

Managing Building Automation – are you ready?

Quick - how many networks run through your building?

If you said one, you're wrong. For many IT professionals a physical network means TCP/IP over Ethernet and Cat5 cable. But what controls your heating, lighting, air conditioning, elevators, public address, intercom, telephone, fire detection, intrusion detection, CCTV and access control? In most buildings these systems are separately connected with their own wiring schemes and protocols. Visit the service room or look in the ceiling void and you'll probably find a real rat's nest of cables snaking everywhere with little indication of function. At the last count there were over a dozen incompatible protocols for building automation systems (BAS) to choose from: not to mention the proprietary offerings of larger companies. Each one of them demands it's own network. You've probably got a handful of mutually incompatible control networks in your building right now; all put in at different times by different companies.

Does this matter?

Not if life were still as simple as in the 80's when many of these systems first appeared. But today, companies must continuously try to cut costs and improve performance. Do you really need to heat your office if you are away at a conference? Sadly the heating system is too dumb to know how to ask your diary, so it makes it cosy anyway. Can a colleague from another division gain immediate entrance for today's meeting with his own access badge? Nope – those wretched incompatible protocols again! However, stuff can leave all too easily. You can protect data with software, but a sneak thief can still take a manager's laptop in a trice. Surely there is a way for it to signal that it is leaving without its owner? Growing concerns about security will demand greater integration of systems to plug potential gaps.

Management has come to expect IT to solve many corporate problems and these are no different. So what has IT got to offer building automation? As it happens, a lot. In fact the hardware, software and management expertise of IT is ideally suited to tackle building automation.

In 1990, an Ethernet interface card for a PC cost around £200 (\$310) from a specialist supplier. Today you can buy one in the high street for £10 (\$15.50). The costs of connectivity have plummeted. Many building automation systems were designed when 9600 baud was considered fast and 8 bit microprocessors cost more than today's Pentiums. So the logic of using bespoke signalling systems has vanished. Most buildings are now wired with Cat5 cable, often connected to hubs or routers located at each floor. Because the company's operational data courses through this system, it is usually robust and better maintained and protected than the myriad BAS networks.

So controlling BAS via the IT network is no longer expensive or difficult. Other than digitised CCTV, the generated traffic from BAS is minimal. To avoid collisions with operational traffic, a second Cat5 cable costs less to install than a bundle of different buses. This often makes sense if the company also wants to put in VoIP on a separate network. The voice channels can be given the QoS priority with the BAS signals having a lower importance. Who cares if a command to turn on the heating is a couple of milliseconds late? But if BAS goes on a data network, who is going to run it? IT is really the only candidate.

The emergence of IT management has happened in a generation. We've come from mainframes in special air-conditioned rooms, serviced by white-coated technicians to commodity PC's and client/server. Tomorrow promises web-services and networked devices. The narrow world of batch processes for accounts and payroll has given way to technologies like ERP and CRM that put IT at the core of operations. Today's IT manager is no longer a geek but a potential candidate for CEO. He (or she) probably knows more about how the company really runs than anyone else. He has handled the budgets and managed the people.

His experience in integrating and managing heterogeneous systems means he is ideally suited to weld together the different needs of the facilities and security management. Companies in the US are beginning to put all these functions directly under IT.

If you accept the responsibility for building automation, what can you expect?

Your first impression will be of travelling back in time. Unless you have a new building to control, there will be the nightmare of legacy systems, usually from many different suppliers. Up until now integration was usually a sort of 'band-aid' approach involving relays, bespoke device drivers and a PC based control package to bind it all together. Because each system is different, maintenance and upgrades can be a costly nightmare. Your own staff probably won't have the expertise or the interest to maintain it. So you are possibly faced with training the security manager. Bear in mind that this person is probably an ex-policeman, whose knowledge and love of computers is barely measurable.

But don't give up, because software and technology from IT will make your life easier soon. As we saw, making BAS network-ready is now cheap and increasing numbers of manufacturers include Ethernet ports in their systems. That only leaves the software interfacing. Here too help is on the way in the shape of XML. Many of the protocol groups are working on XML versions of their command and data sets. Industry initiatives such as UPnP, which is based on TCP/IP and XML, will allow much easier integration and control of systems. As a bonus, they will also become more flexible to cope with the frequent company restructuring, remodelling and relocation that is such a part of corporate life.

New systems based on XML standards will be easier to specify, install and integrate. But what to do about legacy systems that work perfectly but don't understand TCP/IP and XML? Just as with your legacy operational software, there will be hardware and software 'wrappers' which allow the old systems to continue giving service but will leverage the existing investment by offering an open interface for signalling, configuration and control. Software, based on XML messaging, to control these systems is beginning to become available. In turn the newly bundled building systems can then offer their services to the rest of the corporation as a web service. True integration of operations is then possible. Web services are the key.

The web services revolution is in its infancy. Currently the greatest application of the technology is behind the firewall. But the economic model is too powerful to resist and full-blown web services will eventually be the preferred way of doing business between corporations and their associates, partners and customers. IT is the natural choice to manage the deployment of web services. Because they will use the same, XML-based technology, building services will naturally fit with IT. In fact, as the technology gets more reliable and invisible, IT departments themselves will morph into 'Corporate Services' sourcing and providing information, expertise, and management tools (e-Learning, e-Commerce, e-Operations, e-HR etc). Building automation will just be a part of a much wider spectrum.

So don't look at the management of building automation as a chore but an opportunity. Use the experience and knowledge you've built in IT to tame the beast. Progressively apply the new standards to the systems and bind them into the company's operations. You'll have plenty more challenges like this and the experience will be very useful on the way up the corporate ladder.