Integrated Automated Controls for Data Centers-Philosophy & Approach

White Paper #8

SYSKA HENNESSY GROUP

Consulting + Engineering + Technology + Construction

Integrated Automated Controls for Data Centers – Philosophy & Approach

By Carlos Petty, Associate Partner
Syska Hennessy Group, New York, NY

Critical facilities such as data centers use a wide range of mechanical-electrical support systems that are essential to their day-to-day operations. These support systems are very sensitive resources which upon failure would cause loss of data and pose a possible threat to the environment. Protecting these resources from predictable, as well as unpredictable conditions or abnormal situations requires advanced environmental monitoring and control. In addition to standard lighting, heating, cooling and ventilating systems, energy that is used in critical facilities require different approaches and strategies to reduce energy consumption. In Data Centers, energy use accounts for a significant and increasing portion of operating costs. Managing energy consumption without compromising reliability or environmental requirements presents a challenge. The challenge in cutting costs lies in improving equipment performance while reducing energy consumption without diminishing the comfort, safety or security of this environment.

A clear philosophy and approach that embraces technology trends and energy-efficient automation measures used in combination for critical facilities will reduce overall energy use. Improving system performance, while simultaneously reducing energy consumption, has sparked the need for increased system automation and system integration. A successful building automation system design recognizes and takes advantage of new control products by implementing new control strategies that compliment each product.

Today's design trends include use of programmable logic controllers (PLCs) for critical central plant equipment, monitoring of uninterruptible power supplies (UPS) and power quality monitoring, leak detection/hydrogen detection systems, instant alarm forwarding/notification, lighting control, security access control/CCTV surveillance systems, ventilation controls, permanent air quality monitoring, utility metering and communication via a structured cable plant.

The controls industry has recognized this increased need for component, equipment, and system interrelatedness and is moving to more open communication protocols that facilitate easier integration into local and/or distributed facility monitoring and control systems. Many controls vendors are moving away from proprietary, vendor specific communication protocols and are implementing web-based, enterprise-friendly standard protocols such as SOAP, XML, SNMP, etc. The acceptance of BACnet and LONWorks as component level open protocols has also allowed more flexibility for facilities to install intelligent control devices onto existing computerized control systems.

Use Programmable Logic Controllers (PLCs) for Critical Plant Equipment

Critical facility environments require sophisticated controls. Mechanical and electrical systems supporting the critical environment must be designed with redundant equipment to reduce single "points-of-failure". The use of programmable logic controllers to monitor and control mission critical equipment has quickly become the "de-facto" application. Programmable Logic Controllers (PLCs) should be utilized for all central utility plant equipment serving critical facilities such as: primary/secondary chillers, backup chillers, cooling towers, associated pumps, fuel oil systems and normal and emergency electrical distribution systems. Each primary PLC should be designed with a corresponding backup PLC in a "mirrored" configuration to

automatically and seamlessly perform the same functions as the lead PLC upon failure of the primary PLC.

The system architecture should consist of a network of independent, standalone programmable logic controllers (PLCs) that support dual communications over a high speed (100 Mb) Industrial grade Ethernet Transmission Control Protocol/Internet Protocol (TCP/IP) local area network (LAN) using an IP protocol. Fiber optic cabling should be specified to ensure the control network has communication speed capability to support large data communication demands. The LAN should be installed in a ring configuration between each PLC, physically using separate communication paths to provide overall system redundancy. Communication cables should be installed in rigid conduit for physical protection. The LAN must incorporate full duplex communication between PLC controllers, servers, and workstations connected to the LAN. The PLC LAN should support a minimum of two (2) servers, which operate in a fully redundant synchronized manner ("mirrored" servers). One server will operate as the primary server, while the other operates as the backup. Upon detection of a system fault or loss of a "heartbeat" signal disabling the primary server, the backup server will switch over and provide all functions of the primary server in a seamless manner that ensures uninterrupted monitoring, control, and operation of the critical facility infrastructure. When the primary server fault has been corrected and the server restarted, the system automatically updates the primary server and switches over from backup to primary server on completion of the update.

New programmable logic control units are capable of sharing point information with other programmable control units. The PLC LAN allows for data transfer between PLC's directly, such that control sequences or closed loop control executed at one control unit may receive input signals from sensors connected to other units on the network. If the PLC Ethernet LAN

communications link fails or the originating PLC unit malfunctions, the control loop can continue to function, using the last value received from the failed control unit. This should result in a control system alarm notifying the facility operators that the control system is continuing operations with compromised input data.

Power Quality Monitoring

High-speed power quality monitoring systems are specialized systems that use extremely high-speed data capture sensors and memory intensive computer analysis and storage devices to monitor and trend power quality at critical points in the electrical supply and distribution systems. Typical measuring locations include incoming utility power feeders, emergency (generator) power feeders, UPS system incoming power feeds, and UPS outputs. Power quality parameters can include phase voltages and amperages, leading/lagging power factors, real and reactive power, etc. The monitoring and trending of these parameters can allow facility operators to identify and troubleshoot serious power related issues such as power surges (spikes), voltage drops (brown-outs), and grounding issues. These electrical issues can be near instantaneous or can occur gradually over time. These power issues can also result in serious impacts to supported equipment such as chillers, pumps, and other equipment with motors, Variable Frequency Drives (VFDs), etc.

Due to the extremely specialized nature of these systems, they are frequently setup as standalone monitoring systems that communicate to the Building Automation and Control System via gateways, SNMP traps, and OPC protocols where centralized viewing and event notification/escalation occurs. Some Power Quality Monitoring systems are web-compatible and can be accesses and viewed via standard internet protocols affording another means to integrate to web-capable Building Automation and Control Systems.

Electrical Power Distribution Monitoring

Electrical distribution system monitoring allows users to check essential power distribution equipment and site status. Some of these systems can also communicate over the Internet with any standard Web browser. Some applications provide the ability of monitoring multiple switchgear and breaker line-ups, emergency generator systems, Automatic Transfer Switches (ATSs), Transient Voltage Suppression Systems (TVSS), Uninterruptible Power Systems (UPSs), Power Distribution Units (PDUs), and even Remote Power Panels (RPPs) provided each component and/or system controller is provided with the necessary communication capabilities. These components and systems frequently communicate over wide-area networks (WANs) using TCP/IP and Simple Network Management Protocol (SNMP) network layers. When parameters exceed user-defined limits, or a dry contact changes states (for example breaker position), alarm notification can be sent out via email, pager, and SNMP traps.

System-to-System Integration via OPC

Many control systems, monitoring systems, and miscellaneous "intelligent" devices (such as leak detection and hydrogen detection systems) provide a means to directly communicate to other standalone or networked monitoring systems. Communication is accomplished through the use of third party communication protocols such as Modbus or Open Process Control (OPC).

OPC is an industry-standard protocol created with the collaboration of a number of leading worldwide automation and hardware/software suppliers in cooperation with Microsoft. The OPC standard offers real plug-and-play software technology for process control and factory automation, and provides seamless, open, and easy enterprise-wide communications.

OPC eliminates the need for the development of numerous custom interfaces (gateway drivers) to access data from multiple vendors' devices, and the driver conflicts that often result among thousands of different types of control devices and software. A controls industry initiative, called oBIX (Open Building Information eXchange), previously know as the CABA XML/Web Services Guidelines Committee, is a technical committee that promotes standard protocols to facilitate open data transmission and communication between otherwise vendor specific applications.

Instant Alarm Forwarding/Notification Software

Simple Network Management Protocol (SNMP) is a widely used protocol by network administrators for receiving alarms and coordinating responses to facility incidents. Using existing Network Management Systems (NMSs), facility personnel can be notified of problems automatically via email, mobile phone or PDA. SNMP "traps" are software mechanisms for passing alert or alarm events from one network to another. Use of SNMP "traps" can allow Building Monitoring Systems (BMS) alarms to be routed to the IT enterprise network where the IT command center (network operations center or NOC) can automatically register and monitor critical alarms. This also enables all facility related alarms to be monitored by the NOC and allows for a consistent and coordinated notification and escalation between both the facilities staff and IT staff.

New BMS controllers are capable of placing alarm data onto the Owner's Network Management Information Base (MIB), where it is then forwarded to network management systems as an SNMP TRAP. Alarms from network switches and routers can be correlated with heat, humidity, or other facility alarms, enabling early problem identification. This provides the dual advantages of being more cost effective as well as eliminating a single point of failure.

SNMP Alarming provides additional flexibility to Owners to define which facility alarms to forward via SNMP. Nuisance alarms can be filtered. Receiving alarms via SNMP also means that other integrated NMS software packages can act on them, such as daily trend report generation. Most new IT equipment has embedded sensors that monitor the inlet air conditions entering the server. ASHRAE technical committee TC9.9 "Mission Critical Facilities, Technology Spaces, and Electronic Equipment" is currently promoting and working with IT manufacturers to develop open protocols that will allow data from temperature, humidity, or other sensors embedded within IT equipment to be shared with the facilities staff using the enterprise LAN and interfaces with the BMS so that they can monitor, trend, and alarm on problems at the server level directly. This may allow facilities staff to receive advance notice of too hot conditions and a quicker reaction time to mitigate and hopefully avoid overheating servers and associated impacts.

Security Access Control/CCTV Surveillance Systems

Advancements in internet browser web applications currently allow many BMS manufacturers to seamlessly integrate to Security and Access Control equipment. Remote retrieval of real-time building security data and reports and alarms can be mapped to BMS workstations. Supportive application software provides system diagnostics for routine maintenance instantly to the operator.

Access to Digital Video Recording (DVR) equipment allows operators to view recorded video. Operators can search events by time, date, location, specific camera, or alarm. In at least one site, whenever a cabinet door is opened, a sensor sends a signal to the site work-flow server checking that an open work ticket exits. If no open ticket is identified, a digital camera

takes a photo of the person accessing the cabinet and a security guard is dispatched with photo in hand to investigate the activity.

Lighting

As a nation, we spend about one-quarter of our electricity budget on lighting. Much of this expense is unnecessary. Technologies developed during the past 10 years can help us cut lighting costs by 30 to 60 percent while enhancing lighting quality and reducing environmental impact.

A greater potential to save on electric energy is realized when automatic lighting controls, automatic shade controls, photocell daylight dimmers near windows to control fluorescent fixtures and occupancy sensors are used in conjunction with an integrated building automation system.

Recent advances in LED lighting holds true promise for the future of commercial lighting and controls. Not only are LED lamps more energy efficient and environmentally sound, but they can be "tunable" so as to vary the lighting spectrum to emulate morning, mid-day, or evening light. When this technology reaches fruition the BMS system may be the natural tool to use for monitoring and managing these functions.

Digital Addressable Lighting Interface (DALI)

Digital Addressable Lighting Interface (DALI) is a bi-directional, digital protocol developed by lighting manufacturers for the control of light source levels. The initial application was for the control of fluorescent lamps, both linear and compact to be followed by the control of additional light sources such as HID, LED, incandescent, etc. Using this new digital standard in lighting control, it is possible to combine easily the installation of existing 1-10v interfaces with

the advances of intelligent lighting control. This system closes the gap between previous 1-10v technology and expensive bus systems. DALI-driven lighting networks can easily be connected to Building Automation Systems.

Ventilation

The first priority of HVAC systems is to provide an environment that promotes comfort and safety within any building type. HVAC systems heat, cool, control humidity and introduce filtered fresh air into the building. HVAC systems waste energy due to thermal losses in ductwork as it travels through ductwork, improper mechanical equipment sizing during design, excessive HVAC demand due to inefficient building envelope or inefficient lighting and office equipment, along with poor control strategies.

Variable Frequency Drives

Manufacturers of Variable Frequency Drives (VFDs) now are capable of providing units with direct communication interfaces such as BACnet, allowing the building automation system to directly communicate and control each drive. Using this strategy more information is available to the user. VFD's have proven to substantially reduce fan and pump energy at part load conditions. Primary/secondary pumping systems and HVAC equipment with variable frequency drives (VFD's) controlled via a building automation system should be considered for use with high efficiency HVAC equipment due to their efficiency at part loads and reduction of initial installation costs by as much as 20%.

Electronic Variable Air Volume Box Controllers

In a Variable Air Volume (VAV) system, a VAV box in the occupied space regulates the amount of supply air delivered to the space, based on the thermal needs of the space. Electronic VAV box controllers provide temperature and air flow information directly to the building automation system, insuring that VAV box minimum supply air ventilation settings are maintained during partial loads. The electronic thermostats that control the associated VAV box also act as temperature sensors that can be monitored by the BMS so that the facilities staff can monitor conditions remotely and to provide alarm notification of out of spec conditions. By use of the BMS, these VAV boxes can be automatically commanded using time-of-day, day-of-week programs to set temperature set points during unoccupied times to reduce energy consumption.

Indoor Air Quality (IAQ)

Indoor Air Quality (IAQ) generally refers to the quality of the air in an indoor living environment. Other terms related to IAQ include Indoor Environmental Quality and "Sick Building Syndrome." Complaints about IAQ range from simple complaints about the air smelling odd to more severe situations, where the air quality causes illness and loss of work time. It is difficult to identify a single reason for IAQ complaints because of the number and variety of possible sources, causes, and varying individual sensitivities.

IAQ problems can be caused by poor or uncontrolled ventilation, overcrowding, cigarette smoke, microbiological contamination, outside air pollutants, and off gassing from materials in the office and mechanical equipment. Improper IAQ may include comfort problems due to improper temperature and relative humidity conditions.

Air Quality Monitoring System

Building owners and/or property managers should consider the use of a permanent air quality monitoring system for controlling indoor air quality (IAQ). ASHRAE acceptable level of carbon dioxide (CO_2) for an indoor office environment is 1000 ppm ("normal" CO_2 outside level is about 300 to 400 ppm). Carbon monoxide (CO) levels in office environments should be below 2 ppm. OSHA regulates levels of CO for industrial locations. Duct mounted and wall-mounted sensors are available to be utilized by building automation systems to ensure proper fresh air ventilation rates are maintained at all times. These systems are also frequently used in parking garages and loading dock areas to activate ventilation systems in response to high CO or CO_2 levels during high use times.

Demand Controlled Ventilation

Use Demand Controlled Ventilation (DCV) controls for data center support areas such as lobbies, waiting areas and conference rooms. DCV saves energy by ensuring that the proper amount of mechanical ventilation is supplied by continuously monitoring space and occupancy conditions by measuring CO_2 concentrations per ANSI/ASHRAE Standard 62.1-2004, "Ventilation for Acceptable Indoor Air Quality." Significant energy can be saved when used in conjunction with typical variable air volume (VAV) designs.

Planning for Disastrous Events

In our Nation, heightened awareness about potential airborne pollutants due to terrorist attacks is becoming part of our everyday life. Mechanical HVAC equipment primary used to ventilate and condition air is now becoming an important part of building-wide security procedures. Engineers must pay close attention by augmenting HVAC designs with automatic exhaust and purge system functions, along with low leakage dampers properly installed at all outdoor air intakes, to minimize opportunities of external potential airborne pollutants entry into any part of the building. One big challenge in this area is that the systems must respond

differently depending upon where the source of contamination occurs. If a contaminate source is external to the facility, the facility HVAVC needs to sense the condition and rapidly shutdown all outside air and exhaust systems. If the source is internal to the facility, the HVAC system needs to sense the condition and respond differently, possibly by either a complete shutdown or perhaps by initiating a "purge" sequence. Regardless, the system will be most effective if the contaminate is detected automatically be sensors that can communicate to and control the HVAC system response without needing staff intervention.

Automatic Ventilation System Shutdown

A potentially useful capability is to integrate security functions with the building automation system, by providing for automatic shutdown of ventilation systems due to the detection of chemical, biological, and radiological pollutants or agents detected outside the building. This strategy requires direct two-way communications with each dedicated security-related monitoring system. Redundant fan and damper control functions via a dedicated automation system workstation should be located within the building's security office. The system should be powered by emergency power.

Reducing Communication Cabling Costs

Many buildings that are supported by a building automation system, security system, lighting system, elevator monitoring system, etc. use its own separate communication cabling. These buildings must therefore be designed to support multiple pathways, communications closets and equipment rooms. Each system is installed and commissioned by multiple contractors, ensuring that the initial costs for these required building systems remain high. As an alternative, some buildings have combined the traditional IT cable network to support both the IT "enterprise" and the facilities BMS network via a virtual private network (VPN) solution.

Utilize a Structured Cable Plant

New building automation system design trends include the ability to communicate on a common communication infrastructure or "structured cable plant". An engineered structured cable plant allows several building systems to share one IT infrastructure such as security, lighting control and building automation. Each system communicates in a secure, independent manner. This strategy takes advantage of the fact that data communications for many systems shared the same communication protocol such as the PC industry standard of Ethernet TCP/IP (IEEE standard 802.3). New direct digital control panels (DDCPs) that reside on local area networks (LANs) can also connect to the Internet using static IP addresses. As more and more data center systems are designed to integrate with each other, less cabling will be required, reducing initial installation costs and yearly maintenance.

Measuring Building-Wide Energy Efficiencies

Measurement of building-wide utilities is becoming an accepted part of facility operations due to such standards like the U.S. Green Building Council's Leadership in Energy and Environmental Design (LEED) rating system. In order to achieve a LEED rating, utility measurement for energy efficiency is required. For critical facilities, the Green Grid in collaboration with the US Department of Energy is promoting datacenter efficiency metrics including Power Usage Efficiency (PUE) and Data Center Efficiency (DCE) measurements. The electrical distribution monitoring system is the best candidate for automating the required metering and can produce simple reports that can track and trend these values.

Utility Measurement

New electronic meters are now available in the marketplace which allows for the measurement of electricity, natural gas and steam. Some meters are capable of connecting to existing local area communication networks or directly to the internet. Many meters support TCP/IP, Modbus and Extensible Markup Language (XML) protocols. New meters can be assigned a static IP address or can receive one by a Dynamic Host Configuration Protocol (DHCP) request.

Many of these energy-efficiency automation measures and strategies can be used in combination. One thing is clear, a knowledgeable engineering firm with an understanding of the needs and expertise in the design of critical facilities should be engaged to consult on and develop the design. The firm must have design professionals who are LEED certified and who are experienced in promoting Green solutions in every design. The firm must also have a dedicated commissioning group. It is essential to develop a comprehensive commissioning plan that will test all air and water related mechanical systems and their related controls under all aspects of operation, so that facility energy waste can be revealed and reduced. The commissioning process ensures that everything will work as intended; ensuring optimal performance levels for each new control strategy is achieved while protecting our resources for future generations.

……