

Current Status of PSIM Development

Submitted by Adlan Hussain, Marketing Manager at CNL2010/6/9

An interview conducted by Adlan Hussain, CNL Marketing Manager, brings a number of insights on PSIM. The following contributions suggest the way Matthew Kusher, CNL President, defines the buzzword.

An interview conducted by Adlan Hussain, [CNL](#) Marketing Manager, brings a number of insights on PSIM. The following contributions suggest the way Matthew Kusher, [CNL](#) President, defines the buzzword.

What does PSIM offer in the way of command and control/situation management capabilities that video management systems (VMS) and access control systems (ACS) don't, especially when the latter are IP-based and can be integrated?

Full security management system integration using a PSIM platform is very different from simply connecting disparate systems using a VMS or an ACS. Whether from business unit acquisitions or a desire to move toward a centralization of corporate services, progressive companies are facing the business decision of how to bring disparate systems together into a single, unified, integrated security management platform. 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 is almost impossible to bring all of these systems together into a single system. Most security equipment manufacturers have made interoperability through a common GUI almost impossible.

Companies are looking to combine their existing security systems, expand with their chosen brand, and slowly replace failed components with that chosen brand. The optimum platform for this is the PSIM platform. Unfortunately, there is currently no universally accepted term for what a PSIM is and what it isn't. It is surprising how far some VMS and ACS companies are willing to stretch the description so as to at "PSIM" to their product labels.

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. Some of these key differences are: Vendor Independence: The majority of VMS and ACS are not open architected; the manufacturers of these technologies have vested interests in selling their technology to the exclusion of all others. They will settle on a smaller customer base and possibly a niche market in order to secure the sale of as much of the system's software and hardware as possible. If an end-user desires to integrate a competing VMS or ACS, they have a very small chance of receiving any help from the primary manufacturer. In most cases, VMS and ACS

manufacturers will be quite hostile to such requests, often threatening to withhold warranty or tech support.

Migration: A true PSIM provides a strategic platform for managing the migration from old to new technologies. It is often used by organizations to phase in new technology across their enterprise over a period of time. This is often the prime driver of a PSIM solution, as it has the most measurable impact on hard capital and operational costs.

Level of Integration: Integration is a much overused word in the security industry. What most manufacturers call integration is simply connecting systems using basic protocols to pull in feeds of alarm data, video images, or card usage. A true PSIM solution provides a much higher level of integration, providing a bidirectional interface with an auditable database management system. 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.

Powerful Authentication and Permissions Systems: PSIM software is designed to integrate into corporate authentication policies using corporate IT standards. This ensures a consistent level of security across the organization, regardless of system, operator, or user. An additional advantage is that a PSIM can offer administrable role-based permissions which help enforce corporate compliance and complete a full security, safety, and HR program management system.

High Availability/Disaster Recovery: Well designed PSIM solutions allow organisations to build high levels of resilience for five nines, giving 99.999 percent of uptime. In a command and control facility, down time of any type for any reason is unacceptable, even for routine maintenance. Many are surprised, often at the worst of times, that their security system has several single points of failure.

Process Guidance and Intelligent Workflow: A significant added value of PSIM is its ability to guide an operator through the process of managing alarms, whether they are from a fire alarm system, an access control system, video content analytics, etc. This is typically done to ensure security operations comply with processes in line with enterprise risk management, or that are needed to ensure compliance with regulatory bodies. Often the need to enforce regulatory compliance is the key value driver of a PSIM solution; this is also a feature missing from most ACS and VMS platforms.

Management Reporting and Integration of Business Systems: A true PSIM is based around adding business value; its ability to link into other business systems allowing it to increase overall business performance. Business speed and incident impact are now too far reaching to keep important situational data down at the operational level. In-depth and specialized reporting can be easily generated using simple built-in tools.

Management reports can be automated and sent out to relevant individuals by e-mail. Generally, end-users create different levels of reports for different levels of management. For example a shift supervisor would receive relevant reports on his shift, a security manager would receive overall security performance and incident based reports, and a CISO would receive high level KPI-based reports. To further drive value from the security system out to other departments of a company, PSIM data mining and analytic capabilities can be utilized to create highly specialized reports for other department heads. For example, video data from a camera on a loading dock combined with a truck gate card reader normally used by the security department can be used by the headquarters department to enforce vendor compliance with drug tests and site safety induction currency. The facility manager can use that same data to monitor his internal staff's safety procedures while loading the truck and verifying that the operator loading the truck is current on his equipment operation license.

Some VMS vendors are positioning themselves against PSIM by calling it a custom, expensive solution for high-end, high-security needs. How accurate is that perception of PSIM's applicability?

PSIM creates business value by levelling proprietary physical security systems and bringing security operations in line with other business systems. This in turn allows physical security to interact with other business systems and take its place within corporate governance. This is functionality that VMS integration simply cannot provide.

A VMS has limited use; typically it is purchased as a system to prevent security problems. In reality, the value that it provides is to help piece together the chain of events after a security incident has taken place. Video analytics have promised to make surveillance systems more proactive. In practice, these software and hardware additions have been greatly oversold in their capabilities. Even those VMS whose users have attained an acceptable level of functionality with their video analytic systems do not have the tools to integrate into the company's key operational business needs.

It is true that in the pioneering days, PSIM solutions started life at high end in high security facilities, as this is where the need was greatest. Software development and processor power have greatly accelerated the use of these systems, and they are now much more commonly used. Today, deployments of PSIM can be found in education, corporate enterprise, maritime and air ports, critical nation infrastructure, law enforcement, homeland defence, and a growing list of more sectors.

The reality is PSIM solutions have become significantly more sophisticated in the last few years, with significant emphasis on adding organization value, whether this is through hardened security, increased efficiency, or reduced ongoing costs. The crucial factor being that the customer can decide what their priorities

are and implement all or just a few modules of a PSIM according to their unique situation. The good news is that the cost for PSIM solutions continues to decrease.

The commercial, off-the-shelf nature of these products means that 80 percent of a typical PSIM solution is preconfigured. Unsurprisingly, organizations of a similar type like critical national infrastructure, have similar security needs and policies as one another. This allows for the use of templates, which can be quickly customised for individual organisations. Furthermore, as governments get involved with specifying guidelines for security best practices; these policies are starting to look even more similar to one another.

As PSIM manufacturers grow the integrations they have to a larger number of security systems, they allow greater use of existing infrastructure. This alone can provide sufficient saving to warrant the use of a PSIM platform. And because real PSIM solutions are modular, organizations only pay for the functionality they need, bringing down the cost of deployment. As a result, the deployment cost of these solutions is coming down as they become easier to implement. The use of wizards and plug-n-play technology is now making PSIM solutions viable not only for large companies, but now for medium sized organizations as well.

When you talk about PSIM as a solution for integrating disparate physical ACS, how can or does PSIM address the issue of multiple physical credentials within an organization?

PSIM software integrates data at a database level, so it can work with a headquarters database as a single point of contact to update credentials for multiple ACS. This ensures corporation-wide identity management that works both efficiently and securely.

We have instances where our software is used to integrate ACS from multiple manufacturers, across multiple facilities. One badge will allow an individual to gain access to all buildings, irrespective of what ACS may be in use. Without the software, the end-user would have no choice but to replace the access control systems in some of these buildings, which would cost significantly more money and cause much more inconvenience during the cutover phase. The reason for this is simple; access control vendors rarely share their SDKs and APIs with their competitors. Their goal is to sell their proprietary software and hardware, not to integrate with other access control systems.

What are some of the technical and nontechnical issues that arise when PSIM is proposed for tapping into VMS and other systems owned by third parties?

In today's market, there are very few issues, technical or nontechnical regarding integration with VMS and

other third-party systems. Smart vendors understand that PSIM is not competing with their business and are keen to get their products integrated into PSIM products, as they recognize the value it offers end-users. The proprietary nature of some VMS products meant that each was completely different, based on different underlying technologies; this meant that a lot of time had to be set aside to develop the required drivers. Fortunately this is changing, and video interoperability standards such as the PSIA and ONVIF will help make future integrations quicker and less costly.

Aside from vendors, a major issue was the ability of integrators to consult, develop, deliver, manage, and maintain successful PSIM projects. Typically the skills required to deliver PSIM successfully were found in IT integrators, which lead some to create partnerships with security integrators and converge the two disciplines. Again, the industry has moved on, and we are finding more and more security integrators investing in the skills required to implement these solutions.

How might PSIM solutions interact with IT-based security solutions like SIEM to provide a comprehensive view of enterprise security? How interested are customers and/or prospects in achieving such a view?

Our software has the ability to use standard IT connectivity such as ODBC to integrate with other business systems such as SIEM, Tivoli, SAP, and a host of HR Systems. This ensures organizations can create holistic solutions to provide enterprise-wide integrated security systems for Enterprise Risk Management solutions. Examples of uses include Enterprise Single Sign On (E-SSO), On boarding and Off boarding, physical and logical alarm management, and hardening of physical and logical security posture. In addition, we are the PSIM developers who have a freely available DDK, which allows third parties to write drivers which talk directly to our software.

Largely, drivers for the adoption of this technology include the hardening of security for compliance to industry regulation and increasing risk associated with operating in certain industries such as critical national infrastructure, pharmacological, biotechnology and finance.

We are seeing a lot of interests from organizations looking to create solutions between physical security, logical security and building management systems. The ability for an organization to prove and enforce compliance to evolving standards such as HIPAA, Sarbanes Oxley, and HSPD-12 means they need to have these intelligent systems in place.

Increasingly we are also seeing M&A activity, corporate social responsibility, and green issues as drivers of this technology in the corporate space. The last few years have seen the creation of the Chief Security Information

Officer, who is responsible for both logical and physical security. This has been a catalyst for converged solutions, which make greater use of technology for enterprise wide security management, focusing on reducing security operational expenditure.

Recent acquisition activity within the PSIM sector has led some industry commentators to question the strength of PSIM solutions, should we believe them?

I personally disagree with this; the PSIM market is stronger than ever. In the case you are referring to we see that a key VMS provider has acquired a PSIM vendor for a sum which cannot be described as insignificant. If we asked ourselves why they have done this despite the fact that they have a very strong VMS offering, we can only come to the conclusion that the PSIM product offered them significantly more capabilities than their current products.

I am aware some industry commentators have pointed out that the value of the deal signifies a weakness in the PSIM market. What we must remember is that PSIM vendors invested a lot of marketing dollars in educating the market on what was possible with a PSIM solution. Maybe we were too early; we all know the security industry is slow at technology adoption, just take network cameras, whilst these offered clear benefits over analog technology they have only recently taken over analog cameras in sales volumes. The last couple of years have seen PSIM as an accepted method of integration; the fact that a key industry name has bought into the technology is proof of that.

There is also speculation that this may lead to more PSIM vendors being acquired by VMS or ACS vendors looking for a quick way to connect to other systems. This goes against the basic principles of a true PSIM platform; as soon as they are acquired by a vendor they lose their open nature as competing vendors won't want to work with them any longer. For us at least, we see vendor independence as a key strength.

In summary, PSIM is a new application area not covered by other security applications that relies heavily on IT integration skills. How are CNL and the other major players going to bring this technology to market?

All the serious PSIM vendors are selling through and building a hybrid sales channels who can address both security and IT issues. In most cases, we assist in the sales process and architecting of the solutions, but insist that we use the first installations as a way of transferring technical skills. This is working well as it makes the transition for traditional security integrators easier, as they have the benefit of our extensive experience.

We predict a number of smaller specialist consultancies will develop to assist the security integrators in designing, commissioning and implementing PSIM solutions. If the security industry develops like other industries through this phase of integration and collaboration, we will see that as these hybrids get to a reasonable size, the majors will start buying them.