GREAT WALLS and Small Gates

IT and FM Communities Have To Open Small Gates In Their Respective Walls To Accommodate Overlapping Territory.

By Andy McMillan
President & CEO,
Teletrol Systems Inc.
as Published By
Technology Century (The Engineering Society of Detroit)

China's Great Wall was constructed to secure the country's territory from those "outside" who might inadvertently or deliberately invade it. A large number of people worked over a long period of time to make the Great Wall the awesome structure we see today. In much the same way, IT professionals and Building Automation Systems (BAS) professionals have constructed elaborate "walls" around their systems to deter inadvertent or deliberate trespassing. However, the growing need for effective energy management solutions coupled with the growing ubiquity of web technology is creating a situation where both the IT and BAS communities have to open small gates in their respective walls to accommodate overlapping territory.

IT systems in most organizations have become mind-numbingly complex. They consist of a wide array of distributed devices performing a range of functions. Some devices perform functions of direct value to the organization, such as data servers and office PCs. Others serve no direct function but exist merely as essential elements of the infrastructure, such as network routers and switches. Throughout the system data flows in endless intertwined streams under the tacit direction of layered routing algorithms. The sheer complexity of these systems and the multi-path data flows they encompass makes it very difficult to fully assess the impact of adding unfamiliar components or transaction types to a system.

Virtually all IT groups maintain infrastructure elements that support mission-critical business applications. Through the hard teacher called "experience," IT professionals have learned that accidents, mistakes, carelessness and malicious behavior can all result in costly system downtime or data loss. As a result, over the years IT professionals have learned they need to secure their IT infrastructure at multiple levels.

Sophisticated network management tools have evolved to help IT professionals deal with security and the complexity of the systems they maintain. Even so, complete analysis or precise modeling of real-world systems is beyond the reach of most IT groups. As a result, they must rely on generally accepted "best practices." Following best practices eliminates the need for detailed analysis in many situations and minimizes the risk in many others.

While the IT world has gone about its business of developing, deploying and securing its systems, BAS professionals have been involved in a similar, parallel endeavor for building automation systems. Modern building automation systems are complex, distributed systems that control heating, cooling, lighting, security and other building systems. They perform real time control, data collection and data processing functions. Real time control functions include discrete activ-

ities, such as unlocking a door when an appropriate code is entered, and continuous activities such as adjusting air vent dampers to maintain specified room temperatures. Data collection and processing functions are diverse, ranging from maintaining a rolling 30-day building temperature profile to generating monthly reports on energy utilization. Like IT systems, building automation systems are mission critical and must be secured against both inadvertent and deliberate tampering.

The BAS industry has evolved its own set of standards and best practices over the years for much the same reasons the IT industry developed them. However, the standards and practices developed for building automation systems are generally different from those developed for IT systems. This dichotomy came about for several reasons, including:

- the requirements of the two domains are somewhat different;
- the characteristics of computing devices used in the two domains are different;
- different people in user organizations are typically involved in the two areas;
- different suppliers serve the two markets;
- different industry organizations serve the two communities.

Parallel standards and practices have not been a problem historically because the systems were installed separately and the areas of overlap were small enough that the cost of duplication was insignificant in relation to the total cost. However, the advent of web technology and recent trends in building automation are increasing the areas of overlap and motivating more integration between the two domains. As a result, differences in standards and practices are becoming a bigger issue in many organizations.

One of the most important issues facing BAS professionals today is energy management. With the rising cost of energy and the increasing volatility of energy prices, real time monitoring and control of energy usage on an enterprise level offers the potential for considerable savings. As a result, there is an increasing emphasis in the building automation arena on data aggregation across geographically distributed sites. Since duplication of IT wide-area data communications is not practical, there is a growing demand for BAS interfaces to the enterprise network infrastructure.

In addition to energy management, there are a number of other business requirements driving the need for interfaces between BAS systems and IT systems. One is improved maintenance dispatching. Another is the need to integrate access control, environmental control and lighting control into comprehensive building security solutions. Still another is the facilitation of building management outsourcing. In all these cases, actually implementing system interface strategies that simultaneously accommodate the standards and best practices of both IT and BAS requires the involvement of both in the BAS acquisition decision process.

The building automation industry has incorporated commercial technology borrowed from the IT community. Such technologies include Ethernet, TCP/IP, Web servers, Intranets, XML and PC workstations, among others. Many suppliers, though, have adopted technologies without regard for the "best practices" that make those technologies effective in IT environments. For example, some suppliers have developed building automation systems with Web-based interfaces that require the use of a custom Web server or special firewall ports rather than using a standard server like Apache or IIS. Other suppliers provide products where the communications between the building automation system and desktop PCs utilize communication protocols like BACnet and LONworks which are unknown in the IT world. Integrating these systems with a company's IT infrastructure can seem risky because they violate some of the most basic IT "best practices. "

Most IT professionals recognize the introduction of non-standard forms of communication over the IT infrastructure creates operational and maintenance risks. Given the potentially high cost of system failures, IT professionals are rightly risk-averse and therefore strongly resist any effort to introduce such non-standard solutions. So, how can an organization bring about the necessary integration of these systems?

The simplest approach (from a technical point of view) is to select building automation products that are designed to be "IT-friendly" in the first place. IT-friendly BAS products are designed to utilize the IT infrastructure with minimal variance

from IT standards and best practices. These products limit the use of BAS-specific communications protocols to interactions among BAS controllers. For communications between BAS devices and IT servers/workstations they utilize XML over HTTP. As a result, these systems are compatible with standard firewall configurations and network operation norms. Even with the most IT-friendly BAS solutions, though, may still have some special requirements. For example, one of the most common special requirements is a need for BAS controllers to have dedicated IP addresses. Over all, achieving the necessary level of IT and BAS system integration in these circumstances largely comes down to careful planning and reasonable accommodation.

As the BAS industry continues to evolve, more and more suppliers will migrate to solutions that are IT friendly. For now though, it is not always be practical to drive BAS purchasing decisions from the perspective of IT integration effort. Legacy systems compatibility, cost constraints, functionality requirements and many other things may lead to the adoption of a BAS that is distinctly "unfriendly" in the context of standard IT environments. In these circumstances, achieving cost-effective integration at an acceptable level of risk may not be easy. One approach adopted by some users is to install a parallel Ethernet infrastructure for the BAS system. A single point of interconnection between the two systems is provided through a carefully managed router or application gateway. In other cases, the BAS system utilizes the enterprise infrastructure, but is isolated a separate segment via intelligent switches or is contained within a Virtual Local Area Network (VLAN).

The use of the enterprise network backbone for BAS system communication and IT integration offers substantial operational and cost benefits to facility managers. One of the biggest benefits is the fact that the enterprise network is designed and maintained by the IT group so the facility manager does not need to deal with it. Another benefit is ability to house a BAS data server in the IT group, thus taking advantage of the IT group's expertise in server administration, backup and support. However, use of the enterprise backbone also creates some issues for the facility manager that have to be addressed.

One issue that comes up when a BAS utilizes the enterprise network is denial of service events. IT professionals strive to protect their enterprise networks from the impact of viruses and worms. In reality, though, complete protection still eludes most organizations. As a result, facility managers using the enterprise network for BAS connections must design their systems to operate safely even when backbone connections are lost. Another issue in using the enterprise network is the need for continuous coordination between facility management and the IT group. Failure to maintain coordination can lead to unacceptable BAS system interruptions. For example, IT network reconfigurations that are transparent to typical computing devices (such as PCs and printers) can easily impact BAS devices, especially if they use fixed IP addressing.

For many organizations there is a growing business benefit in effectively linking BAS with IT systems. The technologies employed in the two domains are converging and over the next 3-5 years seamless integration may come about through industry acceptance of a web services solution. In the meantime, however, there are several approaches to achieving some level of integration while maintaining appropriate security for each system. IT-friendly products, isolation of BAS within the IT infrastructure and parallel infrastructures have all been successfully employed. To make any solution effective though, requires a good working relationship between the facility management team and the IT team. Where the two are successful at working together the IT and the building automation systems are both properly secured, yet usefully interconnected. Somewhat like having two Great Walls that intersect at a pair of small, matching gates. ❖

For more information, contact Andy McMillan, President & CEO, Teletrol Systems Inc. at 603-645-6061, or email him at *andym@teletrol.com*