PSIM and Management Systems

A Comprehensive Review

Building.
Technology.
Solutions.

messe frankfurt

Table of Contents

1. What is PSIM

With increasing connectivity and digitalization, the demands placed on security solutions have grown ever more complex. Physical Security Information Management (PSIM) and other management systems are indispensable tools in the modern security landscape to meet these growing requirements. They provide a central platform for integrating and controlling various security technologies, significantly enhancing efficiency and responsiveness. Through automation and enhanced situational awareness, they help detect threats early and respond appropriately.

This white paper offers a comprehensive overview of PSIM and other management systems, their functions, advantages, and presents leading providers on the market.

PSIM stands for Physical Security Information Management. It is a software platform that integrates multiple disparate security systems and controls them through a unified interface. In short, PSIM acts as the brain of a security system. It collects data from various security devices such as:

- Video cameras
- Access control systems (e.g., card readers)
- Fire alarm systems
- Intrusion detection systems
- Sensors and IoT devices (e.g., motion or temperature sensors)

PSIM then analyzes the data, alerts security personnel in case of potential threats, and can trigger automatic responses according to predefined Standard Operation Procedures (SOPs), such as locking doors, initiating evacuations, or triggering alarm chains.

2. Key Functions of PSIM

2.1 Integration: PSIM systems combine various security systems into a single user interface

The integration of data from video surveillance, access control, intrusion detection, fire detection, or building management systems into a central platform usually takes place via open interfaces and APIs (Application Programming Interface). PSIM systems use standardized protocols (e.g., ONVIF, OPC, BACnet) or manufacturer-specific APIs to communicate with the various security systems. These interfaces receive, interpret, and present data in a common format. Often, PSIM platforms also use middleware, which acts as a mediator between heterogeneous systems. This middleware translates proprietary protocols into a unified data model that the PSIM can process. This is often referred to as deep integration with a manufacturer or a manufacturer's products.

The data received from different sources is normalized within the PSIM system, meaning it is converted into a standard format. As a result, alarms, status messages, or control commands can be processed across systems. Processing can also include analysis if a PSIM analyzes integrated data streams to identify relationships and automatically initiate actions.

2.2 Situational Awareness: Operators receive a real-time picture of the current situation

When integrated into PSIM systems, especially video management systems (VMS) provide real-time visual information. Live camera feeds offer immediate visual insights into security-critical areas, allowing security staff to see exactly what is happening, not just that an alarm has been triggered. Features such as multi-screen display, PTZ control (pan, tilt, zoom), and heat maps enhance situational awareness. PSIM systems combine camera images with other data sources, such as access control information, alarm messages, and sensor data, to create a context-rich overall picture. This makes it clear who tried to access where and when, which sensors were triggered simultaneously, and whether there are unusual behavior patterns. The aggregated information is displayed in a unified graphical interface—often with maps, dashboards, and live feeds—so security personnel can react quickly and purposefully.

2.3 Automation: PSIM can trigger predefined actions based on specific events

PSIM systems can automatically trigger predefined responses to certain events, such as displaying live video of a particular door and triggering an alarm when a blocked card is used for access. This can be automatic, or operators may be given step-by-step instructions for responding to incidents ("Guided Response"). This ensures standardized, traceable procedures during critical events. Advanced, AI-supported PSIMs can also automatically detect unusual behavior, such as lingering in sensitive areas, identify patterns in data (e.g., recurring incidents), and help optimize processes. Cross-system control within PSIM also allows the automated control of other systems and subsystems during an incident. For example, when a break-in is detected, lights can be switched on and doors locked. Police are notified, and cameras are focused accordingly.

2.4 Incident Management: Assistance with documenting and managing security events

Incident management in a PSIM system is a central component of its functionality. It enables security organizations to efficiently detect, assess, control, and document security events. When an incident is detected—such as a door opening outside business hours, a fire alarm, or an intrusion attempt—the system generates an "event." For each incident type, standardized response plans (SOPs—Standard Operating Procedures) are stored. The system guides the operator step-by-step through the appropriate response (e.g., open camera view, notify police, initiate evacuation), some of which can be automated. The system automatically documents who did what and when and enables communication with external agencies and internal teams. Escalations are triggered if there is no response within a defined time.

Each incident is comprehensively logged (including videos, system data, actions taken); reports can be generated automatically for audits or evaluations. In post-incident review, important insights ("lessons learned") can be documented after the event is closed. Intelligent systems thus help analyze vulnerabilities or optimize SOPs.

2.5 Scalability: PSIM is suitable for individual buildings, industrial complexes, as well as whole cities

The scalability of a PSIM system is one of its greatest advantages—especially in complex, heterogeneous, or rapidly growing security infrastructures. Good systems are horizontally scalable, meaning a PSIM can be deployed at multiple locations (e.g., branches, subsidiaries, production sites) simultaneously, and new locations or systems can be easily integrated into the existing architecture without having to set up the system from scratch. Most systems are also modular, so new functionalities can be added as needed.

3. Types of Management Systems

Apart from PSIM, many other management systems address particular security needs, such as:

- Video Management Systems (VMS): These systems manage and control video surveillance.
- Access Control Systems: They regulate access to different areas of a building.
- Alarm Management Systems: These systems monitor and manage alarms from various sources.

4. Installation of Management Systems

Whether PSIM and management systems are best installed in the cloud or on-premises depends greatly on the requirements, IT infrastructure, and security level of the organization. Each model has distinct pros and cons.

Comparison: Cloud vs. On-Premises in the PSIM Environment

Criteria	Cloud Solution	On-Premises Solution
Installation Effort	Low (provided by the supplier)	On-Premises Solution
Scalability	High – new locations/systems easily integrated	High (own servers, network, configuration)
Costs	OPEX (monthly/annual fees)	Limited – restricted by physical hardware
IT Personnel Requirement	Low – maintenance by provider	CAPEX (high initial investments)
Updates & Maintenance	Automatic by provider	High – own IT/security department necessary
Data Security & GDPR	Dependent on provider & region	Manual, often associated with downtime
Availability	High – redundant cloud data centers	Full control over all data
Connectivity	Internet connection required	Dependent on local IT infrastructure
Critical Infrastructure	Not always permitted (e.g., authorities, military)	Can also be operated offline

When is on-premises better?

For operators of critical infrastructure, those who want to retain full data sovereignty, whose locations do not have stable internet connections, or who do not want to be dependent on the provider or the cloud.

When is the cloud better?

A cloud installation increases flexibility and can be quickly scaled. It is also advantageous when a company has distributed locations or a central command center. The entry costs are lower and less IT personnel is required. Some AI-powered PSIM functions are cloud-based.

Hybrid Model – The Middle Ground

Many companies and organizations are now taking a hybrid approach, i.e., local data processing and storage (e.g., video data, access) on-premises and centralized control, analysis, and reporting via the cloud.

Conclusion: For small to medium-sized, dynamic organizations, the cloud is often more practical. For large, security-critical organizations with high compliance requirements, on-premises is frequently the better choice, and a hybrid model, if well installed and configured, offers the best of both worlds.

5. The Market

The global market for all IoT in commercial buildings (Building IoT / BIoT) is expected to grow from USD 64.1 billion in 2024 to USD 101.0 billion in 2030, representing an average annual growth rate of 7.87% in the base scenario.

Memoori's new report, "IoT Platforms in Smart Commercial Buildings 2025 to 2030," provides useful information about this rapidly evolving ecosystem.

The global revenue market for security software reached a record high of over 82 billion US dollars in 2023. This represents an increase of 13.4 percent compared to the previous year. However, this figure also includes software for IT security.

According to a Markets and Markets study, the global PSIM market size is expected to grow from USD 3.5 billion in 2024 to USD 4.3 billion by 2029, with an annual growth rate of 4.6%. The demand for PSIM solutions is increasing due to the need to protect organizations against increasingly sophisticated threats. The convergence of cyber and physical risks is further driving this development.

Mordor Intelligence estimates the size of the global market for physical security information management at USD 1.66 billion in 2024. The market is expected to reach USD 3.53 billion by 2029, representing an average annual growth rate of 16.24% during the forecast period (2024–2029).

6. The Range of PSIM and Management Software for Security Applications

If you want to take a closer look at the comprehensive range of software for security management, you need to examine the systems offered by individual providers in detail. The following overview explains the offerings from many leading suppliers, without claiming to be exhaustive. The author contacted a selection of leading providers in advance and asked them to answer the questions. The responses from the manufacturers who were asked and replied are presented in this chapter. First, the providers are introduced and their range of offerings is explained, before the providers' answers to the following questions are summarized.

6.1 Questions for the Manufacturers

To gain a better understanding of the capabilities and possible applications of PSIM and other management systems in the security sector, the most important providers were asked to answer the following questions:

- Do you see your system(s) as an overarching PSIM or rather as an integral component of PSIM systems?
- What do your system(s) achieve in terms of integrating security components and where are the main advantages?
- Which users need a PSIM system and who is better served with management systems that cover partial areas?
- For which target group (company size, industry, complexity of installation) is your system most suitable, or where can it best play to its strengths?
- What advice would you give to users considering introducing a new PSIM system?
- What advice would you give to users who want to replace their PSIM?

7. Providers of PSIM and Management Software

7.1 AARMTech (India)

AARMTech, headquartered in India, offers a Physical Security Information Management (PSIM) software platform designed to integrate various security system modules, including access control, surveillance, fire alarms, road blockers, and perimeter security. The AARMTech PSIM provides an effective solution for managing security operations in control rooms that handle large volumes of information. The platform incorporates multiple modules, allowing for functional extensions tailored to specific design areas, such as circuit simulation, and features a comprehensive schematic capture interface. Its simulation algorithms are based on nodal analysis and trapezoidal rule integration. Additionally, the software enhances productivity by supporting modules dedicated to sector-specific information management. Integration with Perimeter Intrusion Protection, GIS mapping, and other networks—such as command and control systems, telephony, and radio communications—enables the creation of robust, customized security and control solutions, all managed through a unified control panel.

.

7.2 Advancis (Germany)

Advancis offers a comprehensive solution for Physical Security Information Management (PSIM) with WinGuard. The open integration platform enables central management and control of various security, building, and communication systems. WinGuard also integrates IT infrastructure, as well as dispatch and ticketing systems. The system collects events from connected systems and intelligently visualizes them to support user situation awareness. Dynamic instructions and automated actions assist users in the control center.

Do you see your system as an overarching PSIM system or rather as an integral component of PSIM systems?

Our WinGuard system is clearly designed as an overarching PSIM system. This means we do not offer stand-alone solutions for video or access control, for example, but a vendor-neutral platform that brings together a wide range of security and building management systems on a central interface. WinGuard acts as a superordinate management system that does not replace individual subsystems, but intelligently links, visualizes, and makes their functions process-oriented and usable. The focus is not just on technical integration, but also on operational efficiency—how information is presented intelligently and user-friendly and how workflows are guided and documented in the event of an incident. We thus consciously position WinGuard as the central platform in the sense of a true PSIM system—not as a component within a PSIM, but as its core.

What services does your system provide in terms of integrating security components, and what are the main advantages?

WinGuard collects events from the diverse connected systems. Intelligent visualization of these events, dynamic procedures, and automatic actions running in the background support and ease the workload of operators in the control center. This significantly simplifies complex workflows and enables operators to fully assess and optimally resolve occurring situations. Currently, more than 550 interface drivers are available for various security, building, and communication technology systems, including IoT, robotics, and drone (UAV) systems. The development of new interfaces is also possible. Thanks to this vendor neutrality and open architecture, the entire technical infrastructure of a building can be visualized and controlled with WinGuard.

Which users require a PSIM system, and who is better served by management systems that cover only sub-areas?

A PSIM system like WinGuard is used whenever a large number of different security-relevant systems are to be integrated and centrally controlled via a single platform. This mainly concerns users with complex infrastructures—for example, operators of airports, critical infrastructure, industrial companies with site security, data centers, or public institutions. These organizations usually operate a large number of heterogeneous systems—such as video surveillance, access control, intrusion and fire detection systems, building automation, or communication systems. A PSIM system brings these worlds together, creates transparency, and enables operators to respond quickly and in a standardized way in critical situations.

For users with only a few subsystems or whose requirements are less complex operationally or technically, a specialized management system—such as pure video management or access control—may be the more economical solution. These systems are often optimized for a specific function and deliver strong performance in that area. The decisive factor is not the number of systems alone but also how much processes should be automated, standardized, and centralized—and the role of compliance, documentation, and interoperability, for example. A PSIM does not replace specialized systems, but serves as the central, superordinate platform that makes their potential usable in combination.

For which target group (company size, industry, installation complexity) is your system best suited, or where can it best play to its strengths?

In addition to industry, finance and administration, data centers, correctional and forensic facilities, transportation, healthcare, or military institutions, WinGuard is used in many other sectors, such as amusement parks, stadiums, or museums. Alongside specific solutions for different industries, open interfaces and collaboration with other companies enable the expansion of the system and the coverage of additional use cases. WinGuard is scalable from a single workstation to internationally networked control centers and can be expanded at any time with additional servers, workstations, functional modules, and interfaces.

What advice would you give users considering introducing a new management system?

Our advice is: Think process-oriented and long-term. Analyze carefully which individual subsystems are to be integrated, which processes need to be supported, and how scalable the solution should be in the future. Pay attention to vendor-independent platforms with open architecture to ensure flexibility and independence. In addition, all relevant stakeholders should be involved at an early stage—from the IT department and building management to the control center.

What advice would you give users who want to replace their management system?

You should carefully examine the weaknesses of the existing system and what needs to be improved in the new system. A clear migration plan is important to avoid downtime. Rely on a flexible, open platform with broad interface support—so existing systems can continue to be used or integrated step by step if necessary.

7.3 American Dynamics / Johnson Controls (USA)

American Dynamics, a brand under Tyco Security Products (now part of Johnson Controls), offers a comprehensive suite of physical security solutions. While not traditionally categorized under PSIM (Physical Security Information Management), their offerings provide functionalities that align closely with PSIM objectives. The Victor Unified Client is American Dynamics' flagship platform designed to unify video surveillance, access control, and other security systems into a single, cohesive interface.

Do you see your system as an overarching PSIM system or rather as an integral building block of PSIM systems?

The answer to this question to me is based around the use case requirement of the customer. A PSIM can mean different things to different people. The American Dynamics victor client, from my perspective, can sit in both camps. It can be a PSIM and an integral building block of PSIM. I say this because the victor client is flexible in its application and deployment. The demarcation is based upon the other systems that it is being integrated with. The whole point of a PSIM, or integrated security solution, is to bring together a collection of security, life safety, building management systems and present, as a minimum, a single interface for Security Operations Centre staff to interact with from a situational awareness perspective, in addition to facilitating action/reaction scenarios across several disparate systems. E.g. a Fire Alarm creates an event to call to screen the map of the area of the fire, the local cameras to view what is happening. Also, to provide the same information retrospectively when assessing an event.

If the predominant eco system of the Fire, Intrusion, BMS, Access Control is from within the JCI portfolio, or from any of JCI's strategic partners, then the victor client provides PSIM functionality. Where the installed systems are very diverse and without cohesion of a single manufacturer or few manufacturers, then an overarching PSIM is a must to provide the one point of monitoring function.

What services does your system(s) provide in relation to the integration of safety and security components and what are the main advantages?

The American Dynamics victor client is first and foremost a Video Management System; there are integrations to our own products and strategic 3rd parties. The integration list can be found here: compatibilitymatrixaws - American Dynamics

Due to the flexibility and scalability of the victor VMS, the solution offered can be diverse when including the integrations. Ultimately therefore, the solution can be Situational Awareness (deliver the right information to the right person at the right time so they can perform their duties accurately and efficiently) based upon video only; or with integrations such as Access Control, Fire, Intruder, the solution becomes more holistic and facilitates the "Single Pane of Glass" philosophy; one point to present the information to enable an operator to focus their attention on a single client

Which users require a PSIM system and which are better served by management systems that cover sub-areas?

This depends upon the operational requirements of the end user. A PSIM particularly serves a customer where they have multiple VMS, multiple Fire, multiple Intruder systems etc. The job then of the PSIM is to ultimately be the front end for all these diverse systems from multiple manufacturers. Where the product poll is either all in-house or where the products are from strategic partner manufacturers, this is when the victor client can act as the front system and manage the action/reaction across the systems.

For which target group (company size, sector, complexity of installation) is your system best suited or where can it best play to its strengths?

The victor client is usually, though not exclusively, the domain of enterprise customers, critical infrastructure, financial entities and similar. Equally it can be deployed in more modest installations. The key is the scalability of the platform. The primary strength is the solution driven approach to the product development; the ability to provide the high level of Situational Awareness already mentioned. Additionally, there are the intrinsic feature sets which facilitate a high level of redundancy (essential for Critical Infrastructure) the open platform approach to integrations; equally important is the customer base's voice of customer feedback drives the product development.

What advice would you give to users who are thinking about introducing a new management system?

Research, research, research! Be very clear on what the needs and expectations are. Integrations between disparate systems are challenging therefore you need to know what the PSIM supplier's policy is with regards to when they update their product in relation to when the integrated products are updated by those manufacturers. A PSIM is not always needed; a single supplier solution for security, life safety and building management can many times provide the functionality needed without the additional expense of a PSIM.

Establish what are the on-going costs, for SSAs and software updates

What advice would you give to users who want to replace their management system?

Basically the same as above question. Also be realistic in what the needs are; if the management system is being replaced however older security / life safety products are not, then this might create integration challenges. Establish what systems the new management system is capable of with regards to product integrations. Do not assume that a management system with a specific protocol, for example BACnet is compatible with another BACnet system. Test and check!

7.4 ARES Security/Vidsys (USA)

ARES Security Corporation is a leading security software company and developer of the Enterprise Security Platform that is proven to reduce costs and increase effectiveness in numerous industries. The Avert software was developed in 1999 in coordination with the Defense and Threat Reduction Agency to protect U.S. Nuclear assets. The solution has been protecting the country's most critical assets since then, and in 2012 ARES Security was established to commercialize and expand the capabilities of Avert.

ARES Security has grown to expand its offerings through a series of acquisitions and advancements to provide a comprehensive suite of solutions that benefit any organization's security and safety operations. The company strengthened its position in in PSIM field by the acquisition of assets and contracts of Vidsys, based in Vienna. Vidsys, now an ARES Security company, provides mission critical Physical Security Information Management (PSIM) software to Government Agencies, Corporate Enterprises, Transportation Agencies and other Iconic Properties in North America, the Middle East, and the Asia Pacific.

Do you see your system as an overarching PSIM system or rather as an integral building block of PSIM systems?

ARES Security's Enterprise Security Platform (ESP) is an overarching solution that goes well beyond the traditional boundaries of physical security information management. It is architected as a comprehensive application-based ecosystem that unifies disparate security, safety, response, and building management subsystems. The ESP is designed to serve as the central intelligence layer, offering advanced functionality such as digital twin modelling, AI-enhanced analytics, and autonomous robotic operations - all of which expand its value beyond that of a typical PSIM system.

What services does your system provide in relation to the integration of safety and security components and what are the main advantages?

The ESP provides seamless integration with over 450 safety, security, building information, and detection systems—including access control, intrusion detection, video surveillance, fire alarms, emergency communication, and building automation. These integrations are enhanced by a user-configurable interface that consolidates alerts, workflows, and automated responses into a single pane of glass.

Which users require a PSIM system and which are better served by management systems that cover sub-areas?

Organizations with complex or large-scale operations—such as critical infrastructure, government agencies, enterprise campuses, airports, and utilities—benefit most from a true PSIM system. These users typically manage numerous disparate systems across multiple locations and require unified oversight, rapid threat assessment, and coordinated response capabilities. Conversely, smaller facilities with limited integration needs or static security environments may find sub-area management systems sufficient. However, as risks evolve and technology matures, many organizations find themselves needing the scalability and resilience that a PSIM platform offers.

ARES Security's Enterprise Security Platform (ESP) incorporates built-in data federation and comprehensive support for standard operating procedures, fully aligned with existing information-sharing policies and organizational hierarchies. This adaptable framework enables the platform to scale efficiently in accordance with an organization's evolving requirements—ranging from localized deployments to enterprise-wide implementations across global operations.

For multinational or geographically distributed clients, ESP's federated architecture empowers individual sites or facilities to operate independently, utilizing tailored integrations and capabilities specific to their operational context. These decentralized implementations are centrally connected, enabling executive-level oversight through a unified dashboard that provides enterprise-wide visibility while preserving site-level autonomy. This architecture also supports advanced security for multi-agency data sharing allowing clients to customize security to match inter-agency (public and private) MOU's down to the element level, including both event and rules based data sharing.

For which target group (company size, sector, complexity of installation) is your system best suited or where can it best play to its strengths?

The Enterprise Security Platform is best suited for mid-to-large enterprises operating in high-risk, highly regulated, or logistically complex environments. Although the platform's ability to effectively scale, enables the solution to be utilized by smaller agencies or organizations as well. ESP's strength lies in its adaptability. It can be deployed in phased approaches or as an enterprise-wide platform and is particularly valuable where integrated command centers, advanced analytics, or autonomous operations (e.g., drone or robotic patrols) are desired.

What advice would you give to users who are thinking about introducing a new management system?

When introducing a new management system, users should begin with a clear understanding of their long-term operational goals and risk profiles. It is essential to choose a platform that is open, scalable, and capable of integrating existing and future systems. It is crucial to prioritize user-friendly interfaces that facilitate rapid onboarding and provide intuitive operation. Additionally, seek out solutions that support automation, simulation, and incident drills to ensure preparedness. It is important to consider not only current needs, but also the future-readiness of the solution—particularly with the anticipated growth of AI, robotics, and digital twin technologies.

What advice would you give to users who want to replace their management system?

For those replacing legacy management systems, it is crucial to ensure data continuity and integration with existing infrastructure. When evaluating vendors, it is essential to consider their proven interoperability and future-forward innovation. It is advisable to avoid one-size-fits-all solutions and instead opt for modular architectures that can evolve with organizational growth. Proper planning for change management, including user training and phased implementation, is necessary. Leveraging the opportunity to replace the system can help unify operations and elevate overall resilience. The Enterprise Security Platform excels in transitions from siloed systems to integrated security ecosystems, offering robust migration support and extensive third-party compatibility.

7.5 Bold Group (USA)

For over 40 years, Bold Group has served the security and alarm industry by providing a comprehensive range of alarm monitoring and integrated financial and business management solutions. These solutions are specifically designed to achieve optimal business performance for central monitoring stations, dealers, and integrators. Bold Group was established in March 2019 through the operational merger of Perennial Software, Bold Technologies, SIMS, and Secure Global Solutions (SGS). The company is recognized as ono of the industry's trusted provider of mission-critical alarm monitoring and financial management technology. They offer flexible, automated solutions that streamline customer workflows, enhance efficiencies, and maintain consistent processes. These capabilities enable critical response services that safeguard life and property.

The product portfolio of Bold Group includes esteemed alarm monitoring systems such as Manitou, stages, and SIMS. These advanced systems are complemented by top-tier accounting and business management systems, including SedonaOffice and AlarmBiller. Their comprehensive suite of solutions is supported by a network of strategic partnerships, technical support, and extensive ongoing training programs.

7.6 Eagle Eye Networks (USA)

Eagle Eye Networks is a global leader in cloud video surveillance and offers an open, true cloud platform that works with artificial intelligence to dramatically transform video surveillance systems into an even more powerful tool. With video AI, the possibilities are limitless for keeping communities secure and engaged, helping business improve operations and customer service, and enabling manufacturers to build higher quality products in safer environments.

Eagle Eye's 100 percent cloud-managed solutions are smart, simple, and secure. The Eagle Eye Cloud VMS (video management system) is flexible enough to power the future of video surveillance and intelligence. Purpose built for the cloud and AI, it addresses customers' security needs with infinite scalability, flexible pricing plans, a wide array of advanced analytics, and an open RESTful API platform for unlimited customization. Founded in 2012, Eagle Eye is headquartered in Austin, Texas, with offices in Amsterdam, Bangalore, and Tokyo.

Do you see your system as an overarching PSIM system or rather as an integral building block of PSIM systems?

Eagle Eye Networks offers a cloud-based Video Management System (VMS) that acts as a key component within a PSIM framework. It does not function as a full PSIM but connects easily with PSIM platforms and other security technologies through open APIs and industry-standard protocols.

What services does your system(s) provide in relation to the integration of safety and security components and what are the main advantages?

Eagle Eye Networks provides cloud video surveillance with integrated capabilities designed to enhance security systems. The platform connects seamlessly with access control systems, alarm systems, and analytics platforms to offer comprehensive security solutions. Key advantages of this system include a cloud-based architecture that eliminates the need for local servers, secure access to live and recorded video from any location, AI-powered search and object recognition features, centralized management for multi-site operations, and open APIs that facilitate connections with third-party systems.

Which users require a PSIM system and which are better served by management systems that cover sub-areas?

Organizations with complex infrastructures and multiple security systems—such as transportation hubs, city-wide installations, and critical infrastructure—require a PSIM. Businesses focused primarily on video, such as retail chains, schools, or small offices, can achieve their goals with a dedicated VMS.

For which target group (company size, sector, complexity of installation) is your system best suited or where can it best play to its strengths?

Eagle Eye Networks is best suited for multi-location businesses such as those in retail, healthcare, logistics, and hospitality. It is also ideal for small to medium-sized enterprises that require quick deployment and scalability. The system is particularly beneficial for organizations with limited IT staff that prefer low-maintenance solutions. Additionally, it serves companies that need centralized video access across multiple sites effectively.

What advice would you give to users who are thinking about introducing a new management system?

Define your goals, list your existing systems, and choose a platform that supports integration, remote access, and future growth. Focus on systems that reduce complexity, improve visibility, and adapt as your business changes.

What advice would you give to users who want to replace their management system?

Start with a clear understanding of what's not working—performance gaps, hardware constraints, or high support costs. Look for systems that simplify infrastructure, protect your investment in existing equipment, and streamline operations from day one.

7.7 Fast Systems (Switzerland)

FAST is a pioneer in the field of digital security and surveillance technologies and is revolutionizing the way organizations and governments protect people, property and assets. The core R&D team of FAST comprises the combined experience of over 150 man-years and 500 000 installed video channels in over 15 000 installations worldwide.

Their TERRA 4D PSIM organizes sensor and system data into structured formats and presents it in a geographical context, enhancing situational awareness in real-time. By analysing sufficient data and patterns, the system provides valuable insights, allowing for quicker correlations and supporting safety officials in decision-making, protocol identification, resource allocation, and determining deployment strategies. Operators can utilize a virtual interface to review events across time and space for enhanced operational understanding.

TERRA 4D is based on a 3D geographical information system, in which a Digital Terrain Model (DTM) represents a three-dimensional elevation layer of the ground. This is complemented by satellite imagery and current and historical aerial photographs.

Do you see your system as a comprehensive PSIM system or rather as an integral component of PSIM systems?

Our TERRA 4D platform provides tools that significantly accelerate response times in control centers and for mobile units, increase efficiency, and reduce operating costs in every phase of situation management. TERRA 4D is manufacturer-independent and supports cross-platform interoperability. The unified user interface enables remote control of other platforms, connected sensors, and subsystems, including air, land, sea, and space-based platforms.

What services does your system provide in terms of integrating security components, and what are the main advantages?

In today's increasingly networked world, system platforms with multiple geographic locations, numerous information sources, and different areas of responsibility are becoming more common. Therefore, seamless integrations are essential for efficient operations such as crisis management, crime prevention, or everyday routine tasks.

The main advantages of our TERRA 4D platform include the prediction of events that affect multiple locations and areas of responsibility, and the ability to respond as quickly as possible. At the same time, TERRA 4D maintains the individual responsibilities of all participants, as well as control over information ownership, ensuring that only relevant information is selected and made accessible to the appropriate operator.

Integrated solutions based on the TERRA 4D platform provide a comprehensive situational picture based on a 3D GIS model that georeferences existing and future data sources. The platform ensures selective distribution of data as needed and offers access to various data services such as environmental information, weather data, news services, and current reports. Additionally, it improves the reporting, response, processing, and resolution of incidents, increases efficiency, and reduces operational costs. With its ability to shorten response times and minimize risks, the TERRA 4D platform represents a forward-thinking solution for complex security requirements.

Which users require a PSIM system, and who is better served with management systems covering partial areas?

A comprehensive PSIM system like TERRA 4D is particularly suitable for users who need a central overview of their security infrastructure, especially in complex environments such as critical infrastructures, industrial facilities, or airports. It is ideal for those who require rapid and coordinated responses to incidents, as the system

provides a comprehensive situational overview and automated workflows. In addition, users who wish to utilize extensive data analyses to detect trends and make informed decisions will benefit. TERRA 4D helps reduce system complexity and increase efficiency by centralizing processes and avoiding redundant tasks. The system is also flexible and scalable, making it particularly suitable for organizations planning future expansions and technologies.

Management systems that cover specific areas are particularly suitable for smaller companies with only specific and isolated security requirements, such as simple video surveillance. They are sensible when the security infrastructure is straightforward and does not require networking, or when the budget does not allow for comprehensive integration. The choice between a PSIM system and a specialized solution ultimately depends on the individual needs, the complexity of the security requirements, and the long-term goals of the user. Our experience shows that integrated platforms like TERRA 4D, with their centralized control, improved efficiency, and scalability, are especially convincing in demanding environments.

For which target group (company size, sector, installation complexity) is your system best suited, or where can it best play to its strengths?

TERRA 4D is optimally suited for medium-sized to large companies and corporations in industries with high security requirements and complex infrastructures. This includes, in particular, critical infrastructures (KRITIS), industry, logistics, public institutions, and authorities. The strengths of TERRA 4D come to the fore in demanding integration projects with heterogeneous system landscapes that require centralized situational awareness, automation to increase efficiency, and enhanced security. TERRA 4D offers scalability, flexibility, and the possibility of individual customization for organizations aiming to future-proof their security.

What advice would you give users considering the introduction of a new management system?

Introducing a new management system is a strategic step that should be well thought out. FAST Systems recommends that users review the provider's expertise through references and customer feedback and look for a future-proof, scalable platform. A phased implementation with a pilot project makes the introduction easier and reduces risks. Clear objectives, user-friendliness, as well as the highest standards of data security and compliance are crucial for long-term success.

What advice would you give users who want to replace their management system?

It is essential to clearly define the weaknesses of the current system and precisely formulate the objectives of the new system. Likewise, the integration capability of the new system with the existing infrastructure should be thoroughly examined to avoid possible problems. A phased introduction helps to reduce risks and increase user acceptance. User-friendly design plays a key role as it reduces training requirements and increases user efficiency. For long-term future security, it is advisable to choose a provider with a clear development strategy and a focus on new technologies. Finally, the partner should have extensive experience and in-depth industry know-how to ensure a smooth transition.

7.8 Funkwerk (Germany)

Funkwerk Security sees itself as a solution developer and system integrator for innovative security technology. With over 50 years of experience and a team of experts, the company offers comprehensive cross-industry solutions, covering all project steps from consulting and planning to system technology selection, installation, service, maintenance, and continuous further development of the installation.

Do you see your system as a comprehensive PSIM system or rather as an integral component of PSIM systems?

ViPRO.gms 5 KRITIS is an independent, comprehensive PSIM system that brings together all security-relevant systems on a central platform. It meets the highest requirements for availability, IT security, and the precise mapping of processes. The solution addresses both operational efficiency and regulatory requirements in security-critical environments.

What services does the system provide regarding the integration of security components, and what are its main advantages?

The PSIM system ViPRO.gms 5 KRITIS takes on the central integration and control of a wide variety of security and building technology components within a uniform platform. These include, among others, video surveillance systems, fire alarm systems, access control systems, intrusion detection technology, and communication systems. All information from these systems is brought together in predefined process logics, visualized, and transferred into automated or manual action scenarios.

The key advantage lies in the standardization and centralization of the user interface: operators, especially with changing personnel such as security services, no longer need to be trained on various different systems. Instead, all security-relevant information and control options are available in a uniform and clear format. This increases response speed, minimizes sources of error, and significantly reduces personnel costs for training and operation.

A unique selling point of ViPRO.gms 5 KRITIS is that as a manufacturer, we offer three central software solutions – PSIM, video management, and communication systems – from a single source, all fully integrated. In contrast to solutions where external systems are connected via interfaces, our software platforms are directly linked. This enables an especially stable, high-performance, and future-proof system architecture in which all modules are optimally coordinated with each other.

Which users require a PSIM system, and who is better served with management systems covering partial areas?

Our solutions are mainly used in the context of Critical Infrastructures (KRITIS). In these areas, the need for an overarching, central control and monitoring platform is clearly defined and often required by law and regulation. The use of a PSIM system is indispensable here, as it is a matter of centrally bringing together, evaluating, and quickly controlling a wide variety of security-relevant systems from different trades.

Management systems that only cover partial areas can be useful and sufficient in less security-critical environments, such as in an office building where mainly access control is to be combined with video surveillance. This also applies to smaller industrial plants without high security requirements, where individual subsystems such as video management systems (VMS) or building management technology are sufficient.

For which target group (company size, sector, installation complexity) is your system best suited, or where can it best play to its strengths?

Our PSIM system unfolds its strengths especially in facilities assigned to critical infrastructure and NIS2 – infrastructures with high complexity, security-critical requirements, and decentralized structures. These mainly include facilities and companies subject to the KRITIS regulation and the NIS2 directive. Typical users are operators in the fields of energy supply, water management, healthcare, transport and traffic, as well as government institutions.

What advice would you give users considering the introduction of a new management system?

Our most important advice for users: Choose a manufacturer who not only supplies the software but also takes responsibility for planning, installation, and commissioning of the system from a single source. Especially PSIM systems are highly complex and require, besides profound knowledge of classic security technology, extensive know-how in IT security, network technology, process control, and system-specific characteristics. This expertise usually lies with the manufacturer itself and can hardly be ensured through sole partner or distributor models.

Equally crucial for smooth and future-proof operation is the IT competence of the provider. Most practical challenges arise at the interface between security and IT systems. Our many years of experience have shown that integration and operational problems frequently occur precisely at this interface. When introducing a PSIM system, the focus should not only be on the software solution itself, but on a competent, experienced, and IT-oriented manufacturer who plans, delivers, integrates, and provides long-term support for the system – ideally, all from a single source. The management system should map the individual operating processes – not the other way around.

What advice would you give users who want to replace their management system?

A management system switch is a sensitive and complex process that should be well prepared, both technically and organizationally. Customers should allow enough time for thorough consultation and intensive preparation. A PSIM or management system should not only integrate technology, but above all map and efficiently support the operator's individual processes. Therefore, we recommend early and direct consultation with the manufacturer and a detailed explanation of your own processes and requirements.

7.9 Genetec (Canada)

Genetec is a leading provider of intelligent and innovative networked security products, services and solutions, whose vision from the outset has been to reduce the redundancies created by the use of numerous different security systems. Based on customer feedback, it became clear that the integration of individual security products involved considerable time, cost and effort for maintenance and upgrades. Against this backdrop, a physical security platform was created that brings together multiple products so that they function as a unified system.

Genetec Mission Control is a decision management system that helps to understand unfolding events and quickly identify the best course of action. It simplifies the response coordination between stakeholders, speeding up incident resolution.

Security Center SaaS is a unified physical security solution that one can choose to deploy in the cloud or as a hybrid solution. It unifies access control, video management, forensic search, intrusion monitoring, automation, and many other advanced security capabilities.

Do you see your system as a comprehensive PSIM system or rather as an integral component of PSIM systems?

Genetec Security Center is not a classic PSIM system in the traditional sense. Genetec Security Center is a complete, unified security system that transcends the traditional boundaries of a PSIM. It natively integrates video surveillance, access control, automatic license plate recognition, communication, intrusion detection, and more within a single platform. The system was conceived from the ground up as a unified solution that evolves with organizational needs.

What services does the system provide regarding the integration of security components, and what are its main advantages?

Security Center integrates numerous security components on a common platform, going beyond mere event monitoring: Security Center is designed to centrally consolidate data – for effective management of security policies, monitoring ongoing processes, and conducting informed analyses. This allows organizations to benefit from improved situational awareness, unified command and control functions, and easier system administration and scalability.

Which users require a PSIM system, and who is better served with management systems covering partial areas?

Genetec Security Center is scalable and modularly expandable. It can initially be used as a stand-alone video management or access control system. Customers can expand it to a full security platform according to their needs, budgets, and at their own pace. This makes it suitable, unlike conventional PSIMs, not only for organizations with complex operations but also for users who initially want to set up smaller structures, but are planning for future growth.

For which target group (company size, sector, installation complexity) is your system best suited, or where can it best play to its strengths?

Genetec Security Center is suitable for organizations of any size, especially for industries with increased security requirements such as banks, energy and utilities, cities and municipalities, airports, data centers, educational institutions, healthcare, public safety, retail, gaming, transportation, and event venues. The system's strengths are best revealed in organizations with multiple locations, complex installations, and a need for central management. Thanks to its unified architecture, even smaller setups – for example, with 40 cameras and 30 access readers – benefit from the comprehensive functions.

What advice would you give users considering the introduction of a new management system?

Don't wait too long – new legislation like the KRITIS umbrella law or the NIS2 directive is massively driving modernization in security and cybersecurity. Before introducing a new system, security managers should thoroughly assess their own requirements: Which functions are needed now and in the future? What integration of existing systems is required? Genetec recommends relying on open, scalable platforms. Another important parameter is provisioning: The cloud has long arrived in most areas of business – yet security departments still lag behind compared to other units. Whether as a complete cloud or hybrid solution, there is great potential here: more security, high scalability and permanent availability, as well as the ability to utilize data potential even more effectively.

What advice would you give users who want to replace their management system?

A transition should be planned in a targeted manner. Important factors include the migration capability of existing devices and data, adherence to operational processes during the transition, and openness to future expansions. Unlike closed, proprietary systems with limited compatibility and no update guarantee, organizations using open-architecture solutions can integrate a wide variety of cameras, analytics tools, and other devices. When selecting the new solution, preference should be given to systems that consider cybersecurity and data protection from the outset. Careful planning and collaboration with experienced partners will facilitate the transition and ensure operational continuity.

7.10 Gretsch-Unitas (Germany)

Since 1990, ela-soft – a company of the Gretsch-Unitas Group – has been developing the manufacturer-neutral building management system GEMOS PSIM. Since 2019, GEMOS has been distributed by BKS. The system enables the manufacturer-independent management of a wide range of media, communication, and security systems, such as fire alarm systems, hold-up and intrusion alarm systems, video surveillance systems, access control systems, extinguishing and smoke extraction systems, and much more. With GEMOS, all technical installations are integrated via a central, user-friendly interface.

GEMOS is a manufacturer-independent PSIM system that integrates numerous security, media, and communication systems. It provides a central platform for monitoring and controlling security-related subsystems, such as fire alarm, video, and access control systems. The open architecture and standard protocols enable seamless integration into higher-level systems. It supports both hazard prevention and the fulfillment of increased requirements resulting from laws such as NIS-2 and the KRITIS umbrella law, which strengthen IT security and resilience.

What capabilities do your system(s) offer for integrating security components, and where are the main advantages?

GEMOS monitors, detects, and transparently displays all security information and events (malfunctions, alarms, and other states) of all integrated physical security and information systems (GEMOS interfaces). GEMOS, which we refer to as a building management and organizational system, is more than just a technical means of bundling information. It organizes central monitoring, processing, and visualization of extensive security information from various industries into an independent risk management system. The system provides a holistic view (what-when-where) of all security events. This significantly increases efficiency in monitoring, detecting, and responding to security incidents.

GEMOS offers modules that can be tailored to individual security requirements. Key benefits include manufacturer-independent integration of subsystems, platform independence with support for both Windows and Linux, and a customizable graphical interface. The web-based operation allows use without additional software installation, while central data storage ensures all information is saved on the GEMOS server.

The GEMOS “Enterprise One Server” guarantees operational reliability for security technology. Real-time data exchange is encrypted in accordance with BSI standards using TLS 1.3 and AES-256. Automatic data synchronization between GEMOS servers provides additional security through monitored and encrypted replication.

Which users require a PSIM system, and who is better served with management systems covering partial areas?

The choice between a PSIM (Physical Security Information Management) system and specialized partial management systems depends on individual requirements. Typical PSIM users come from the following fields: industry, finance, smart building, healthcare, data centers, energy suppliers, trade, public institutions, education and research, justice, logistics, transport, and event complexes.

The upcoming NIS-2 Implementation and Cybersecurity Act (NIS2UmsuCG) will require around 30,000 companies in Germany to increase resilience, especially in the physical security of critical infrastructures. Operators of critical infrastructures (KRITIS) in eight sectors must expect stricter requirements and regulated standards. Currently, there are 1,132 registered operators with 2,095 facilities, but the number of affected companies will increase significantly due to legal adjustments and expanded sectors.

For which target group (company size, sector, installation complexity) is your system best suited, or where can it best play to its strengths?

GEMOS is suitable for companies of any size. Small businesses can use simple solutions, while large corporations can centrally control complex systems. It is modular and scalable, with functions that can be adapted to requirements.

The system is particularly designed for security-critical sectors such as critical infrastructures, correctional facilities, or data centers. It offers cross-system interactions, intuitive operation, and flexible customization options.

With over 750 interfaces, GEMOS is a leading manufacturer-neutral building management system in Germany. The web-based interface allows for individual operating concepts, graphical adjustments, and direct integration of building floor plans. Alarm handling, workflow management, and comprehensive logs are core functions. GEMOS ensures maximum availability with redundancy concepts such as network and server fail-safes.

What advice would you give users considering the introduction of a new management system?

A manufacturer-neutral building management system like GEMOS offers high security, efficiency, and future viability. Clear objectives should be defined: central control, process automation, infrastructure resilience, or regulatory compliance. An analysis of the current system landscape is necessary to identify existing subsystems and weaknesses. Future-proofing and scalability should be considered, as well as training for staff to use the system effectively.

What advice would you give users who want to replace their management system?

A system change should be well considered. Risk analyses must be carried out continuously and adapted to current threats. In many cases, a targeted upgrade or functional expansion can achieve the desired result without a complete system replacement. GEMOS offers a future-proof platform that grows with the company's requirements. It is advisable to contact a GEMOS partner or BKS GmbH directly to make informed decisions and protect investments.

7.11 Hexagon (Sweden)

Hexagon's Safety, Infrastructure & Geospatial division announced the expansion and rebranding of its portfolio of physical security solutions to HxGN dC3. The new name, which stands for Detect, Command, Control and Collaborate, reflects the company's approach to protecting people, property and assets by supporting the entire lifecycle of an incident to minimize its impact.

Since acquiring leading physical security solution provider Qognify in April 2023, Hexagon has been extending and integrating its offerings into the broader Hexagon ecosystem. The newly expanded portfolio will continue to serve as a platform for growing Hexagon's footprint in the physical security space.

New to the portfolio is the AI-enhanced HxGN dC3 LidarVision (formerly Accur8vision), a 3D surveillance system based on volumetric LiDAR detection technology. It goes beyond traditional perimeter protection to secure entire areas instead of just the fence line, with the ability to track intrusions even in low light and classify objects using Hexagon's proprietary AI neural network, DeepTection.

The portfolio also includes HxGN dC3 Video (formerly Qognify VMS), an open-platform video management software (VMS), and HxGN dC3 Orchestrator (formerly Situator), an enterprise-class physical security information management (PSIM) software. Solutions for advanced video analytics, forensic search and centralized management and monitoring of multi-site physical security systems complete the HxGN dC3 core portfolio.

Do you see your systems as comprehensive PSIM or rather as an integral component of PSIM systems?

The HxGN dC3 Orchestrator acts as a comprehensive PSIM, while HxGN dC3 Video is an essential component of PSIM systems.

What capabilities do your systems offer for integrating security components, and where are the main advantages?

Hexagon provides a "single pane of glass"—meaning the visualization of information from diverse subsystems in one interface with uniform usability. By merging and combining information, users gain improved situational awareness. The addition of incident-related data is made possible by standardized, dynamic input forms that enable structured and unified collection of relevant information. The system guides users through the optimal response process with digitized Standard Operating Procedures (SOPs), supporting efficient and standardized incident handling.

Which users require a PSIM system, and who is better served with management systems covering partial areas?

A PSIM system is especially significant for organizations with a central security control center. It is also suitable for companies operating numerous subsystems—especially systems of the same type from different manufacturers, such as various video management systems (VMS).

For which target group (company size, sector, installation complexity) is your system best suited, or where can it best play to its strengths?

The system's strengths are most evident in the enterprise environment, i.e., for larger organizations with a complex technological ecosystem. This includes sectors such as transportation (rail and air), large corporate campuses, and urban infrastructures.

What advice would you give users considering the introduction of a new management system?

When introducing a management system, security goals and the derived use cases should always take center stage—the choice of technology should follow from this. It is also important to think in terms of processes: aggregated information is helpful but should always be viewed in the context of incident and event response. Another important step is mapping existing technologies and subsystems and matching them with available or to-be-developed interfaces. Finally, involving users early in the system and information design is crucial to achieve acceptance and real value creation.

What advice would you give users who want to replace their management system?

Before replacing an existing management system, users should carefully consider what additional features and use cases they expect from a new system. It is also important to determine which shortcomings users see in the current system and what specific improvements they expect from a new solution. Another key aspect is thoroughly checking whether and to what extent the available subsystems are supported by the new system. Finally, it is essential to involve users early in the system and information design to foster acceptance of the new system and ensure sustainable value creation.

7.12 Hikvision (China)

Hikvision provides advanced Physical Security Information Management (PSIM) solutions that integrate video surveillance, access control, and alarm systems into a centralized platform. Their AI-powered analytics enhance security monitoring and incident response for businesses and critical infrastructure.

Hikvison's HikCentral Professional Series provide modular platforms for common business applications, including Video, Access Control, Attendance, and more. While featuring their own functionalities, those applications also offer flexible combination to meet the needs of a broad range of custom scenarios like yours. Moreover, the application modules all come with the same interface design for the series platforms, greatly reducing learning requirements for the various systems.

7.13 Honeywell (USA)

Honeywell (US) offers advanced Physical Security Information Management (PSIM) solutions in their Honeywell Building Automation offering that integrate surveillance, access control, and alarm management into a unified platform. Their systems enhance situational awareness and streamline security operations for critical infrastructure and enterprises.

Honeywell's WINMAG plus (V06) offers a new common user interface with improved menu and user guidance, a new, more flexible pay-as-you-go licensing model, and a new software architecture, making it a powerful, scalable solution with easy integration and compliance with compliance standards.

In addition, WINMAG plus V06 offers extended support for drivers for fire and intrusion alarm systems, video and access control systems, escape route technology/escape door control and voice alarm systems from Honeywell, as well as the integration of systems from various third-party manufacturers.

The new software architecture of WINMAG plus V06 is suitable for both high-end private properties and global enterprise solutions with distributed locations. An important functional enhancement for installers is the simplified creation of workflows and a customisable user interface.

WINMAG plus V06 manages and visualises burglar alarm technology, fire alarm technology, access control technology, video technology, escape route technology/escape door control under a common user interface. Messages are displayed graphically or in text form.

7.14 Integrated Systems (ISS) (USA)

An ISS provided PSIM will allow organizations to integrate and control multiple disparate security applications and devices through one comprehensive user interface. The system empowers security personnel to identify and proactively resolve technology-systems related situations. All of the video, access control, sensors, analytics, networks, building systems, etc. can be integrated into a PSIM System that enables numerous organizational benefits, including increased control, improved situational awareness and management reporting. In addition, an ISS PSIM solution will allow organizations to reduce costs through improved efficiency and to improve security through increased intelligence.

7.15 Milestone Systems (Denmark)

Milestone Systems is a leading global provider of video management software (VMS) headquartered in Brøndby, Denmark. The company has been part of the Canon Group since 2014. Its product portfolio includes the XProtect video management software (VMS), the advanced BriefCam analytics platform and the Arcules video surveillance as a service (VSaaS) solution. Milestone facilitates the centralisation of cameras, sensors and locations and unlocks the full potential of video data. The manufacturer develops open platform solutions for IP-based video surveillance that are particularly valued for their scalability, interoperability and user-friendliness. Milestone's solutions are used in numerous industries, including critical infrastructure, transport, retail, education, healthcare and city surveillance.

In the field of video management software (VMS), Milestone offers a modular platform with its main solution, XProtect, which supports both small installations and large-scale, complex systems. XProtect enables the integration of a wide variety of cameras and sensors from different manufacturers and offers functions such as live view, recording, event management, AI-supported analysis functions and scalable system design.

Strictly speaking, Milestone does not offer a complete physical security information management system. However, thanks to its open architecture, XProtect can be easily integrated with other security systems (e.g. access control, fire alarm systems, building automation) and thus serves as a central visualisation and control platform. In combination with partner solutions from the Milestone ecosystem, XProtect can therefore also be used in extended PSIM scenarios, especially when it comes to consolidating and displaying security-related information in a central interface.

7.16 Nanodems (USA)

Nanodems offers an industry-leading, intelligent platform that seamlessly integrates all components of physical security into one converged platform. Centralized command and control along with automated monitoring, enhances operational efficiency and safety whilst reducing risks and costs. The easily extensible open architecture platform helps users to utilize their existing infrastructure as well as making your organization future proof.

Nanodems NDIS platform delivers these critical infrastructure entities an intelligent PSIM solution, which converges and unites all disparate physical security systems to provide a centrally managed command and control station. The platform seamlessly tracks and monitor all systems including perimeter, intercom, ACS, CCTV, UVIS, ANPR, access control und intrusion alarm and radar systems.

7.17 Network Harbor (USA)

Network Harbor supplies PSIM systems for use in government, commercial, military, and educational environments. Its products include tools for video surveillance, audio networking and recording, network monitoring, personnel management, physical access enrolment, and integration platforms such as LightHouse.

LightHouse is structured to combine these elements, along with compatible third-party systems, within a single framework. The development of the LightHouse PSIM system involved more than fourteen years of research and testing focused on quality assurance. The PSIM aims to integrate security components into one interface and provides operational control through a unified platform. It is compatible with a variety of internal and external security devices. The PSIM has been deployed across multiple sectors, including federal, military, energy, municipal, and commercial locations.

7.18 Persistent Sentinel (USA)

Persistent Sentinel has more than 19 years of experience developing Physical Security Information Management (PSIM) software for civilian and government security solutions. The HiRSA software's versatile design is applicable for security applications in various domains: installation, maritime and port security, and anti-terrorism. It combines intelligent agent software technology with existing communications infrastructures to produce a robust network to detect and counter suspicious and criminal/hostile activity.

The HiRSA PSIM solution offers essential capabilities including event collection, analysis, verification, resolution, reporting, and audit trails. HiRSA provides a detailed Common Operating Picture (COP) with sensor locations visualized over satellite imagery, offering operators a comprehensive security overview. Key features include integration of any sensor or surveillance system, even legacy technologies. It is a customizable and scalable software that collects and analyses data to create a high-resolution COP. It enhances real-time event management, generates tailored alerts and actions, and improves data management and video recording capabilities.

7.19 Primion (Germany)

Primion Technology is a German company that plays a significant role in the field of security technology, particularly in the areas of access control, time recording and hazard management systems. The company offers integrated solutions that are used in security-critical areas such as industry, public authorities, healthcare, airports and data centres. Primion's SecurityManagement (pSM) is a security control room system that is recognised by VdS and combines various security systems on a single platform. With scenario planning, processes can be automated in advance and manual interventions are supported by workflow scenarios. The mobile app enables location-independent control. The solution offers uniform security management for comprehensive security and combines access control, fire alarm, video surveillance and many other security functions in a single system. It enables centralised control, ensuring a faster and more effective response in emergencies.

Do you see your system(s) as an overarching PSIM system or rather as an integral building block of PSIM systems?

At Primion, we see ourselves as a solution provider that offers both: essential building blocks such as Access Control systems, and a full PSIM application for monitoring and interacting with a wide range of integrated systems. This dual capability allows us to cover key aspects of converged security and deliver tailored solutions to meet the unique needs of each customer – whether they require standalone components or a comprehensive PSIM platform.

What services does your system(s) provide in relation to the integration of safety and security components, and what are the main advantages?

Our Access Control solutions ensure physical security for buildings, rooms, and sensitive areas – down to individual lockers or server racks – by granting access only to authorized personnel at any given time. In combination with pSM, our PSIM application, system statuses can be monitored in real time, alerts routed to the appropriate staff, and manual interventions executed instantly when needed. pSM creates a centralized interface that provides full situational awareness by integrating and visualizing a wide range of systems. Whether it's remotely unlocking a door or disabling a smoke detector during maintenance, users benefit from a consistent, intuitive experience. By aggregating data from fire and intrusion detection systems, video surveillance, and even IoT devices such as temperature or flood sensors, the system paints a clear, consolidated picture of potential threats – rather than overwhelming users with isolated alerts and fragmented information.

Automatically displaying live video feeds from areas where alarms are triggered allows for rapid assessment of the situation. In some cases, cameras themselves can initiate alarms, for example by detecting trespassing or unusual behaviour in predefined zones.

Which users require a PSIM system and which are better served by management systems that cover sub-areas?

Subsystems like Access Control or Intrusion Detection often work well as stand-alone solutions, and many already offer basic features such as alarm notifications. For smaller installations or environments with minimal interaction, operating these systems in isolation can be sufficient. However, we increasingly see customers adopting PSIM systems even when managing a single subsystem. For example, displaying all smoke detectors on a digital floor plan significantly enhances usability and situational awareness compared to interacting directly with the device itself.

The more complex the infrastructure and the more subsystems involved, the greater the value of a PSIM solution. With pSM, users gain a centralized view of all alarms and events, can assign or escalate tasks within their team, and avoid the need for extensive training across different systems. By abstracting and visually representing data –

regardless of its source – PSIM simplifies diagnostics and decision-making, enabling teams to focus on the incident rather than the system behind it.

For which target group (company size, sector, complexity of installation) is your system best suited or where can it best play to its strengths?

As mentioned earlier, the true strength of pSM lies in its ability to integrate multiple systems and streamline operations across diverse environments. The more subsystems are connected, the more significant the benefits – from guided decision-making to automated workflows. Even small businesses can benefit: for example, pSM can provide a quick overview of all open doors and windows before locking up at the end of the day. Medium-sized companies, which may not have full-time monitoring staff, appreciate automated alerts and process controls.

For large enterprises and critical infrastructure operators, pSM delivers centralized control over complex security architectures. It enables the monitoring and management of all infrastructure components through a single interface – a task that would otherwise require multiple specialists.

Thanks to its intuitive visualizations and the ability to flexibly navigate camera footage and respond to alerts in real time, staff can proactively intervene before incidents escalate. Whether managing hundreds of sensors at a major facility like an airport or connecting multiple remote sites, pSM scales effortlessly.

What advice would you give to users who are thinking about introducing a new management system?

“Start small – and grow with it.” While the ultimate goal may be to integrate all relevant systems into a PSIM platform, even incremental steps can deliver immediate value. Connecting just one or two key systems early on helps users familiarize themselves with the interface and quickly experience the benefits: such as centralized alerts, streamlined workflows, or improved situational awareness.

Thanks to the modular design of pSM, additional systems can be integrated at any point and will instantly benefit from existing processes like automated notifications or alarm routing. For example, starting with emergency buttons in elevators might later evolve into integrating CO_2 sensors or temperature alerts; all within the same ecosystem and leveraging the same established response workflows.

What advice would you give to users who want to replace their management system?

“Think big – and think ahead.” If you’re already familiar with the advantages of centralized management systems, a system replacement is the perfect opportunity to explore what more is possible. It’s often the less obvious integrations, such as linking CO_2 or air quality sensors, that provide crucial insights.

In the case of a smouldering fire, for instance, early CO_2 detection could be critical even before a smoke detector reacts.

A modern and flexible platform like pSM enables users not only to detect and manage incidents more effectively, but in many cases even to prevent them by intelligently combining data from various sources to form a more complete picture.

Replacing a system also means revisiting your risk landscape. It’s an ideal moment to reassess current and emerging threats – including cyber risks, which increasingly overlap with physical security concerns. Preparing for these challenges in advance helps ensure that your staff can respond confidently, even under pressure.

7.20 Prysm Software (France)

Prysm Software has been part of the Vitaprotech Group since 2022 and specialises in software solutions for security applications. With AppVision, the company provides a PSIM platform for security, protection and technical management systems. This platform is open, scalable and neutral, enabling the integration and control of devices and applications via a central interface. AppVision can be used regardless of project size or complexity. Targeted training provides partners with the knowledge they need to implement and further develop the solution independently. This ensures that the solution meets the current and future requirements of end users.

Do you see your system as an overarching PSIM system or rather as an integral building block of PSIM systems?

AppVision is a software platform designed for interoperability. It is fully customizable and can be used as a Physical Security Information Management (PSIM) system, but its applications extend far beyond that. It can function as a hypervisor, a supervision system, a building management system (BMS or BOS), a command and control system, a crisis management system, or even a Security Information and Event Management (SIEM) system. AppVision unifies the management of diverse systems for safety, security, IoT, and energy. It aggregates data to create comprehensive solutions and develops tools like scenarios, workflows, reports, and dashboards tailored to specific needs. Its interfaces are customized for different roles, enabling effective operation. Alarms are managed with workflows, severity controls, and histories for review. Real-time visualization and support for 2D, 3D, or GIS maps enhance operational oversight and navigation.

Which users require a PSIM system and which are better served by management systems that cover sub-areas?

Users who require a PSIM system are security operators needing real-time operation capabilities, security managers looking for effective reporting tools, and facility managers aiming to manage energy consumption and predict maintenance operations. Such systems enhance decision-making by providing a unified vision and global supervision across diverse operational needs.

For which target group (company size, sector, complexity of installation) is your system best suited or where can it best play to its strengths?

Thanks to its adaptability and customization capabilities, AppVision can meet the requirements of all vertical markets, all kind of customer. We have a proven experience. However, the more heterogeneous systems there are to federate, the more our system will have its place. I would say that AppVision best suits to smart & safe cities, to prisons, to data centres, to smart-buildings, to multi-sites companies.

What advice would you give to users who are thinking about introducing a new management system?

Choose an off-the-shelf product (not a specific development for each project), open, vendor-neutral and customizable. Open means that you are able to develop connectors to third-party systems if you have the technical capability within your team. It's a way to avoid being locked in by a supplier at the slightest request for development. The system should be vendor-neutral in order to have the freedom of choice in products and technologies you want to deploy, and also to enhance existing infrastructures. Customizable to accommodate the unique requirements of each vertical market. It is also important to purchase software maintenance to receive regular updates for features and security.

What advice would you give to users who want to replace their management system?

It is the software that must adapt to the uses of the site, and not the uses of the sites that must adapt to the way in which the software is designed to be used. Regarding project management, our advice is to plan a test environment, and do not neglect functional analysis.

7.21 SureView Systems (USA)

The SureView Suite from SureView Systems is a Physical Security Information Management (PSIM) platform delivered as Software as a Service (SaaS), offering three software tiers intended to support the management of physical security programs.

It provides a single interface to coordinate alarms and events received by a Security Operations Center (SOC) from any system, device, or source in real time. Response capabilities enable SOC teams and field staff to connect, providing situational awareness, and real-time location and status updates for personnel and assets.

Field operations include incident tracking and investigation tools that support record-keeping, compliance, and efficient communication between operations and investigation teams.

7.22 Veracity Solutions (Scotland)

With a comprehensive product range, rich in innovation, Veracity provides critical components, sub systems and completely integrated solutions. These are developed for targeted market segments across multiple industry verticals, including critical national infrastructure sites and other high end security applications.

Veracity's Integrated Security Management Systems enable the management and control of multiple physical security and related systems. Sometimes called PSIM (Physical Security Integration Management) systems, they provide a centralised and comprehensive view of an organisation's security infrastructure, enabling better situational awareness and efficient incident management.

The Veracity group of companies acquired VMS Ltd in 2019 after many years of close cooperation, allowing it to offer a wider range of security system solutions backed by additional resources and personnel. At the beginning of April 2022, the Company name was changed to Veracity Solutions Ltd, to reflect the tighter integration within the Veracity group of companies, and indeed tighter integration of the increasing range of Veracity products with their PSIM solutions.

8. About the Author

Dr Heiko Baumgartner

Freelance journalist with a strong focus on life science, security and chemistry

Thanks to his extensive experience as Publishing Director at a leading international science publisher and his expert knowledge as Editor-in-Chief in various specialist editorial offices, Heiko Baumgartner builds a bridge between innovations and technologies and their practical applications

www.heikobaumgartner.com
https://www.linkedin.com/in/dr-heiko-baumgartner-b85853a/

Rechtliche Hinweise[1]

[1] Rechtliche Hinweise

For experts.
By experts.
With experts.

Our content thrives on different perspectives. Curious?

To platform

Join us!

Do you have any questions, ideas or would you like to contribute something?

Please contact us – we look forward to hearing from you!

Johanna Krumbiegel
Media Relations Manager Building. Technology. Solutions.
Phone +49 69 75 75 - 52 20
johanna.krumbiegel@messefrankfurt.com

Rebekka Wolz
Coordination Building. Technology. Solutions.
Phone +49 69 75 75 - 62 72
rebekka.wolz@messefrankfurt.com