



Manufacturers, vendors and end users have set up the LonMark Interoperability Association to administer the program. LonWorks is particularly strong in Europe and Asia, and its popularity in the United States is growing rapidly.

In an article entitled "Understanding Open Protocols" in Building Operating Management in August 2001, author James Piper recommends a four-step approach to the selection of the correct protocol. The savvy security manager should heed his advice.

Security systems manufacturers did not follow the BAS/HVAC community in their pursuit of open protocols, instead hiding under the cloak of the "UL standards prevent us from doing so" mantra. In reality, they were afraid of losing their client base and considered this to be a sensible strategy to keep control of their customers.

BACnet and LonWorks have not succeeded to any great extent in integrating with security. BACnet is making some progress appearing as an interface on some fire alarm panels and other alarm panels, but very little else.

IT's Influence on Security Protocols

The convergence of IT and physical security is adding a new emphasis to the area of open systems protocol, in that the more the security department uses the existing network (controlled and funded by IT), the more dependent security will become on the IT system. IT departments generally prefer working with open systems, which allow them easy access to the information they need to do their job effectively. Remote locations can now more easily connect to the network, but the connection is controlled by the IT department, which sets the rules, regulations and standards.

IT departments also generally prefer working with hardware and software that they understand and that can be supported within the existing communications infrastructure. Thus PCs using Intel or AMD CPUs are preferred, and software operating systems like Windows, Linux and Unix are likewise preferred. The only area in which a degree of flexibility is permissible is that of embedded PC field controllers.

In Peter's white paper, he also indicates that developments in other areas of the industry have paved the way for other protocols that may well overshadow the BACnet/LonWorks debate. Among these new protocols are the following.

XML: Extensible mark-up language, or XML, allows software to communicate with other software and will set a new standard for all software communication. Furthermore, it allows for backward and forward code migration.

OPC: OLE for Process Control brings in the depth and breadth of industrial automation. The use of XML in OPC will result in a whole new specification: OPC-XML.

UPnP: Universal Plug and Play is already in use in the home automation market and is based on XML. It is used for video, audio, lighting, HVAC and security, and it is now moving into the wireless arena.

.NET: A relative newcomer, Web Services or .NET has significant backing from Redmond.

According to Peter, all the effort being put into XML-based software could bring about an era in which buyers will be free to decide on best of breed for each system element as they can do today with IT hardware.

On a related note, if the Security Industry Association has its way, its Open System Interoperability and Performance Standards (OSIPS) will prevail. OSIPS is currently being presented to the U.S. government and the Department of Homeland Security as a way to get rid of the many different proprietary offerings and replace them with a unified standard protocol, which may or may not be open to all.

Third-Party Suppliers

Another way in which a number of manufacturers are attempting to overcome the difficulties in providing their customers with an open solution is to embrace third-party suppliers. Manufacturers are reaching out to third parties that have demonstrated an ability to produce reliable, cost-effective sub-systems that can be combined to make up a totally integrated solution.

A recently commissioned market survey of 320 independent security dealers and consultants in December 2003. Many of the survey's questions dealt with the manner in which security dealers and consultants prefer to go about the integration process. One question in particular went to the heart of the open systems protocol topic, asking respondents if they would prefer access control products that integrated with their own internally-developed enhancements (biometric, DVR, etc.) or that integrated with mature third-party products. More than 77% indicated that they would prefer to integrate with mature third-party products rather than with in-house product offerings. The responses from security dealers and from consultants were very similar.

The adoption of open systems protocols by an increasing number of manufacturers will allow end users to the move away from proprietary services and products, resulting in more choice, a reduction in built-in obsolescence, an easier path to upgrades and integration into third-party systems.

Lionel Silverman, P.E., a professional engineer, has been working in the security and access control field for the past 25 years in both the USA and South Africa. He is vice president of business development for Facility Robotics Inc., a nationwide systems integrator specialising in building automation and security systems for larger multi-location and prestigious clients. Mr. Silverman is a member of IEEE and ASIS.