

## Piecing Together the PSIM Puzzle

BY LING-MEI WONG 2010/10/12

Physical security information management (PSIM) promises to make life easier for security operators. Instead of managing systems separately, PSIM provides a converged platform, bringing the most relevant information to the fore while advising the best course of action. Operators can piece together the whole picture from many disparate systems. In the event of a fire, smoke detectors can sense the fire, cameras can offer video verification and the PSIM can list response measures for the operator to take. An integrated platform maximizes existing investments, combining multiple systems into one seamless interface. However, each provider has its own way of bringing multiple inputs into a cohesive whole, resulting in varying definitions of what true PSIM is.

Physical security information management (PSIM) promises to make life easier for security operators. Instead of managing systems separately, PSIM provides a converged platform, bringing the most relevant information to the fore while advising the best course of action. Operators can piece together the whole picture from many disparate systems. In the event of a fire, smoke detectors can sense the fire, cameras can offer video verification and the PSIM can list response measures for the operator to take. An integrated platform maximizes existing investments, combining multiple systems into one seamless interface. However, each provider has its own way of bringing multiple inputs into a cohesive whole, resulting in varying definitions of what true PSIM is.

Physical security information management (PSIM) is one of the hottest buzzwords in the industry. Sometimes referred to as "situational awareness" or "command and control," more viable solutions show that convergence is now a real-life trend.

The benefits are clear for holistic management. Instead of tracking access control on one workstation, video on another and intrusion on a third machine, operators can have a bird's-eye view of all systems through PSIM.

"Technologies such as video analytics and PSIM help automate video monitoring, filter out irrelevant information, and provide operators and guard forces with the data they need to make more intelligent decisions — typically referred to as 'actionable data' in

the language of IT; 'situational knowledge' in the language of public safety; and 'total domain awareness' in the language of homeland security," said Aberdeen Group in a March 2010 study on video surveillance.

All the flowery terms mean one thing: Bringing the most important information to the operator 's attention. Instead of trying to watch 100 video feeds, control room staff can manage their time better and respond to issues faster. "With the same number of full-time equivalent staff , the topper formers in Aberdeen's study are



able to support 3.3-times more cameras and 21-times more alerts requiring evaluation and action by guards or operators," Aberdeen Group said.

PSIM does not replace human operators, but helps them make sense of multiple inputs more efficiently. "For example, an operator monitoring an unidentified object in the airport can simultaneously view pictures from multiple cameras, access video archives to trace the sequence of events leading to the placement of object and path it has taken, monitor the chemical identity signal from a robot explosive detector, and evaluate evacuation procedures from a crisis management tool," said Bhaskar Ganguly, Global Marketing Director for Critical Infrastructure Protection, Automation and Control Solutions, Honeywell International.

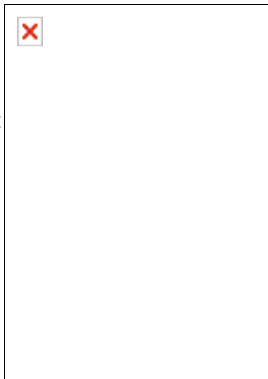
**PSIM, VMS, ACS**



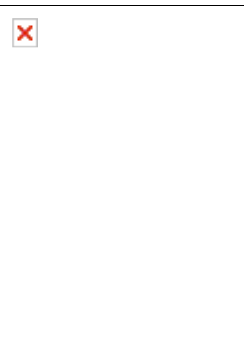
Management software such as VMS or access control software (ACS) keeps tabs on individual devices in a system, sometimes even integrating inputs from other subsystems like intrusion. However, such management platforms cannot integrate all — including elevators, climate control and lighting — and usually are proprietary. True PSIM is vendor-agnostic and should give operators a clear set of steps to follow, depending on what sort of emergency is taking place.

No universal definition exists for PSIM. "There are many unique features which clearly set a PSIM platform apart; most of which have been customer-driven to answer real business challenges and provide bottom line value," said Matthew Kushner, President of the Americas for Computer Network Limited (CNL). "It's surprising how far some VMS and ACS companies are willing to stretch the description so as to add 'PSIM' to their product labels."

A converged management platform needs to do more than pull in feeds of alarm data, video images and card usage. "A true PSIM solution provides a much higher level of integration, providing a bidirectional interface with an auditable database management system," Kushner said. "This level of integration is the only way to provide local sites with complete command and control, regional managers with overall situational awareness and senior management a dashboard view of how a security situation could impact their business's bottom line."



System-specific management software has limited functionality. "There are many VMS and ACS platforms that offer integrated solutions in a box," said Brandon Arcement, Manager of Global Security Technology, Building Efficiency, Johnson Controls. "They typically don't have the flexibility of a PSIM software, as engineers are frequently focused on priorities other than just third-party integrations, and they are somewhat constrained by the application and control logic code at the base of their software."



As ACS and VMS address specific system needs, they are less complex compared to PSIM. "With an open PSIM, you can include almost everything," said Holger Maier, Product Manager for Building Integration System, Bosch Security Systems. "On the other hand, some ACS solutions integrate just video and intrusion, but are much easier to install for VARs and system integrators."

Genuine PSIM solutions correlate relevant data from more security systems better than any other type of software. "Because PSIM solutions are built to support a variety of

systems and technologies, the operator display and flow of information deliver a much more holistic view of the environment," said Larry Lien, VP of Product Management, Proximex. "It's not focused on just video or alarm information, but connects and correlates information from many various sensors and systems to give operators the most relevant data in order to respond better to incidents."

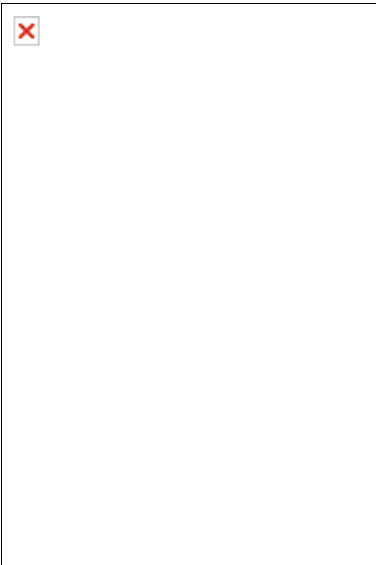
**System Integration**

There are a number of ways to integrate systems into PSIM. Some PSIM providers team up with hardware manufacturers to support their solutions, while others work exclusively with software companies. This results in different degrees of integration in the final management platform.

There are three ways to integrate systems for PSIM. First, there is hardwired integration, Arcement said. Then there is standard protocol integration, involving protocols such as BACnet, Modbus, Lon or OPC.

A standardized OPC client in the PSIM communicates with any OPC server, making integration simple. "The subsystem can deliver any data from the connected detectors and cameras, so the PSIM can process and display this information," Maier said. "On the other side, the PSIM can be programmed to control the many different connected subsystems from one common customized user interface."

Finally, systems can be integrated with APIs or SDKs from the manufacturer, which is the most robust integration. "APIs expose more information than a standards document can and thus allow a developer to support more functionality in the integration," Arcement said. "One drawback is that these integrations take time to schedule and develop, and they often need significant maintenance when subsystem versions change."



The software approach usually pays off better than spending effort integrating with hardware. "The real play here is the integration of event information and controls; therefore, software integration is usually the way to go," said John Moss, CEO of S2 Security.

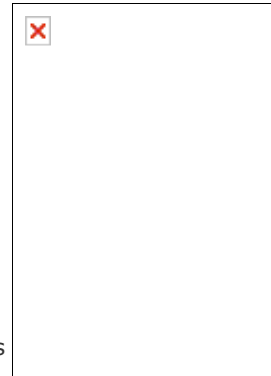
SDKs enable system integrators and installers to create different user interfaces, such as for VMS, said Alf Chang, Senior Consultant for A&S magazines and a former installer. Most sensors are covered by standard protocols, so a Wiegand card reader will integrate with nearly all platforms.

However, the maintenance of multiple systems is complex. "If you try too much to optimize each piece of the system, the system can become quite fragile," said Kevin Daly, CEO of Maxxess Systems. "Often, a looser integration does not bring with it as significant a penalty as you might think, since it can provide you with more flexibility if the system components change."

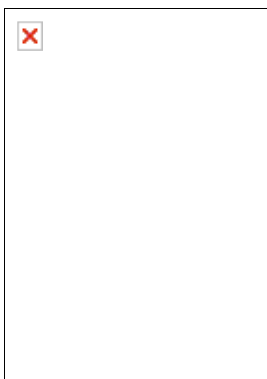
**Making New Friends**

Integrating third-party software is not hard technically, but the manufacturer may not want to reveal all of its secrets. Thus, the PSIM software may be able to display the proprietary software, but cannot run all features natively, such as built-in analytics.

Integration with third-party systems is straightforward if the subsystems support industry standards. "ONVIF is a great example for such integration and will enable integration of not only network cameras but also serverbased analytics engines and access control going forward," said Anand Mecheri, CMO of Siemens Building Technologies.



The PSIM platform's integration is as deep as system manufacturers provide through their SDKs and APIs. "The biggest obstacle is typically a multitude of different systems which give acceptable service at the local level, but due to the intentional proprietary nature of these systems, it's almost impossible to bring all of these systems together into a single system," Kushner said. "Most security equipment manufacturers have made interoperability through a common GUI almost impossible."



At a recent project, the user wanted to use Agent Vi analytics on Milestone Systems' and Cisco Systems' respective VMS systems. However, each system displayed the analytics so differently that additional manipulations were required for uniform operator response, Kushner said.

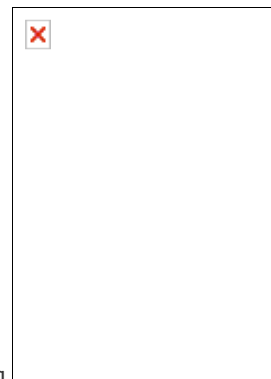
It is reasonable to expect most day-to-day functionality to be available in the PSIM, but usually not all features are transferred, Arcement said. It could be that the protocol or method of integration did not allow certain types of information to be transferred; the subsystem manufacturer chose not to expose that functionality

through the shared API or the PSIM developer chose not to support a certain portion of the SDK.

Intergraph emphasizes emergency response, so only the most essential functions are integrated for operational needs. "Not everything needs to be integrated right away, if ever," said Bob Scott, Executive Director of Security Solutions Strategy for Intergraph. "Our goal is to provide our customers with value by increasing their operational capability through integration and by providing a platform or framework that can grow and evolve with their needs."

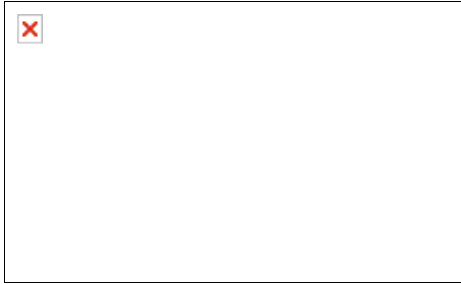
**Real-World Technology**

PSIM delivers real benefits, but is not for everyone. A small installation with four cameras does not require a command-and-control platform to manage an overwhelming number of inputs. In general, large projects facing higher risk, such as airports, nuclear power plants and hospitals, are more likely to benefit from using PSIM.



As construction has slowed down, has demand for PSIM gone down? Some experts believe so. "I expect the number of PSIM installations has been lower recently," Chang said. "Most commercial high-rise buildings can use their own surveillance management software as an alternative to PSIM, at least for physical security installers."

ADC, a subsidiary of Robert Bosch, thinks differently. "In Singapore's context, we've been seeing increasing prospects and tenders based on seamless integration," said Daniel Ko k , Bus in e s s Deve l opment Manager for ADC Technologies International. "IT infrastructure serves as the backbone for communications of virtually



all electronicsbased systems. As technology advances and is able to cater to a wider bandwidth at faster speed and reasonable cost, security products will naturally follow in tandem and leverage on the backbone.”

Other market players have also observed growth for PSIM. “We've seen the mature markets like North America and Europe use PSIM

more frequently in existing facilities, while emerging markets like Asia and the Middle East have requested PSIM more frequently for greenfield construction projects,” Arcement said.

More users facing high risks have adopted PSIM. “These tend to be companies who are geographically dispersed or concerned with business continuity,” Ganguly said. “If the customer is building a new facility that he sees as being high security risk, he would likely invest in the latest technology to mitigate the risk he sees in a possible breach.”

PSIM is sometimes installed for efficient business management. “In some cases, customers have already built their primary security infrastructure and now want to use the available information productively and intelligently to earn returns,” Ganguly said. “This is possible only when a PSIM system is installed and used in day-to-day operations.”



The number of PSIM projects has increased significantly, particularly for existing buildings with disparate security and building subsystems that need to be incorporated into a new or additional installation, said Stephen Moody, Security Development Manager, ViS Security Solutions. Integrating multiple subsystems, however, requires significant resources and can face roadblocks for third-party equipment. In the next article, we examine what makes a PSIM solution good, along with cost considerations and challenges.