SIEMENS

Technical Article

Industry Sector
Building Technologies Division

Zug (Switzerland), March 28, 2011

Truly Open Standards: the way ahead for security management

By Neville Miles
Vice President, Head Security Solutions, Systems and Products, Siemens Building Technologies Division

We have all heard by now, how the world of tomorrow will be shaped by the recognised social 'megatrends' of urbanization and demographic change. But for the growing urban population, security will still, undoubtedly, be one of its most fundamental requirements. Larger companies, utilities and civil infrastructure are already demanding comprehensive security concepts that ensure real continuity and commercial survival and recent technological developments in digital image processing, biometrics, interactive user experiences and real-time location technology, are already making genuinely 'integrated' security solutions possible. These integrated security solutions will be instrumental in facing the security challenges of tomorrow.

We all know that the integration of traditional security disciplines – access control, intrusion detection and video surveillance with fire safety and building automation systems – is already possible on a single platform, giving operators the benefits of continuous situational awareness along with centralized management and alarm handling. Such security management solutions can already help prevent crime, accidents or attack, detect and warn of any dangers before they occur, and enable staff and external agencies to communicate effectively to deal with any incident or potential threat. Or simply ensure that things run smoothly and safely.
This integration up to now has, however, been achieved largely by leading manufacturers ensuring that their assorted devices could interoperate effectively via software within their own branded systems, all bound by proprietary protocols.

Manufacturers have made great strides in developing proprietary products and systems over recent years, but it is the development of software that is currently driving security technology forward. Although product development is still important and advances are still being made, it is now accepted that the provision of comprehensive, long-term solutions will require more. Security

Siemens Schweiz AG
Industry Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Cornelia von Dewitz
Telephone: +41 41 724-4363
E-mail: cornelia.von-dewitz@siemens.com

systems are far more complex than they were, say ten or fifteen years ago, but the dependence on the human factor still remains. Personnel come and go and today's systems themselves are - in some cases – much more difficult to learn and operate. So one current focus is the development of platforms to guide operators step-by-step in making the most appropriate decisions in an emergency or any other given situation. Other areas of software that have made substantial advances recently, include video content analysis, data mining, management systems and new user experiences.

The successful provision of those comprehensive, long-term solutions with built-in 'future-proofing' will certainly mean establishing the means for systems to communicate, not only with each other but also with products and systems developed in the future. To this end, there is a now a genuine desire for the security industry to establish its own rules for its various technologies and disciplines by the general adoption of common standards. With common interfaces between field devices, automation systems and management stations being standardised, the concept of singular 'proprietary' systems would then be a thing of the past.

One of the first moves towards this fundamental ability to run products and application programs from different vendors, to interact with other computers across local or wide-area networks regardless of their physical architecture or operating systems and to operate effectively with them, was the use of Internet Protocol (IP) technology, the set of communications protocols used for the Internet and other similar networks. In the first IP-based systems, most interfaces were proprietary, although some default standards existed, but this was brought about by market dominance rather than a developed standard. Proprietary IP systems were viewed by many as a retrograde step, as they locked the end-user into buying all items within the system from a single manufacturer.

To integrate and transfer data on a single network, Internet Protocol (IP) technology formally consists of the first three layers (Physical, Data Link, Network). But most networks today are based in some way on the Open Systems Interconnection (OSI) Reference Model, a set of seven layers that define the different stages that data must go through to travel from one device to another over the network and communicate fully between one another. The first three layers employed by IP-based systems ensure the cables connect and the data gets through in a timely manner without error - but does not ensure communication.

So, the use of IP technology alone does not ensure real connectivity - it is simply one step along the way. A truly open standard has a defined application layer, the layer that supports application and end-user processes, where communication partners are identified, quality of service is

Siemens Schweiz AG
Industry Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Cornelia von Dewitz
Telephone: +41 41 724-4363
E-mail: cornelia.von-dewitz@siemens.com

established, user authentication and privacy are considered, and any constraints on data syntax are recognized. To attain real interoperability, which will bring about huge benefits to the industry, we need to have all levels of the OSI model defined. For this to happen, the industry as a whole must explore and embrace ways in which technologies based on truly open standards across all the industry's disciplines, can be developed. This is where the drive for open standards within the security industry, led by organisations such as ONVIF (Open Network Video Interface Forum) and PSIA (Physical Security Interoperability Alliance), comes into its own.

Open standards will bring benefits throughout the industry. For the end-users, an open standard will mean a more cost-effective, flexible solution. They will be able to choose from the most suitable combination of products, regardless of manufacturer. And, by future-proofing their system, it will mean security of investment, with reduced cost of ownership - through simplified installation and lower integration costs. For the system integrators and security consultants, it will mean increased flexibility and the freedom to specify products from different manufacturers, thereby meeting the specific needs of customers more easily. For the manufacturers and the software vendors, it will mean interoperability with other manufacturers' products - without loss of their own brand identity - and extended market opportunities. They will also benefit from lower development costs as well as increased market interest.

Open protocol initiatives are already moving developments within the industry forward. The effort to establish a worldwide standard in IP-based video technology has already gained momentum and, as a result, conformant video transmitters and receivers are now able to communicate with each other and exchange information such as live video, audio, metadata and control information. Both specifications ensure that appropriately conformant devices are also automatically 'discovered' and connected to network applications. As a result, it is already possible to ensure interoperability between network video products of different brands and it is far easier for end-users, integrators, consultants and manufacturers to take advantage of the possibilities of network video.

With other industries - telephony, television, leisure/comfort - moving wholeheartedly towards native IP, the security industry is currently lagging behind in the adoption of truly open standards. But, having ONVIF (255 member companies, 615 compliant products) and PSIA (92 member companies, 82 compliant products) each striving to establish the one global standard, robust competition is driving the quest for open standards within the industry onwards. Both are, even now, working towards bringing open standards, not only to the video sector, but also to access control, analytics and software. The aims of this extension in both organizations, is to promote interoperability of security devices across all segments, supporting licence-free standards and

Siemens Schweiz AG
Industry Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Cornelia von Dewitz
Telephone: +41 41 724-4363
E-mail: cornelia.von-dewitz@siemens.com

specifications for the whole security industry, which are vetted in an open and collaborative manner.

But the move to open standards - and those many benefits they will eventually bring throughout the security industry as a whole - will only succeed when buyers are actively specifying compliant products. It seems that some players within the industry still believe they can remain detached from the crusade for integration with other manufacturers, maintaining their proprietary systems and their 'captive' customers' reliance on their products, systems, servicing and pricing - and it is only through the tendering process and a mandatory insistence on products and systems that are compliant with an open standard, that this attitude will be changed. Many buyers and end-users are already aware of the benefits and insisting on interoperable products and systems often in big tenders, but it still requires an effort by the industry in promoting and marketing the impressive 'plug and play' ability of compliant products already available.

With this increasing desire for 'plug and play' capability, open standards might also mean the opportunity for security devices to interoperate and communicate outside the conventional 'security' arena. For instance, it might soon be commonplace for video surveillance systems to be utilised in the event of a suspected outbreak of fire by verifying the authenticity of any alarm, the location and spread of the flames and in checking the occupancy of the building (while physically possible) throughout the entire incident. Access control systems already include time and attendance recording but could also be used to verify the suitability and training records of staff to use certain restricted equipment. The opportunities eventually afforded by open standards will be almost without limit.

The main challenge that currently faces the industry in developing truly open standards for IP-based systems is the adoption of a single standard by the whole industry. Both ONVIF and PSIA face several years' work in developing really comprehensive protocols that remain live, describe all parts of the security system and deliver backwards compatibility. The standard that the industry finally chooses must be solid in all aspects of its specification, must offer genuine, 'plug and play' capability and be fully adopted by a recognised international standards authority.
As a leading player in the security market, with a long history in both video and access control systems, the business unit Security Solutions from Siemens Building Technologies Division evaluated the two major standards initiatives and chose to focus support on ONVIF. The ONVIF specification works towards a comprehensive video interface including support for video metadata and its Web Service-base which facilitates fast and simple integration. The three founding member companies were particularly strong in the video market and Siemens was also satisfied with the original statement issued by ONVIF, regarding intellectual property rights (IPR). This

Siemens Schweiz AG
Industry Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Cornelia von Dewitz
Telephone: +41 41 724-4363
E-mail: cornelia.von-dewitz@siemens.com

indicated the members' belief in the need for existing and future contributors to work impartially towards an open standard in order to ensure the success of the standard, relinquishing any rights they held in protocols and ideas that might be taken up.

One result of the close collaboration within ONVIF, was the launch in 2010, of the integrated security management system, Siveillance Fusion, by Siemens Building Technologies Division. The solution combines video monitoring, access control and intrusion protection on an IT-based platform and enables customers to manage all security-related processes in an integrated environment. The system also enables other information sources, such as Fire, Comfort and Point of Sale (POS) as examples, to be networked and monitored. But most importantly, Siveillance Fusion gives customers freedom of choice in selecting field-level components, allowing customers to choose from over 650 ONVIF conformant IP video cameras, for instance.
Siveillance Netwatch, an integrated solution to link physical and IT security for the first time, running as a module under Siveillance Fusion, (or Siveillance Vantage/Siveillance Command) was also launched. Siveillance Netwatch platform enables the systematic monitoring of selected IT components and their performance, and creates alarms, which are displayed and handled via the security management systems, should something be suspicious, providing a complete security view including components performance in real-time. Already the industry is showing a lot of interest and Siemens has plans to develop it further.

The continued and growing need for security brings with it the need for new solutions, systems and processes that facilitate the efficient flow of people, assets and information. The Siveillance family stands for integrated security solutions from Siemens, offering command and control, complete security management and wide-area surveillance solutions. It is the result of the desire of one leading system integrator to fulfil the fundamental needs of their customers; providing a future proof, open, comprehensive solution to their security problems and allowing their customers to focus on their own core value propositions. In working towards achieving this, Siemens has also worked on another of the security industry's challenges; the development and adoption of a single, truly open security standard spanning all areas of security and being available to everyone to benefit from. The possibilities that the Siveillance portfolio brings, combined with open industry standards, will certainly bring an exciting new era to the security industry – an era almost without limit.

The **Siemens Industry Sector** (Erlangen, Germany) is the worldwide leading supplier of environmentally friendly production, transportation, building and lighting technologies. With integrated automation technologies and comprehensive industry-specific solutions, Siemens increases the productivity, efficiency and flexibility of its customers in the fields of industry and infrastructure. The Sector consists of six divisions: Building Technologies, Drive Technologies,

Siemens Schweiz AG
Industry Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Cornelia von Dewitz
Telephone: +41 41 724-4363
E-mail: cornelia.von-dewitz@siemens.com

Industry Automation, Industry Solutions, Mobility und Osram. With around 204,000 employees worldwide (September 30), Siemens Industry achieved in fiscal year 2010 total sales of approximately €34.9 billion. www.siemens.com/industry

The **Siemens Building Technologies Division** (Zug, Switzerland) is the world's leading provider of safe, secure and energy efficient solutions for buildings („Green Buildings") and building infrastructure. As a service provider, system integrator and product supplier Building Technologies offers building automation, HVAC, fire safety, security, low voltage power distribution and electrical installation technology. With around 42,000 employees worldwide (September 30), Building Technologies achieved a turnover of €6.9 billion in fiscal year 2010. www.siemens.com/buildingtechnologies

Siemens Schweiz AG
Industry Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

Public and Press Relations: Cornelia von Dewitz
Telephone: +41 41 724-4363
E-mail: cornelia.von-dewitz@siemens.com