Challenges in integrating technologies emerging in electronic security

The field of electronic security systems is very broad and ranges from intrusion detection, access control, tracking and surveillance to screening technologies and explosives detection. **Michael Dever** explores some of the possible challenges facing security managers when it comes to the integration of new or emerging electronic security technologies into new or existing physical security systems.

"SECURITY MANAGERS MUST NAVIGATE THE MAZE OF NEW PRODUCT OFFERINGS TO FIND THE MEASURES THAT DELIVER THE BEST OUTCOME."

The security industry is constantly evolving and developing new electronic security technologies. Electronic security systems have undergone rapid evolutionary changes in the past decade, driven by the needs of the public and private sector to respond to new and more dynamic threats, to reduce the cost of ownership (based on a defendable business case), to improve systems reliability and to provide better interoperability with other related systems such as building automation systems. Emerging electronic security solutions such as IP-based CCTV surveillance systems have leveraged off the signi cant and ongoing advances in electronics in the general market place, particularly in display, computer, memory and network-centric capability and capacity.

There is increasing customer demand for coherent solutions for core building technology systems such as information and communications technology (ICT), building automation systems (BAS) and electronic security systems to utilise a high degree of common communications infrastructure, common user interfaces, multipurpose hardware and aligned installation effort. However, some parts of the traditional security industry can be slow to adopt new technologies, but as more and more of the enabling technologies, infrastructure and solutions are rolled out, IT and BAS companies are now competing for electronic security systems projects, challenging the traditional security industry that must adapt to become IT savvy or partner with an IT savvy systems integrator in order to compete effectively.

Valid concerns have been raised by the traditional security industry about the security issues associated with control of electronic security systems by an external system (e.g. BAS), open protocols and loss of effective trusted control of critical security functionality. These issues currently tend to limit the level of interoperability of electronic security systems with ICT and BAS that end users are prepared to accept, especially at the high security end of the market.

Despite these limitations, there remains a compelling technology-based argument and increasing business pressure to maximise the utilisation of standard network, computer and related infrastructure in a range of security, building automation and core ICT systems.

Apart from the pure technology and functional aspects of the available electronic security solutions, there remains the challenge facing security managers to successfully navigate the maze of new product offerings to nd the range of measures that in combination delivers the best value for money outcome to meet the requirements of the end user.

Employing the correct measures means a feasible and cost-effective solution that is viable over the life cycle of the equipment. Choosing the correct measures is determined by an operational requirements analysis starting with credible threat, vulnerability and security risk assessments followed by risk mitigation options and cost/bene t analyses.

Systems integration

Historically, each electronic security sub-system component (e.g. security alarm systems (SAS), electronic