. This view shall display the images of all managed cameras. This view shall also highlight the camera image border in yellow, when any camera is in an alert state.
            b. This view shall allow the user to select the thumbnail size in either 160 x 120 or 320 x 240.
            c. This view shall allow the user the ability to right click on a thumbnail and open camera view. This view shall be date and time stamped.
        2. Retrieve Clips: The user shall have the ability to either right click on the thumbnail or click on a retrieve clips radio button in the thumbnail view in order to retrieve clips:
            a. The user shall have the ability to search for clips either by relative date or by date range.
            b. The user shall have the ability to display clips based on defined tags/descriptions.
            c. The user shall have the ability to view the displayed clips, tag the displayed clips, delete the displayed clips, or export the displayed clips.
            d. The user shall have the ability to view the displayed clips, tag the displayed clips, delete the displayed clips, or export the displayed clips:
                a. Pod Label
                b. Hostname
                c. Location
                d. Status
                e. Licensed
                f. Model
                g. Device Groups
                h. Camera Label

    B. **Third Party Closed Circuit Television Integration (CCTV)**
        1. The DCIM shall be capable of integrating CCTV into Surveillance using a CCTV Adapter.
            a. The CCTV Adapter Pod shall accept multi-format S-Video and Composite Video as well as featuring DIN, BNC, and RCA input jacks.
            b. The CCTV Adapter pod shall also feature a USB port to enable the pod to be tethered to the base station using a standard USB cable.
            c. The CCTV pod shall convert an analog video source into a digitally converted signal, which shall be integrated into the NetBotz physical security solution.
            d. The CCTV Adapter Pod shall display Images of up to 640x480 resolution, 24-bit color, and up to 30 frames per second (color and resolution may be limited by video source).
            e. The CCTV Adapter Pod shall have an Integrated microphone, as well as a microphone jack (standard 3.5mm miniplug), which shall provide the ability to monitor and capture monophonic audio from the location in which the pod or external microphone are installed.

f. The CCTV adapter Pod shall have an integrated Speaker/headphone jack (standard 3.5mm stereo miniplug) that can be used with unpowered headphones or powered speakers to provide monophonic audio output.
g. The CCTV Adapter Pod shall have an integrated Door Switch Sensor jack (magnetic door switch sensor available separately).
h. The CCTV Adapter Pod shall have integrated Camera Motion Detection.

3. **Reports Perspective**

A. Data shall be collected for the Uninterruptible Power System (UPS), Power Distribution Unit (PDU), Rack PDU (rPDU), Computer Room Air Conditioning (CRAC), Environmental Sensors, Automatic Transfer Switch (ATS) with supplied Generator, Surveillance Camera's (all the above supplied by the DCIM vendor) Multi-vendor SNMP devices (UPS, PDU, CRAC, and rPDU), and other infrastructure systems as specified.

Data collected over time must be stored on a dedicated data partition located on the server appliance for extracting and trending and /or can be exported to a Network Attached Storage Server (NAS).

1. Data collection poll cycles shall be user defined in the user interface to collected data from 1 minute to every 24 hours.
2. Saved Sensor History Reports shall be listed alphabetically in the user interface in the Reports perspective.
3. Data shall be exportable to a NAS Server in a plain text format that shall have a selectable data delimiter of a Semicolon, Comma, Tab, or Space.
4. Data shall be exportable through e-mail, FTP, HTTP, or to a Windows (CIFS) or a Unix (NFS) file share.
5. Device reports shall be run manually through a "Generate Report" button, or reports shall be delivered automatically on a scheduled basis.
6. Device data shall be accessed from the Sensor History Report or Snapshot Report, located in the Reports perspective.
7. The user shall have the ability to create sensor history reports that display line graphs for multiple data points, with data points to be charted on two axes for collected data.
8. The sensor history graph-format reports shall display a linear trend line for twice the time period as the data, on numeric sensors only, when all numeric sensors included in the graph use the same unit of measure.
9. The sensor history graph-format reports shall also display numeric values for the sensor(s) chosen. These numeric values shall display the Low, High and Average, for the time period chosen.
10. The user shall have the ability to create user defined summary-format reports for a device, group of devices, or specific sensors for a particular device, that shall display the High, Low, Average, and the Current value for the user defined time period.
11. The user shall have the ability to create user-defined table-format reports for a device, group of devices, or specific sensors for a particular device, that shall display the Current values for the user defined time period.
12. The user shall have the ability to create pre-defined snapshot reports for one or more specific device groups that shall display the Current values for the particular time the report is generated.

13. The user shall have the ability to monitor the status of storage repositories defined for use with your DCIM server to configure the automatic disk space management system.

4. **Configuration**

   A. **Device Discovery**

      1. The user interface shall allow for discovery of devices by IP address range.
      2. The DCIM shall place all newly discovered devices in an Unassigned group until the user places them in a Created Device Group.
      3. The DCIM shall be capable of auto discovering devices when connected to the private LAN Network A, as well as functioning as a DHCP server to assign IP addresses from a user defined IP address scheme. The DCIM shall also be capable of discovering devices with static IP addresses on the private LAN Network B, defined by its IP address and subnet mask.
      4. The user shall have the ability to schedule discovery of new devices with the following configurable settings:
         a. IP or IP Range
         b. SNMP Settings
         c. Day of the week
         d. Time of the day
      5. The public LAN and/or the private LAN shall have the ability to manage up to 4025 devices.
      6. The user shall have the ability to register the discovered devices for SNMP trap directed polling.
      7. The DCIM shall have the ability to save the created discoveries and display them in a separate tab displaying the following:
         1. IP or IP Range
         2. Periodically
         3. Type of Discovery
         4. Activity
         5. Last run
      8. The DCIM shall also display how many device discoveries are in progress.
      9. The user shall have the ability to import saved device discoveries from a local file, or right click a saved discovery and add a new discovery, edit the highlighted discovery, delete the highlighted discovery, or run the highlighted discovery.

   B. **Building Management Integration**

      1. The DCIM shall communicate device data and events up to a Building Management System (BMS) using the Modbus TCP protocol.
      2. The DCIM shall communicate Modbus TCP using port 502.
      3. The DCIM Building Management Settings shall allow the user to select the devices that will communicate with the BMS.
      4. The DCIM Building Management Settings shall allow the user to generate and remove the slave addresses assigned to each device.
      5. The DCIM Building Management Settings shall have a free text field to search for devices.
      6. The DCIM Building Management Settings shall allow the user to select the data points to manage and define the Modbus register mappings.
      7. The DCIM shall send data to a BMS for discovered multi-vendor devices.
      8. The DCIM Building Management Settings shall allow the user to export the Modbus register mappings and allow the user to import those into additional DCIM.

   C. **Network Management System Integration**

1. The DCIM shall send SNMP traps for connected devices to a user defined Network Management System (NMS).
2. The User shall have the ability to choose a SNMPv1 or SNMPv3 Trap receiver.
3. The user shall have the ability to define the following:
    a. IP address of the NMS
    b. SNMP port
    c. Read Community Name
    d. Severity Level
4. The user shall have the ability to Enable/Disable Traps.

D. **Enterprise Management System Integration**

1. The DCIM shall integrate with the separately licensed InfraStruxure Operations modules for Energy Efficiency and Energy Cost Management, Power and Cooling Capacity Management, Change Management, and Mobile Applications.

E. **Power Management Integration**

1. The DCIM shall be capable of integrating with PowerLogic™ ION Enterprise WebReach and WebReports through the Power Management perspective.

F. **Mass Configuration of Devices**

1. The DCIM shall have the ability to mass configure devices manufactured by the DCIM vendor. This feature does not apply to Multi-Vendor devices.
2. The DCIM shall have the ability to mass configure NetBotz Appliances with the following Mass Configuration options:
    a. Backup/Restore
    b. Camera Settings
    c. Clock Settings
    d. DNS Settings
    e. E-mail Settings
    f. Location Settings
    g. Pod Sharing settings
    h. Post Alert Data settings
    i. Region Settings
    j. Serial Device Settings
    k. SMS Settings
    l. SNMP Settings
    m. User Settings
    n. Web Server Settings
3. DCIM shall have the ability to Mass Configure all settings related to APC devices.
4. The DCIM shall allow the user to select the specific settings to push to the selected APC devices.
5. The DCIM shall have the ability to create a template of settings for the APC devices the user is configuring.
6. The DCIM shall have the ability to edit the template of settings created for the configuring the APC devices.
7. The DCIM shall have the ability to configure APC devices from the template of settings created.
8. The DCIM shall have the ability to multi-select the devices the user is configuring.

G. **Mass Firmware Updates**

1. The DCIM shall have the ability to apply firmware updates to devices manufactured by the DCIM vendor. This feature does not apply to Multi-Vendor devices.
2. The DCIM shall have the ability to schedule an update check to see if new firmware is available.
3. The DCIM shall have the ability to display all devices needing updates.
4. The DCIM shall have the ability to allow the user to select all devices needing updates or select individual devices needing updates.

H. **Scalable Architecture**

1. The DCIM shall have the ability to be scaled to manage up to 4025 devices, with additional device licenses. There shall be no customization or programming involved from the DCIM vendor to add additional devices.

I. **Event Notification**

1. The user shall have the ability to view events from the entire DCIM from an Alarms view.
2. The user shall have the ability to click on a managed device in an alarm state and display the specific nature of the alarm in an Alarm Details pane.
3. The user shall have the ability to configure notification for managed devices based on specific sensors, for the maximum threshold, minimum threshold, range value, below value for time, and above value for time.
4. The DCIM shall have SMS support, when sending notification to a defined user, which will allow the user to configure the text sent.
5. The DCIM shall contain an Alarm History for all managed devices, which shall be sortable by date range.
6. The Alarm History shall display the Time Occurred, Time Resolved, Status, Description, Severity, Device Hostname, Parent Device, and Sensor.

J. **Network Time Protocol (NTP)**

1. The DCIM shall have the ability to act as an NTP server, or synchronize to a user defined NTP server.

2.3 Datacenter Infrastructure Management System Security

A. **Authentication and Encryption:** The communication between the client and the DCIM shall be secured via a Secure Sockets Layer (SSL) 168-bit Triple-DES (Data Encryption Standard) encoded connection.

B. **OpenLDAP and Active Directory:** The DCIM shall have Open Lightweight Directory Access Protocol and Active Directory support.

C. The log in to the user interface of DCIM shall use Secure Socket Layer (SSL) or Secure Socket Handling (SSH) authenticate. The web launch to devices shall occur through a HTTP or HTTPS connection. To increase security, the HTTP or HTTPS connection and the HTTP or HTTPS port shall be user configurable for each device, through the DCIM user Interface.

D. The DCIM shall allow the user to create user accounts ranging from Administrator Access to View Only Access. The DCIM shall have no specified limit to the number of user accounts that can be created. Each of these accounts shall have their own unique login user name and password. An administrator shall have full read/write access to all the DCIM’s functionality. The “View Only Access” users shall only have access, limited to viewing specific groups or devices within those groups, as well as creating graphing trending reports as well as exporting device data reports. The “Read Only” access user shall not be allowed to change the DCIM configuration or device configurations.

E. The DCIM shall have the ability to communicate SNMPv1 or SNMPv3 to monitored/managed devices.

PART 3 - EXECUTION

3.1 EXAMINATION

A. **Verification of Conditions:** Examine areas and conditions under which the work is to be installed, and notify the Contractor in writing, with a copy to the Owner and the Architect/Engineer, of any conditions detrimental to the proper and timely completion of the work. Do not proceed with the work until unsatisfactory conditions have been corrected.
1. Beginning of the work shall indicate acceptance of the areas and conditions as satisfactory by the Installer.

3.2 INSTALLATION

A. **General:** Preparation and installation shall be in accordance with reviewed product data, final shop drawings, manufacturer’s written recommendations, and as indicated on the Drawings.

B. **Factory-Assisted Start-Up:** If a factory-assisted DCIM start-up is requested, factory-trained service personnel shall perform the following inspections, test procedures, and on-site training:
1. **Visual Inspection:**
   a. Inspect equipment for signs of damage.
   b. Verify installation per manufacturer's instructions.
2. **Mechanical Inspection:**
   a. Check the network connections to the DCIM.
   b. Check the network connections to all managed/monitored devices.
   c. Ensure the DCIM is powered and verify power to the optional DCIM Hub (if installed).
3. **Functional Inspection:**
   a. Ensure you can log in to the DCIM.
   b. Ensure any additional license keys are installed on the DCIM.
   c. Verify discovery of managed/monitored devices.
   d. Ensure the owner’s defined groups are configured in the DCIM.
4. **Site Testing:**
   a. Ensure proper notification of alarms through the user interface.
   b. Verify proper notification of alarms through e-mail.
   c. Document, sign, and date test results.
5. **On-Site Operational Training:** During the factory-assisted start-up, operational training for site personnel shall include log in to the user interface, navigation through the menu options, device discovery, generation of reports, creation of groups, creation of users, and setting up alarm notification.

3.3 FIELD QUALITY CONTROL

A. **General:** See [Section 01 45 23 - INSPECTING AND TESTING SERVICES] [Section 01410 - INSPECTING AND TESTING SERVICES].

B. **Manufacturer Field Service:**

1. **Worldwide Service:** The DCIM manufacturer shall have a worldwide service organization available, consisting of factory-trained field service personnel to perform start-up, preventative maintenance, and service of the DCIM system and power equipment. The service organization shall offer 24 hours a day, 7 days a week, 365 days a year service support.
2. **Replacement Parts:** Parts shall be available through the worldwide service organization 24 hours a day, 7 days a week, 365 days a year. The worldwide service organization shall be capable of shipping parts within four working hours or on the next available flight, so that the parts may be delivered to the Owner within 24 hours.

3.4 MAINTENANCE CONTRACTS

A. **A complete offering of Software Support Contracts** for the DCIM shall be available. All DCIM systems under this software support contract shall be entitled to Technical Phone Support, all Software Updates, Feature Enhancements, and development of Multi-Vendor device support during the duration of this contract.

B. **A Statement of work for the Software Support Contracts** shall be made available for the DCIM detailing vendor responsibilities and customer responsibilities.

3.5 DEMONSTRATION

A. **General:** Provide the services of a factory-authorized service representative of the manufacturer to provide start-up service and to demonstrate and train the Owner's personnel.

B. **DCIM Training Workshop:** A DCIM training workshop shall be available from the DCIM manufacturer. The training workshop shall include, but shall not be limited to, a combination of lecture and practical instruction with hands-on laboratory sessions. The training workshop shall include a combination of lecture and practical instruction with hands-on laboratory sessions. The service training workshop shall include instruction DCIM operational theory, configuration and operation, report generation, device discovery, and troubleshooting.

END OF SECTION