White Paper

Making the Case for PSIM (Physical Security Information Management)

What is PSIM Software?
Why consider it over a basic CCTV management system?

The market for PSIM software and solutions is relatively new and grew out of the need for public and private organisations to become more resilient in the face of the threats of the past decade. Significant factors were the homeland security response in the US after 9/11, the failure of a fast, joined up response to Hurricane Katrina, and industrial accidents such as those experienced in the oil and gas sector such as Texas City. The raised security threats mean that it is essential to integrate and automate security systems as far as possible.

A second factor is that technological advances have made it possible to capture, process, analyse and store the large amounts of data that are generated by security systems, including data from sensors and video cameras. Moore's Law and new capabilities in hardware such as video analytics, intelligent fences, smart phones and tablets and more powerful, flexible data networks make it possible to use integrating software applications to provide intelligent, vigilant, surveillance of assets.

Physical Security Information Management offers large ROI

A PSIM solution integrates, automates and governs systems such as CCTV, PID, fire alarms and other HSE (Health and Safety Executive) systems as well as systems such as HVAC and industrial process control. The essential components are listed overleaf.

PSIM Components

Connectivity and Integration

The capability to integrate multiple disparate security systems such as video surveillance, access control, perimeter intrusion detection, fire and safety, public address and building management.

Configuration Management

The capability to define and change policies and parameters related to various connected devices in the underlying subsystems.

Programmable Logic

To enable broad programm-ability of the system for users in complex security environments with multiple integrated systems. PLC allows us to create detailed cause and effect automation and response in even the most complex integrated solutions.

Geospatial Visualisation

Functions for mapping and spatially visualising the actual situation independently from active events.

Response and Workflow Management

Presents users with step-by-step instructions on how to respond to an event. These are detailed, rule-based workflows and are presented within the software in order to maximise the user response to any incident.

Audit, Reporting and Analysis

PSIM systems should provide a comprehensive audit and reporting capability that enables detailed forensic review of an incident and the response. It should be easy to create customised reports that allow for analysis of multiple events in order to optimise policies and workflows.

Resilience

The capability for immediate disaster recovery, business continuity and redundant operation. This includes backup systems (servers, databases, network) for automatic transfer of control room operation and so on. True PSIM systems include self-monitoring capability to protect the integrity of all the integrated systems while maintaining automatic vigilance against threats.

Benefits of PSIM include:

- Systems are no longer silo'd so it becomes possible to have total oversight and control which leads to much greater security and safety for people and infrastructure.
- The ability to integrate industrial and control systems creates huge savings through, for example, avoidance and mitigation of shutdowns.
- Increased safety of employees and public because of enhanced supervision of people and systems.
- A greater ability to anticipate and prevent problems and incidents because of increased real time and near time perception of threats and failures.
- Better compliance with internal systems and protocols, and also with external regimes especially in the area of HSSE.
- Enhanced control, governance and supervision, including audit tools and emergency response capability.

What To Consider

If your organisation is thinking of implementing a PSIM solution or updating an existing, integrated CCTV system, there are several providers in the local and global market offering what may seem to be dependable options. Bear in mind the following criteria when appraising candidate vendors:

- Look for a supplier with a demonstrated track record, solid credentials and a good reputation.
- Does the company have case studies in your industry? Can you contact a referee?
- Do they provide part of the solution or all of it? PSIM implementation on anything other than very small scales requires design and engineering services, bespoke hardware provision and powerful software.
- Beware of companies that can only supply the software.
- Think about the of cost of ownership of each candidate solution: are there likely to be high migration costs? Will you need to abandon current hardware that may still have useful life left in it?
- Beware of solutions that tie your business in to proprietary hardware such as a specific brand of camera. This could prove functionally limiting and very costly.
- Consider the data management and related information security options. Where will your data be stored? How secure is the solution? How easy will it be for you to access historic data?
- Will you be able to access your data from any location? Is there a Web interface? Is there a mobile app for remote access?

- How flexible and open is the PSIM system in terms of integrating with your existing security systems and hardware?
- To what extent will you and the supplier be able to precisely configure the PSIM solution to your organisation's specific needs now and in the future?
- If you require to automate part of the system, such as automatic response to alarms, does the system provide sufficiently for this? What programmable logic tools are offered?
- Does the software provide geospatial visualisation and mapping tools?
- Do you require workflow management capability? Do you want to integrate response protocols to guide the activities of staff following an event? Does the technology provide the capability for this?
- Does the software include a comprehensive audit and reporting capability? Will you be able to generate customised reports?
- Does the architecture of the solution include disaster recovery and business continuity capabilities? Is the solution self-monitoring and vigilant against threats? In other words, how resilient is the PSIM system itself?
- Is the system Secure?

Further Considerations

Do the Maths

When it comes to doing your sums, there are three figures to consider in relation to PSIM:

- Purchase costs, including all hardware, software and engineering services.
- Cost of ownership over several years, say three to five years.
- Your return on investment (ROI). Purchase costs will depend primarily on:
- The complexity of your requirements
- How much bespoke development and integration is required
- How much functionality is available "out of the box"
- How much ongoing support is available and how much you will need to do yourself
- How the licence fee is structured - for example, whether it is a one-off price or an annual subscription
- Maintenance and hosting charges if they apply
- Service and support costs

The main factor in long-term cost of ownership is the openness of the system, that is the extent to which it can integrate with any other hardware and software. If the system is closed / proprietary, you will face substantial future costs relating to integration and upgrade and also much greater installation costs because of the need to replace existing equipment with the necessary proprietary hardware.

Therefore, the ROI from PSIM is a straight ratio between the costs saved through using the system and the costs incurred in acquiring and deploying it.

Savings fall into two categories:

1. Problem prevention:

- Reduction in lost production time
- Decreased costs arising from incidents
- Reduced costs of remediation of problems
- Savings on insurance premiums (very relevant in museums)
- Improved overall productivity and use of infrastructure

2. Efficiency savings:

- Reduced costs of physical supervision (security guards on patrol, invigilation, etc.)
- Reduced costs responding to and investigating incidents (such as on oil rigs)
- Reduced inspection, audit and site visit costs

By examining historical accounts and the logs of current security systems, especially in relation to security incidents, a company should be able to estimate reasonably accurately the annual cost of its current security systems. These can then be projected over a three or five year term and compared with the costs and savings of a PSIM system over the same period. This should give a fairly clear indication of the ROI of a PSIM investment.

- Reliance on human security.
- No thermal imaging.
- No automation (cause & effect).
- Ineffective command and control and workflow automation.
- Lack of integration.
- Preventive controls do not allow enough response time once triggered.

Visual Mamagement Systems Limited is the UK leader in PSIM with customers including national security and defence organisations, oil companies, museums, airports, utilities companies, police forces, local authorities and retailers.

Visual Management Systems Limited
15 Cambuslang Road, Cambuslang Investment Park.
Glasgow G32 8NB. United Kingdom
Tel. +44 141 643 3070 | Fax +44 141 643 3079
Email info@titan-vision.com | www.titan-vision.com