IP Based Control for Mechanical and Electrical Systems in an Enterprise Environment

Joe Noworatzky
Vice President, Engineering
Johnson Controls, Inc.
Introduction

Facility managers of the future will be astonished when they discover that building systems were not always seamlessly integrated into a single enterprise-wide information technology network.

“You mean, thermostats, fire panels, badge readers and other devices ran on separate communication networks inside the same building?” they’ll ask. “That’s crazy! The facility and IT departments must have constantly butted heads. Imagine all the unnecessary costs to keep them operating independently.”

Yes, the “old days” of operating a building will be compared to using cassette tapes for music storage instead of MP3 files, or writing letters instead of text messaging. This future scenario is a lot closer than it seems.

Forward-thinking individuals and companies throughout the building industry view the information technology network as just another utility, where plugging building control devices into the network is like plugging a toaster into an electrical outlet. As long as you don’t ask the utility company for more power than it can provide, no one cares if it’s a toaster or a vacuum cleaner. Similarly, there should be no fundamental difference between using the IT network architecture to cool a building or allowing a smart phone to download files from a wireless network.

Which brings us to the topic of this white paper: IP based control for Mechanical and Electrical Systems in an Enterprise Environment. IP, of course, stands for Internet Protocol. An IP address or set of addresses (along with the supporting IT infrastructure) is the “utility” that should not ask questions of its users – as long as they are properly installed and follow the network’s rules. Mechanical and electrical systems still need their own controls hardware and software in order to automate wide-ranging functions at the field device level throughout a facility. But now, facility managers have one less chore because the IT staff maintains the digital lifeblood. It’s like owning a condo instead of a house.

Over the past few years, there has been a convergence of building management and information technology systems. These two formerly disparate systems, to some extent, have been able to share architecture as well as information. To cite just one example, real-time energy consumption data is now widely available to management outside of the facility department. Building-related data – including energy, security and life safety system information – is easily accessible through a standard Web browser instead of being trapped in the building management system’s workstation.

Convergence of building management and information technology systems is a very good start, but it still lacks the seamless utility concept described earlier. That’s because building management systems have not taken full advantage of the IT network.

This is about to change. A movement in this direction is beginning to take shape within the building industry. It’s called Buildings 2.0. The name represents a drastic departure from the past and builds on the concept of Web 2.0, the second generation of service and utility available on the World Wide Web. Although we continue to make steady progress with integration and interoperability, our systems are still in a Buildings 1.0 environment. We need a leap to get to 2.0 – and IP based control is the starship.

What is IP Based Control?

Controllers That Thrive on the IP Network

With Internet Protocol as the backbone of an enterprise-wide network, everything that requires a standalone network today simply becomes subsumed into the IP master. This is interoperability at the very highest level. In the building management sector of this new environment, controllers are designed for the IP network. More importantly, they are also designed to thrive on the IP network.

Think of today’s building management system as an engine that runs on IP power. This engine, in turn, fuels all of the controllers that link to it (wired or wireless). These controllers provide comfort, security, life safety and other necessities of a desirable work environment.

The high-level engine, which we will call a Network Control Engine (NCE), combines the building management system’s network supervisory capabilities and IP Ethernet connectivity with field equipment control that does all the work.
Devices That are Self-sufficient

In the IT world, most devices connected to the IP network are self-sufficient – they use the IP network, but are not totally dependent on it. The same is true of building management devices on the network. They must have the power to freely exchange information with the rest of the network but must not depend on it to perform critical functions.

Ideally, IP based control systems are embedded with power backup capabilities that, in the event of a power failure, enable them to back up their memory as well as operate field devices. During a power loss, they can continue operations to shut down logically and can tell other devices about the problem. Problems are reported using the existing IT infrastructure – connecting to pagers, printers, e-mail, or network management systems.

Much of this functionality is possible because IP based control devices are compatible with IT-standards like Simple Network Management Protocol (SNMP). This compatibility also allows the IT department to use its network management software to check the status and operation of all network connected equipment. Therefore, IP based controllers can report alarms or warnings based upon memory usage, processor temperature, or other critical operating attributes of the hardware or software.

The IP based controllers should also adhere to the IT-standard Simple Network Time Protocol (SNTP). This provides the standard method of synchronizing time between a designated time server and all of the building management system devices as well as harmonization of this function with enterprise applications.

An ideal Network Control Engine environment, as depicted in Figure 1, offers several advantages over today’s status quo:

- The NCE uses commonly accepted IT standards at the automation and enterprise level. This allows you to install it on the existing IT infrastructure within a building or enterprise – and use standard IT communication services over an Intranet, Wide Area Network (WAN), or public Internet.
- A Web-based interface allows you to access, monitor and control the NCE from a supported Web browser connected to the network it resides on, including secure access via a Virtual Private Network (VPN).
- The user interface and online system configuration software embedded in the NCE allows configuration, commissioning, data archiving, monitoring, commanding and system diagnostics from any device with Web browser software – and does not require separate workstation software.
- Open protocols for field controllers support connectivity to open network standards, providing flexibility in selecting field devices.
- Integral control capabilities provide field-level control of central plant and large air-handler applications, combined with enterprise-level IP network connectivity.
- Expandable I/O point capacity allows you to connect multiple I/O modules to the field controller, which greatly expands field-level control capabilities.

Figure 1
IP Based Network Control
Because IP based controllers are fully compatible with the IT network that is already in place, the building management system can rely on the IT network for safe and reliable transportation of information. This, in turn, allows the IT staff to provide critical planning and maintenance services to make sure the controllers remain healthy. This is like a condo owner playing golf while a team of professionals make sure the complex is comfortable, safe and well maintained.

What IP Based Control is Not

IP based control does not tie you to an individual supplier. Because IP systems by their very nature are open, devices tied to the IP network are capable of being interoperable with other IP-connected devices. While differences in configuration tools and minor variances in the way certain functions are implemented may still require some engineering, this is a lot closer to our goal of a common building system “utility.”

IP based control does not require the elimination of existing controls throughout a building or campus. A good IP based system can talk to backward compatible, or previous-generation, equipment – whether they use BACnet, LonTalk or any other protocol. This preserves the investment in controls hardware, which can be significant depending on the size and complexity of a facility.

Done correctly, IP based control can be evolutionary as opposed to revolutionary. A total changeout of equipment is not necessary to enjoy the fruits of IP based control.

Desirable Benefits of IP Based Control

An investment in IP based control should be rewarded with leading-edge features and capabilities, including:

- Advanced control opportunities
- Superior failure mode ability
- Cost optimization

Advanced Control Opportunities

IP based controllers should be self-tuning. They must possess the intelligence to understand where they are, and to respond to other systems and equipment that request information from them. An IP based controller must be able to query the lower-level devices attached to it, obtain information from them, and configure its own database as required.

Going a step further, building owners should insist on adaptive control – also known as continuous tuning and commissioning – in which devices adjust themselves, with no human interaction necessary. In an adaptive control world, building systems are always correctly tuned to their operating environment, which increases accuracy, extends equipment life, and saves energy.

An IP based controller, through its powerful software capabilities, should be able to accomplish the following tasks with ease...

User Interface

Provide formatted data and graphic screens to any connected Web browser. Authorized users simply log on to the NCE from the Web browser to access the user interface.

System Security

The NCE must recognize legitimate users through the entry of a user ID and password, which the security administrator assigns. The administrator also manages user profiles and accounts at a site or system level. IP integration allows the device to leverage the existing corporate IT directory services for authentication.

Monitoring and Control

The software should be able to efficiently monitor and control all mechanical and electrical systems in a typical building, including HVAC units, the central plant, power generating and energy monitoring equipment, and interfaces to security and fire detection systems. The NCE should be able to monitor equipment by collecting data from field control devices, coordinating the required commands, then routing the commands back to the field equipment.

Transaction Recording

All user actions performed through the NCE should be recorded in a trail log, including logon and logoff, commands to equipment, changes to parameters, and changes to the system configuration.

Alarm and Event Processing

When a value exceeds a defined limit or changes to an off-normal state, the NCE should be able to send alarm or event messages to online Web browsers, pagers, e-mail servers and serial printers. The alarm and event information may include a predefined message to facilitate a fast response to the system problem.

Historical Trend Data

The NCE must support trending of any monitored value at user-defined periods or based on change-of-value sampling. Trend log information can be transferred to an historical database to help analyze the performance of building control systems and locate the source of system problems.

Totalization Data

Analog and pulse totalization features in the NCE should be able to monitor the use of energy and other consumables. Reports can then be generated for cost allocation within a facility, or to support energy and cost reduction programs.
Scheduling
This feature should allow building occupancy periods to be defined, as well as the start and stop times for mechanical and electrical equipment. This means that operating parameters such as temperature setpoints and power consumption limits will be tied to time of day and calendar programming.

Network-Wide System Interaction
Advanced software should allow the NCE to take information from one or more field controllers, make logical comparisons, and issue a set of control instructions to other field controllers anywhere on the network. For example, network-wide system interaction allows all field controllers on a site network to use the input from a single outside air temperature sensor, eliminating the need to wire outside air temperature sensors to each controller.

Superior Failure Mode Ability
Most non-IP based devices rely on another layer of interpretation and integration to transport information to the rest of the enterprise network. They also rely on supervisory controllers or servers for necessary control level applications. This is not the case with IP based controllers.

With its built-in scheduling, trending and other system-level capabilities, the controller does not have to go elsewhere for this data. If communication to the enterprise network is lost, the controller operates as a true standalone device, adapting to the new environment. When the connection is resumed, there is less chance of losing data.

Cost Optimization
IP based controllers are able to use multiple protocols – such as BACnet, LonTalk, N2 – to connect to other devices at the field bus level or at the enterprise level. This interoperability preserves the investment that has been made in the control system. Expenses are further reduced because no middleware or gateways are required to communicate across the network.

The convergence of the building management system and the IT network, via IP based control, has cost advantages in terms of installation and maintenance. A single cabling infrastructure is obviously easier and cheaper to install than multiple proprietary networks for different building-related functions. Returning to the electric utility analogy referenced earlier, consider how expensive it would be to install separate wiring systems for a toaster, a vacuum cleaner and every other machine that needs electricity. Service costs also would be higher to maintain these different wiring systems.

It is a well-established fact that over 75 percent of a building’s total lifecycle costs are consumed after design and installation – in the “maintain and operate” phase. Therefore, it is prudent to make decisions in the installation period that will impact costs for decades to come. IP based control, using the existing IT infrastructure, is definitely a prudent bottom-line decision.

A final point to make under economics is the cost of security. Each organization has a different way to measure its security needs, as well as the level of physical and network security it can afford. IP based control creates the best opportunity and balance to ensure both a secure and accessible environment. Security cost decisions should be made by the facilities department as well as the IT department.

IP Control and the Future
IP networks are the most common element linking intelligent devices today, and they will only become more prevalent within buildings of all types. IP enabled devices can take advantage of the intelligence embedded in other IP enabled devices, thereby adding value to all of them.

Look at what is happening in the telephone industry. Telephones no longer require physical wires running from a central office to your home or business, they have become mobile devices. And, with the addition of an IP address, voice-mail and other features can be retrieved via computer as well as through the phone itself. This trend will expand exponentially as the pool of IP enabled equipment mushrooms in the years ahead. We can only guess what advantages this will bring to consumers and businesses.

IP based control is equally comfortable in a wired or wireless environment. However, wireless is clearly the wave of the future, so this should be carefully considered when moving to IP based control.

Whether wired or wireless, IP based control is an expressway to expanded enterprise applications. We have begun to see this with Web Services, where a device’s data is served to other devices that order the data. Of course, the device must ride on the common IT network to be available to one and all. IP based control is ideally suited for supporting Web Services-based communications where the information might be used in software applications designed to improve an organization’s productivity and efficiency.

The future is full of opportunities to use IP based control and leverage the benefits that have been outlined in this paper. In doing so, you will have laid the foundation for efficient and interoperable systems for decades to come.