As demand for PSIM-based security solutions gathers pace, Darren Chalmers-Stevens examines what is driving the growth in CNI projects and asks what makes a gold standard for assuring resilience and interoperability

PSIM CITY

There are a variety of electronic security vendors – from video management and access control to perimeter fencing systems that today leverage the buzz around physical security information management (PSIM). Yet there continues to be a need to clarify what constitutes true PSIM software. PSIM is a platform that collects and correlates events and alarms from disparate existing and new security devices and information systems (video, access control, sensors, analytics, networks and building management systems) into one common operating picture. PSIM is designed to empower personnel to identify and proactively resolve situations. This integration results in lower risk, improved security, faster response, better compliance and lower operational costs.

Five core capabilities characterise a true PSIM solution: collection, analysis, verification, resolution and reporting. Agnostic software collects data from any number and type of disparate security devices or systems. Data, events and alarms are then analysed to identify security-sensitive situations and their priority. Relevant event information is next presented in a quick and easily digestible format for security officers to validate and manage the situations. A software library with standard operating procedures then resolves the identified situations by utilising systematic instructions based on best practices and the end-user's own policies and procedures. Finally, PSIM software should track all information and steps for compliance reporting, training and, as needed, in-depth investigative analysis and/or prosecution.

To offer a truly technology-agnostic approach, PSIM vendors focus on selling and marketing on a PSIM platform, rather than a range of other security products. Given the need to share propriety code to develop the PSIM interface, true PSIM providers can more easily integrate with the full range of subsystems from all vendors, free of competitive conflicts.

Growing privatisation of critical national infrastructure (CNI) has occurred during the last several decades.

©Getty Images

> **"True PSIM providers can integrate with subsystems from all vendors, free of competitive conflicts"**

With lessons learned from 9/11 and the heightened awareness associated with enterprise risk management, along with the growing threat of cyber-crime, there's an increasing burden placed on CNI organisations to comply with an ever-expanding list of regulations, standards and best practices. In the UK, we've seen physical security regulation for CNI led by the Centre for the Protection of National Infrastructure. In the US, the Department of Homeland Security's Office of Infrastructure Protection has an extensive mandate regarding both public and private sector risk management. Multinational organisations increasingly must comply with multiple layers of statutory and regulatory security requirements, including industry-specific regulations and guidelines. The majority of these laws and regulations encompass both physical security and IT security in some form.

As a result, the compliance burden is twofold. As requirements for new policies and procedures grow, costs increase and there is a need for non-security departments, such as IT, to work alongside risk management, physical security and business continuity teams to understand and assess risk. The potential cost of non-compliance is a compounding factor that causes organisations carefully to weigh the impacts of fines, litigation and reputational damage. An organisation's most vulnerable point could reside way outside the traditional remit of the risk management and physical security departments. For instance, it could be a financial institute's data centre's building controls or a process control system in an oil refinery.

So how does an organisation balance managing a complex risk profile cohesively while ensuring compliance? PSIM solves this critical need by strengthening compliance and mitigating risk. If disaster strikes, a business needs to demonstrate beyond all reasonable doubt that it complied with standards and regulation by following policies and procedures to ensure the best possible outcome. PSIM vendors typically work in partnership with CNI businesses and their consultants to take a holistic view of risk. Without PSIM, personnel alone become the glue for finding, retrieving and sharing information at each stage in the process. This can be difficult in the midst of an emergency involving co-ordination with multiple organisations when compliance to policy and procedure can potentially fall apart.

PSIM CITY

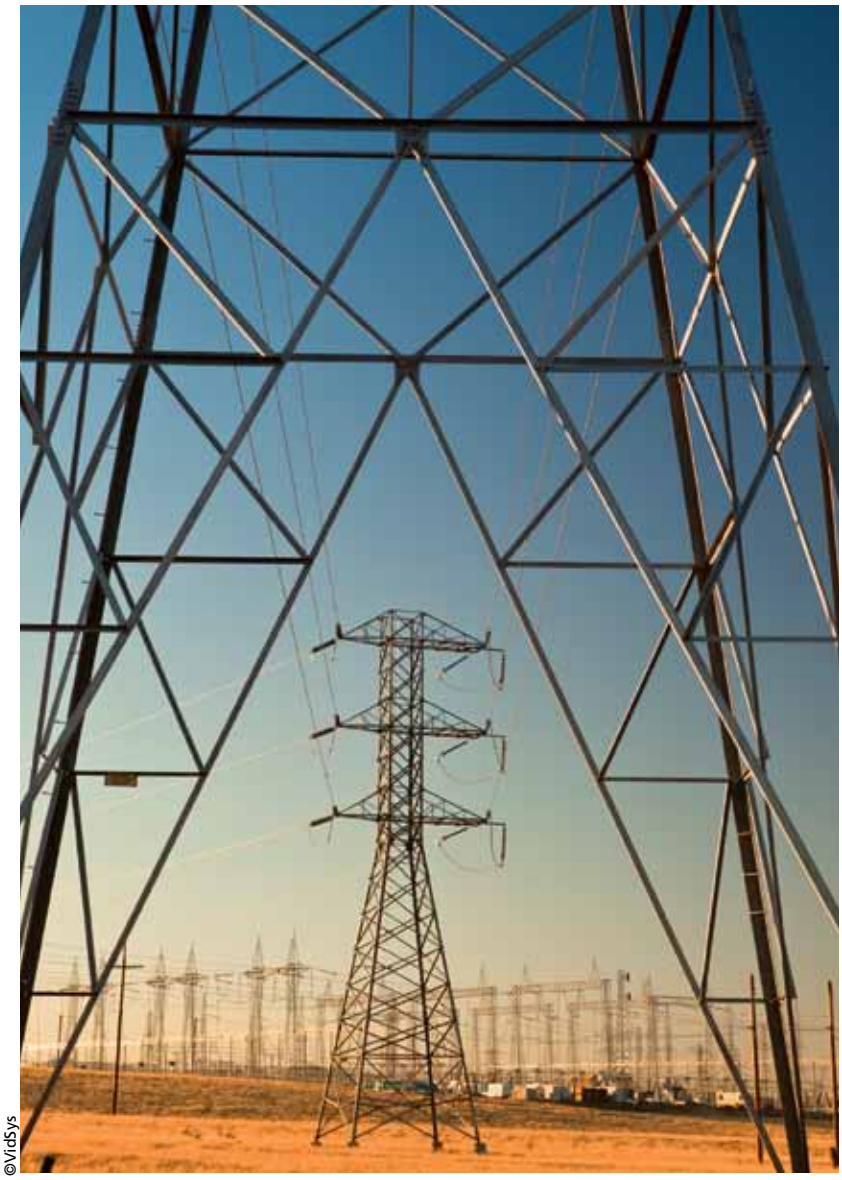
PSIM implementation supports that often-painful interdepartmental convergence of risk management to determine standard policies and operating procedures (SOPs). The PSIM vendor will initially assess security, building and IT systems that present integration opportunities to reduce human intervention while reducing operational costs and mitigating risk. True PSIM solutions enable one complete and intelligent security system by aggregating information from these various systems and automating processes.

By connecting these various operational systems, PSIM monitors events and encapsulates the rules and standard operating procedures (SOPs) for identifying and verifying situations. PSIM then presents operators with intelligent, actionable information for resolving situations as they unfold. This includes the ability to provide real-time escalation of incidents to department heads and other authorised parties, such as emergency services. PSIM's open architecture supports automatic alerting of department heads and specialists via e-mail, text or VoIP so that relevant staff are called to action, even remotely, by leveraging their area of expertise. For instance, a high temperate reading from a data centre's building management system may need the support of a facilities engineer who can utilise remote diagnostic capability enabled by PSIM. Alternatively, the PSIM can alert a maintenance company to attend and repair the system before a situation evolves into a full-blown incident. A corporate network breach will need the support and expertise of IT security engineers remotely to isolate and resolve the threat. All the while, the PSIM software monitors for compliance to ensure best practices for the safest, quickest and most effective resolution.

While compliance is not the only challenge PSIM addresses, we're seeing it as a major driving force in the selection and adoption PSIM-based security solutions. In addition, by automating processes and eliminating the need manually to review and correlate data from multiple systems, PSIM enables attractive time and resource reductions, which translate to cost savings. Providing personnel with real-time information and complete situational awareness drives a more efficient, effective and safe resolution to situations. This co-ordination is not only cost-effective, but results in the compliance goal of hardening resilience of our national infrastructure. An intelligent response through collaboration and information sharing across departments and emergency services also results in saved time, money and, in some situations, lives.

While the great integration and interoperability debates rage on in the security industry, an opportunity presents itself for the market to take the lead on demanding and driving an industry standard. PSIM technology evolved just over half a decade ago, and during that time vendors have typically forged customer-led alliances and strategic partnerships with a majority of the enterprise-level security systems manufacturers. It's among corporations, CNI operators and public sector markets that PSIM is realising its greatest growth – and where more sophisticated enterprise-level systems tend to be operational. It stands to reason, therefore, that a shared benefit for both PSIM vendor and manufacturer is to maintain on-going support for new product releases. There are also simple technical ways around integrating even older analogue systems such as legacy fire or intruder panels. PSIM was developed to integrate analogue and hybrid as well as IP-enabled systems. Manufacturers are forging alliances with PSIM vendors for market penetration opportunities, unique selling points and to demonstrate future proofing their systems.

As a result, PSIM vendors should now be offering commercial-of-the-shelf (COTS) solutions, meaning there is little-to-no customised coding required to integrate systems and deploy the PSIM. The time to deploy and project cost, should now be determined by minimal configuration to meet customers' needs, such as actually integrating the chosen systems and then adapting policies and SOPs within the best practice workflow already residing in the software library. As more PSIM projects come to fruition globally the desire across system manufacturers to make the necessary investment to create open standards will also increase.



©VidSys

Going live: PSIM systems can significantly improve the security of critical infrastructure

Darren Chalmers-Stevens is Vice President EMEA for VidSys and is an internationally recognised security technology expert. He previously served as technology development manager for ADT Fire & Security, and has also held roles with Computer Network Limited (CNL) and Integrated Communications at IBM in the UK, where he managed global solution development and delivery.