



Open Systems Protocol

The movement toward open systems and the desire to use third-party products have become driving forces for new product integration in the security marketplace.

In many respects, the security industry is just coming of age. Only in the past couple of years have software developers begun to really focus on the growing opportunity of open systems. For years previously, security professionals purchased systems in a haphazard manner, buying each stand-alone component from a different supplier.

Each component of a security system was usually installed for a unique reason. Fire systems, mandated by the AHJ and insurance, were often supplied as part of the building. Insurance companies encouraged or required the use of a burglar alarm, especially if the facility had already been robbed. CCTV installations, similarly, were pushed through by management when there was a potential loss of company assets. Photo ID may have been mandated by corporate based on risk-management policies. And access control was the big daddy of them all, often only installed when the horse had bolted from the stable and there was new, strong pressure to secure the complex from unwanted access.

These systems were often incompatible and left the end user with a highly dysfunctional total system. No standards existed, and data was not exchanged between systems. Expansion was not deemed a pressing issue, nor was migration to the next generation of equipment.

About a decade ago, a number of the larger equipment manufacturers who make multiple product lines began to produce highly integrated solutions. This resulted in a number of excellent solutions, but all of them were based on a proprietary architecture. The end user remained limited, because competitors' systems could not be included. The manufacturers' strategy in this was often to protect their own turf.

Peter Manolescue of SecurityXML, wrote a white paper entitled "A Common Security System Protocol." In the paper he paints the security industry as a Cinderella, saying that in many cases security is treated like an

afterthought or an unnecessary expense for which there is no viable corporate ROI. Peter concludes that the eventual solution of open systems integration may come from a totally different area of the marketplace: from any of the number of mainstream software suppliers that are gearing up their product offerings for the security market.

Over the past two or three decades, the mainstream computer world has been bravely pursuing open systems with significant success. The economies of scale and the need to improve efficiency have forced many companies to automate their entire workflow environment.

In the security world, proprietary systems built to accepted and recognised standards appeared to be an acceptable solution for a period of time (mid 1980s to 1990s). However, rising license fees, along with moves by the existing software manufacturers to keep any newcomers out, encouraged developers to devise a whole new level of systems that were not so harshly governed. These became the open systems of today.

This move to using commonly available computer hardware and software became easy to justify as proprietary systems became too expensive to write for and maintain. During the 1990s, an open system revolution swept through the IT industry, converting islands of computers connected by proprietary networks into the Internet—the network of networks based on the following openly available standards:

- TCP/IP—Communications
- SMTP—E-mail
- HTTP—Display of Web pages
- XML—Exchange of data

Open systems are able to communicate with each other and seamlessly transfer information between databases and users. Central to open systems is the use of open protocols—openly published standards to which all software programs must comply,

Many programmers began to write programs that allowed for the easy exchange of information between diverse systems. In the area of facility automation, tremendous progress has been made in the development of systems and methodologies to allow for communication between systems from different manufacturers.

Open Protocols in Building Automation

In BAS/HVAC and lighting in particular, the pressure on manufacturers to make their products talk to each other became a dominant factor in the past decade. Users of these systems began to see the benefits of a networked solution that was operating to recognised standards and that also allowed for adaptability and flexibility.

Two interoperable protocols for building automation systems have emerged over the past decade in the United States: LonWorks and BACnet. The war between these two is by no means over and may never be over. Both protocols have their supporters, and both allow for ease of use.

BACnet was initially developed by ASHRAE (American Society for Heating, Refrigeration and Air-Conditioning Engineers) and is based on a systems-down approach. It consists of a detailed seven-layer methodology for the transfer of information between dissimilar systems. It has gained a lot of support amongst manufacturers, consultants and end users because it allows many older systems to be integrated into newer ones.

LonWorks, on the other hand, places the intelligence on a chip located in each node, thus building the system from the device up. Echelon Corp. developed the communications protocol called LonTalk, and Toshiba and Cypress Semiconductors make the chips. The neat part about LonWorks is that there are some 400 manufacturers who make products that can all communicate with each other.