OPEN STANDARDS

WHY SHOULD THE SECURITY INDUSTRY ADOPT THEM AND WHY ARE MANUFACTURERS RELUCTANT TO DO SO?

CONTENTS

Abstract – **This paper explains the benefits that standardisation brings. It defines the type of standards that exist and explains the differences between proprietary and open standards. The way in which standards are controlled by Standard Bodies are explained. Open standards are defined, and are illustrated with a number of examples familiar to all of us. The benefits to the adoption of Open Standards are explained.**

The security industry has yet to embrace open standards and the existing state of the security market is discussed together with the reasons why the industry is reticent to adopt Open standards. Finally, the way in which Salent's Omnis Networked Surveillance System utilises Open Standards is outlined and the benefits that end users achieve as a result are explained.

1 INTRODUCTION

"The nicest thing about standards is that there are so many of them to choose from."

Ken Olsen (1926 -), founder of Digital Equipment Corp., 1977

In a society that reveres individualism, the cynical and irreverent attitude to standardisation exemplified in Ken Olsen's quote abounds. However, while universal standardisation would unquestionably stifle imagination and inventiveness, the benefits for making technology widely available and cost effective cannot be disputed.

This white paper presents an introductory discussion of Open Standards and their increasing importance within the security industry. It outlines the importance of standardisation, defines the precise nature of Open Standards and explains their unique benefits. This is put into the context of the security industry with a discussion of existing standardisation within the market, the reasons why open standards should be adopted and the way in which Salent's Omnis system utilises open standards to the benefit of our customers.

2 STANDARDS

With the large number of varying standards in existence there are a number of ways in which they can be defined. One such technique is to distinguish between market created standards (**de facto** – '*in fact*') and those introduced by a recognised standardisation body (**de jure** – '*of law*'). The following provides a definition and examples of the three general standards. The later are usually the result of consensus between the members of the relevant standardisation body, often formed from those in both the public and private sectors.

2.1 PROPRIETARY STANDARDS

These are often introduced by private companies in competition with other standards, and lack the backing of official bodies. These standards can be made publicly available for no charge or can be subject to a license fee. Many well-known consumer based standards have been developed in this way and include many of the interfaces on a PC.

The USB bus, for example, that is used to connect many peripherals from cameras, keyboards to mobile phones etc, was jointly developed by Compaq, IBM, Intel, Microsoft, NEC and Northern Telecom. The technology is now openly available for all computer and device vendors. Firewire is another example of a successful standard that was developed by Macintosh for connecting high-speed peripherals and was taken to the IEEE for adoption as a standard (IEEE 1394). This standard gained in popularity for use in PCs and for connecting consumer video recorders.

There are many examples of standards that have not benefited the end user or manufacturers. Within the consumer market, the famous battle between Betamax and VHS left many end users with redundant equipment and lost development effort.

Equally, the CCTV industry has a multitude of standards for controlling Pan Tilt Zoom (PTZ) cameras. The end user suffers in terms of cost, lack of choice and inflexibility. The manufacturers suffer because of the additional effort required to develop and test the different protocols, resulting in a more costly product with no additional benefit to the end user.

Proprietary standards can be 'open' in the sense that they are made freely available but are not of direct benefit to the end user or manufacturers. These standards can also be subject to a license fee.

2.2 STANDARDS BODIES

Recognised public organisations can manage and hold standards. There is a huge plethora of such standards and bodies controlling interests ranging from health and safety, methods of operation (e.g. The European Standard EN50232-1 introduced to cover the security sector) to communication protocols (ITU-T body) and broadcast standards (PAL, TV line definitions).

Without many of these standards, modern day life simply would not function. How easy would modern day life be if the mains power distributed varied from county to county let alone from country to country? Other than the potential health and safety concerns, the cost of goods would increase. When substantial public interests are at stake, adherence to the standard is mandatory often as direct dictates in the form of law.

Within the digital CCTV market there are standards that control the types of compression technology. Many companies have invested a lot of time and money in developing technology that might be used in defining these standards and they wish to get a return on their intellectual property.

The controlling bodies can take different stances in developing the standards. The Joint Photographic Experts Group (JPEG) is responsible for the producing the draft specifications for the JPEG standard, and JPEG200 amongst others. Their philosophy is that the underlying technologies should be provided royalty free by the relevant companies. The draft standards are then submitted to the ISO and ITU standards bodies. The MPEG standards, on the other hand, do require licenses to be purchased for each device. To simplify the licensing process an organisation called MPEG LA centralises the licensing of these standards.

3 OPEN STANDARDS

3.1 DEFINITION & CHARACTERISTICS OF OPEN STANDARDS

Recently a new type of standard distinction has emerged, whether a specific standard is of an open or a proprietary nature. Put simply the distinction is in the stringency of restrictions placed on the use of the standard by its owners. However, openness is not merely restricted to the standards use but applies to the collaborative effort used during its creation and potentially, to the technology necessary to implement the standard. Often the work is carried out in committees through open standards organizations, such as the Internet Engineering Task Force or the World Wide Web consortium.

Conversely, a proprietary standard is characterised by the fact that it belongs to someone. The standard owner can (or does) put restrictions on users' access to it and their use of it; they have complete control of the form and function of the components that use the standard typically via numerous iterations of product releases.

An ideal open standard can therefore be defined as having the following characteristics:

- It is accessible, free of charge to everyone with no discrimination between users.
- It remains free and accessible throughout - for example, owners are committed to openness during the remainder of a possible patent's life.
- It is fully documented, with access to and use of the documentation free.

The resulting philosophy of an Open Standard is that it permits everyone to utilise its specifications to build infrastructure and solutions without any form of licensing.

However one subtle but crucial point is often left out of the definition of an Open Standard. The definition that matters most is that experienced by a customer or end user - "openness" is defined by the ease with which a customer can substitute one product for another. If you use a product, but the vendor providing it triples its prices, how easily can you move from that product to a competing product ? An open product facilitates this. A proprietary product hinders it.

3.2 EXAMPLES OF OPEN STANDARDS

If we consider the landscape of computing over the last decade we can see how a recent outbreak of co-operation between competitors in the software industry has affected the way in which systems are developed.

In 1992 the Internet opened to business traffic. Prior to that point proprietary network protocols dominated, notably Novell NetWare, Appleshare and DECNet. Into this varied bag appeared TCP/IP, an open, royalty-free protocol stack that enabled any participating computer to talk to any other, not just on the company LAN but anywhere in the world. This resulted in a revolution in software paradigms, from computing as something that was undertaken on isolated systems to computing as a process carried out by multiple co-operating components that might be situated on hardware scattered around the office or across the world.

The catalyst for this shift was an Open Standard - TCP/IP. This is one of many important Open Standards that provide strong foundations for software interoperability.

3.3 BENEFITS OF OPEN STANDARDS

The previous section illustrated how the adoption of Open Standards is becoming the norm for large complex software systems – the primary benefit being increased system interoperability. This offers the customer a number of additional benefits:

- **Greater consumer flexibility** – The adoption of Open Standards by multiple vendors increases the competition between them, increasing quality and lowering prices.
- **Reduced risk of dependency on a specific technology** – The risks associated with dependency on a single technology are reduced because Open Standards transcend all vendors and remain durable, as does your selected system.
- **Vendor independence** – The selection of a proprietary system inevitably means adapting and tailoring procedures, data and ancillary systems to ensure compatibility with the system selected. As a consequence, changing this system at a later date may prove costly. An Open System dramatically decreases the cost of changing vendors.
- **System Integration** – Open systems can quickly and easily integrate with new technologies, without the need to consider whether your suppliers,

customers, partners and other related entities will be able to integrate.

- **Improved Quality** - Open Standards, because they are open to all, receive wide peer review thus improving the quality of the technology being standardised.

From this list it is self-evident that Open Standards empower the customer, giving them the ability to optimise their options and the freedom to choose a system that meets their specific needs.

4 Open Standards in the Security Industry

4.1 Existing State of the Security Market

In the past, much like early computer systems and networks, collections of stand-alone components were typical – CCTV installations, access control, alarm systems and building management systems, each produced by different suppliers were the only choice available. Often these systems were incompatible leaving the end-user with a highly dysfunctional and somewhat haphazard total system. No standards existed, and consequently it was impossible to openly exchange data between systems.

More recently, some of the larger manufacturers have begun to produce integrated solutions, similar to the days when proprietary network protocols dominated in the computer industry. Many offer excellent solutions, but are based on proprietary architectures. The end user remains limited because competing solutions cannot be easily integrated.

The problem of the late 20th century computer industry, where my Appleshare network can not easily talk to your Novell Network for example, has been transformed into the problem of the early 21st century where the integrated time recording and door entry system is unable to talk to your CCTV system, neither of which can communicate with the existing building management system. The solution to this is the adoption of Open Standards, which are continually improving to reduce the barriers to the integration of disparate systems.

4.2 Why is the Industry Reticent to adopt Open Standards ?

The simple reason that the security industry is reticent to adopt Open Standards is that the proprietary standards that are currently prevalent, generate higher licensing and recurring revenues. However, pressure is mounting, both from external sources and from within the industry as companies such as Salent begin to develop products and systems of an open nature. As happened with software development, where the adoption of Open Standards revolutionised the computing industry, the move towards Open Standards within the security industry has begun. Software developers are increasingly focusing on the opportunities that the use of Open Systems present.

Within the building industry derived standards such as BACnet and LonWorks have been in existence for a number of years. These protocols allow HVAC (Heating, Ventilation and Control) systems to have a common control-messaging infrastructure. They are however, totally new to many in the security industry.

Is the correct solution for the security industry to adopt these predefined protocols? Currently the security industry has many disparate devices (e.g. Pan Tilt Zoom Controls, Door entry mechanisms and multiplexers etc.) and control and query mechanisms. These have served the industry well, but at a cost to the customer in respect of on-going maintenance. The adoption of these protocols would benefit the consumer. However, this is unlikely to happen quickly and does not resolve the more immediate requirement for systems that interoperate.

The ability to exchange information and link security systems to building control systems is becoming increasingly important. In addition to the demand from customers to reduce running costs there is pressure from governmental departments (for example the US Department of Homeland Security) to improve interoperability. In order to achieve this the security industry will have to adapt and ensure their products are capable of linking adequately to others. The adoption of Web services and other Open Standards would enable this.

4.3 THE OMNIS APPROACH TO OPEN STANDARDS

Having discussed what open standards are, and why they are beneficial we can now consider the ways in which the Salent Technologies Omnis system has adopted Open Standards to meet three of its key design requirements:

1. **Accessibility** – graphical user interfaces which are intuitively easy to use and open programmer interfaces that allow user customisation of the products and the straightforward integration of third party products.

2. **Scalability** – supporting private individuals with tens of cameras up to large industrial consumers with hundreds of cameras.

3. **Extensibility** – ease of integration with existing and future systems (for example door entry and biometric systems) and the ability to quickly add new components such as additional cameras and servers.

4.3.1 ACCESSIBILITY

Accessibility, as defined in this paper, relates directly to ease of use, not just for end users but system integrators, developers, product support engineers and installers. Meeting the varied requirements of such diverse users is important in creating maintainable, scalable systems which are easy to install and adaptable to a wide variety of customers needs.

The core Omnis system utilises Sun's Java Technology. This has an open specification and a wide range of open community processes aimed at continually improving the language's feature set and capabilities. An additional benefit of Java is its platform independence, allowing the Omnis software to run on any computing platform, from standard desktop PCs running Microsoft Windows or Linux to Apple Macs and even mainframe Solaris based servers.

Sun and its Java Technology are also key contributors to the Open Standards movement and Java has had many features built into it for the support of Open Standards; for example it fully supports XML (eXtensible Markup Language) and the range of core technologies being built on top of this, such as SOAP (Simple Object Access Protocol) and XML-RPC (XML Remote Procedure Call). Another example is the full support of Unicode - international character sets which allow swift and easy internationalisation of all messages and user interface controls - a small thing but extremely important in the modern world.

Documentation generated via Omnis is generated as HTML, viewable in any browser, which again has full Unicode support to allow the quick internationalising of documentation. This also means all documentation is easily customisable via HTML to promote your corporate identity.

Imagery is stored in a standard image format – JPEG 2000, the latest generation of compression technologies, providing high compression rates while maintaining image quality. As a consequence, all video sequences can be exported and edited or annotated in commercially available packages, such as Adobe Photoshop or JASC Paint Shop Pro.

Omnis components are all defined using the JavaBeans framework. From a developer's perspective this means that customisation of the user interface for your specific business's needs is quick and straightforward - each control is provided as plug and play components, which are also available to third parties for integration into their applications.

Database communication is carried out via SQL, an Open Standard for database querying. This means Omnis can utilise any existing Oracle database or alternatively, it can use any SQL compliant server such as Microsoft SQL server or MySQL. System configuration and logs are stored in a standard fashion, not in a proprietary, binary format that require expensive tools to view them.

4.3.2 SCALABILITY

Scalability is one of a number of key benefits offered by the Omnis system, which scales easily from a simple system with a single camera and a single desktop PC with combined user interface and data store, to enterprise systems which integrate hundreds of cameras, numerous servers and redundant data store technology. This is achieved via a *virtual matrix* utilising Ethernet networks and TCP /IP transfer for all video data and control information.

In this environment a camera can be placed anywhere on a corporate LAN and can send data to anywhere else on the same network or even, via secure transmission, over the internet to geographically remote locations. Using DHCP, an Open Standard protocol for dynamically adding devices to a TCP/IP based network, adding additional cameras to the system is as simple as plugging the camera into a free Ethernet socket - the system will automatically detect the new device and make it available for users via the OmniControl user interface.

4.3.3 EXTENSIBILITY

Extensibility is the mechanism whereby the Omnis system has been made future proof and durable. Salent Technologies' adoption of Open Standards has been critical to its ability to develop an extensible system that makes Omnis truly unique within the CCTV surveillance market.

All the system messages, from control messages to alarms, are carried over TCP/IP in XML. XML is an open text based format that, in addition to preparing the system for future technologies (as discussed below), makes for smoother product support and installation because it requires little or no propriety tools to decode binary data formats. For example the addition of a new camera type with PZT control amounts to the addition of a configuration file, not an entirely new Omnis software release, which saves the customer time and money.

XML is also the fundamental building block of Web services, which allow truly open and flexible systems. To promote Web services Salent is an active participant in the Obix project, and is a member of OASIS (Organization for the Advancement of Structured Information Systems). This allows Salent to guide the development of Web Services for the security market.

Omnis has a built in Web service interface and, via the combined technologies of UDDI (Universal Description, Discovery and Integration) and WSDL (Web Services Description Language), this interface will be openly published to allow third part applications access to services provided by Omnis.

Other organisations, such as the Open Security Exchange (OSE), seek to promote the integration of disparate components of the security industry. When it formed, the OSE cited lack of integration of physical and cyber security technologies as "the most glaring example of how security management remains fragmented at most organisations today." Organisations such as the OSE and Obix will help provide the focus and direction for the security industry.

This, for example, allows the Omnis system to communicate directly with .Net enterprises, and provides access to all the system control functions and features from that network - even if it initially knew nothing about the Omnis system. Conversely, a door-entry system could provide its services to Omnis via a Web Service, which would then be made available for configuration via the OmniControl user interface.

5 CONCLUSION

Open standards are freely available specifications that allow disparate systems from different vendors to interoperate. By adopting existing Open Standards and being actively involved in the development of new standards, Salent Technologies and its Omnis system provides users with a cost effective, flexible, state-of-the-art CCTV surveillance system, enabled to support the growing momentum behind the Web services computing community.

6 FURTHER INFORMATION

Salent Technologies is at the forefront of the revolution that is introducing Open Standards into the CCTV surveillance industry. Salent has a vast amount of experience in both analogue and digital network technology and can provide valuable guidance when specifying the requirements of a Networked Surveillance system. Please contact us to obtain product information and guidance, or to arrange a product demonstration.

Salent Technologies Ltd

Rowan House, Wyndford Brae, Philpstoun,
Nr Linlithgow, West Lothian, EH49 6RN, UK

Tel: +44 (0)845 22 66 508
Fax: +44(0)845 22 66 509

info@salent.co.uk www.salent.co.uk