

## **A Common Security System Protocol - It isn't over 'til the Fat Lady sings.**

There's a war going on and you're the next target. After years on the sidelines, the control of security systems is desirable territory.

### **Security – a forgotten industry?**

Security has historically been a Cinderella. In most companies it is not part of the day-to-day operations of the firm. Most senior company executives can go for months or years without thinking about security in the workplace. Indeed with the rise of Internet hackers, security is often more about the company's web site or network. It's little wonder decisions on security tend to be delegated to a security or facilities manager with firm instructions to 'keep the costs down'. It is rare that a security system adds directly to the bottom line.

Most security installations are stand-alone and follow the history of the building. Fire systems are usually mandatory so they will be installed from the outset. The first burglary will prompt an intrusion system. Repeated daytime theft of office machinery and PCs will mandate an access control system and increasingly, risks to employees will demand CCTV to record events to ascertain or refute employer's liability. Systems are often sourced from a variety of manufacturers and installers as very few supplying companies do everything. Security buyers are faced with a myriad of products mostly incompatible. Even specifying systems carefully can just produce a 'least worst' solution. Because each system uses proprietary protocols, the buyer is then 'locked in' to the supplier for upgrades and extensions.

### **Building Economics and Commercial Trends**

The way we use buildings is changing. Previously, a company would decide on a site for its operations, purchase the land and commission a purpose-built building. Now offices are built speculatively with only the final fitting out to suit the client. An extension of this comes with 'hot-desking' in financial and consulting firms where executives have no permanent office but use available space at whichever branch office they find themselves. As a result, the total space required can be reduced by up to 30%. Even without going to these extremes, companies need to reconfigure space more frequently. Buildings are often now supplied with moveable walls to create and subdivide offices within hours. How does this match with security systems which can take weeks to relocate, rewire and reconfigure? How many man-hours does it take to reprogram the control software to describe a new layout and match access control badges to new readers and controllers?

Recent studies show that the initial construction cost of a building could be as little as 30% of the total cost over its first 15 years. The remaining 70% of costs come from all the services the building consumes: heating, lighting, maintenance etc. With offices contributing to over 10% of total operating costs of many companies, there are many incentives to look at economies. If an office is empty and won't be used today, why heat it? Can the security system tell the HVAC system to do this without human intervention?

### **Building Automation (BA) and the Protocol Wars**

In BA the situation is a little more advanced than with security systems. However as a result the BA industry has been wracked by the 'protocol wars'. Over a dozen incompatible protocols, often on different buses, have all been developed over the last 20 years. Bigger companies have often tried to impose their own protocols to lock the customer in. Passions run very high but three contenders have emerged from the pack. From the US come BACnet and Lonworks while Europe had produced EIB/Konnex.

Many believe that we are on the last lap of this three horse race. Each camp is looking for allies and converts. Historically HVAC and other building services such as elevators and intercom have had little in common with electronic security. Anyone who has had to build and operate a central control room

for these services will attest to the problems arising from integrating and supervising them. Each protocol champion will claim that the adoption of his technology will simplify the task enormously without the expense of gateways or protocol converters. But if you choose a BACnet based bus, what happens if your preferred access control supplier uses EIB/Konnex? As one wag said, 'The nice thing about standards is that there are so many to choose from'.

The definition of BACnet protocols by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) took a glacial 8 years but has accelerated recently. Having defined the technology for HVAC, their sites are firmly set on security. There will be increasing pressure on security manufacturers to make their products conform to

BACnet. But it's not a foregone conclusion that it will prevail; Lonworks and EIB/Konnex also want your vote. But developments in other areas may mean that none of them prevail. Let's take a look.

### **Extensible Mark-up Language (XML)**

Internet Browsers use HTML to allow software to talk to people. XML allows software to talk to other pieces of software. Just as the PC and Windows imposed a standard on which all software will run, XML will impose a standard for all software to talk. As a bonus it's readable by humans as well. The major advantage of XML is the fact, unlike most fixed protocols, it is extensible backwards and forwards. Earlier versions are not superseded by later ones, they are simply added to. You can be sure that anything bought with today's XML-based protocol will work with whatever comes out tomorrow without expensive upgrades or retrofits.

### **Industrial Automation (IA) Protocols**

In IA the choice is between OPC (OLE for Process Control, a Microsoft sponsored initiative) and supplier-specific protocols, including Lonworks. Arguably IA needs tighter integration and more real time control than BA as manufacturing glitches impact the bottom line faster. So the buyer tends to be more involved with the details of the specification - his job may depend on it! In line with Microsoft's commitment to XML there is a new specification to take advantage of the technology: OPC-XML

### **UPnP**

As always, Microsoft has a long-term strategy in all its target markets. Home Automation is one of them. UPnP (Universal Plug 'n Play) is the technical part of that strategy. Based on XML, it has attracted the interest of hundreds of manufacturers from widely different fields concerned with the home: video, audio, power, HVAC and, of course, security. Ideally you will be able to buy your UPnP device, bring it home and have it introduce itself to your home network and begin to interoperate with almost no help from yourself. Initial tests of this concept at 'Plug Fests' are very promising. The technology is not limited to the home and can easily be adapted to commercial situations. Putting it onto wireless networks (assuming the security concerns can be addressed) should be a snap.

### **Web Services**

Web Services are the new kid on the block. Using XML, the objective is nothing less than allowing any piece of software to be able to call for help from any other, irrespective of its language, operating system or hardware platform. It would be easy to dismiss Web Services as just the latest fad but they deserve to be examined more seriously. With massive backing from all the major players in the IT industry, Web Services are not going away. Indeed, with .NET, Microsoft have based their entire strategy around the technology, already spending more in R&D than the yearly turnover of the entire security industry!

### **Support technologies**

The infrastructure (processors, memory, fixed and wireless network bandwidth) for integrated systems is getting better, faster and cheaper. Even software, notoriously expensive to develop, is coming under control. Object-orientation has not delivered huge savings but it has made software easier to maintain and adapt. New development tools, based around Java, .NET and XML promise to improve programmer efficiency. What were previously impossible or unaffordable functions will be built right into systems at little extra cost. Consequently, connectivity will not be constrained by price.

### **The Fat Lady**

Now it won't have escaped your attention that a common thread runs through much of all this: Microsoft. The use of computers in security systems is not new. What is new is that the security industry is no longer a Cinderella. Worth over \$9 billion in annual sales and growing faster than the general economy it is increasingly centre-stage thanks to publicity around September 11 and Internet hacking. Does Microsoft want a piece of the pie? You bet!

### **A Fatter Lady?**

So will it all go Microsoft's way? Not if the US-based Security Industry Association has its way. In June 2002, SIA organised a three-day Government and Technology summit conference in Washington which culminated in meetings with US Congressmen to discuss how the industry should work with Government and particularly a new giant organisation, the Department of Homeland Security (DHS). One of the clear messages was the need for a unified Communication, Command and Signalling protocol to sweep away the myriad proprietary offerings of the industry. To this end SIA has begun a new initiative, the Open Systems Interoperability and Performance Standards (OSIPS).

In the 70's the US Department of Defence knocked the IT industry's heads together to produce TCP/IP to create the

Internet. Now SIA is apparently pre-empting the DHS to do the same thing for security. Hopefully this can happen quickly, without reactionary forces in the industry fighting rearguard actions to protect their favourite protocol.

### **Standards grow Industries**

VHS, CD, DVD and TCP/IP are all examples of how a standard is an enabler of rapid industry growth combined with continual cost reduction. At present, integrating security systems is project driven, needing a lot of engineer time to write protocol converters and weld together systems that were never designed to work together. Subsequent maintenance and upgrades can be a nightmare. Both security manufacturers and buyers have an interest in formulating a common standard protocol.

With a standard protocol, specifiers can truly work on an 'open playing field'. Buyers will then be free to mandate 'best of breed' for each system element as they can in other fields such as IT hardware.

What is increasingly clear is that this protocol will use Internet technology and XML. Both BA and IA are developing their protocols towards XML. This means that we are within sight of a common protocol to control residential, commercial and industrial environments. Initiatives such as [www.securityxml.org](http://www.securityxml.org) are springing up to collect input from professionals in the industry.

Watch this area, things are beginning to move quickly! Better still, get involved; the industry needs input from all areas to ensure the right outcome.

Whatever happens buying security is going to get a lot more interesting.

© Peter Manolescue August 2002