Physical Security Information Management

Timely and Efficient Situation Management Using Data Fusion, Rules and Workflows, and Simulation with 3-D Modeling

July 2011

VERINT
VIDEO INTELLIGENCE SOLUTIONS™

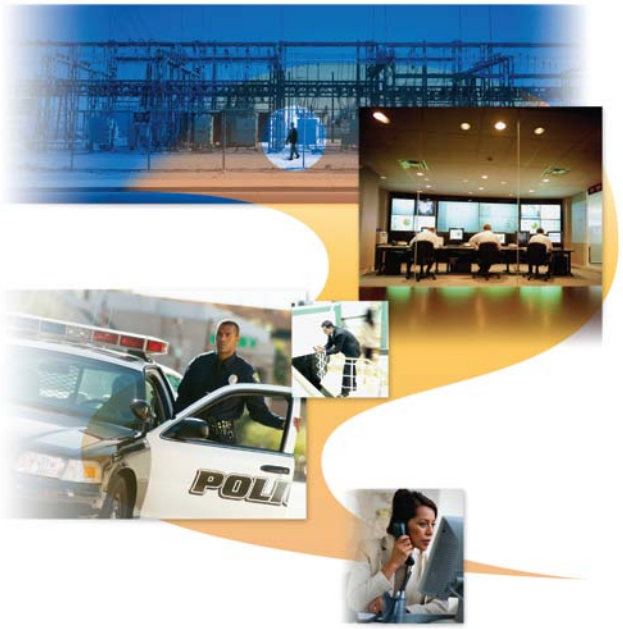
VERINT
VIDEO INTELLIGENCE SOLUTIONS™

Table of Contents

VERINT
VIDEO INTELLIGENCE SOLUTIONS™

Executive Summary

Critical infrastructure — transportation networks, hospitals, schools, power plants and more — underpins a nation's entire economy. Threats to this infrastructure are the highest they've been since 9/11/2001, according to Senior Homeland Security department officials. Yet the systems that agencies and organizations have traditionally used to secure this infrastructure often do not adequately mitigate these risks. While these solutions capture vast quantities of information, bringing all this data together in a manner that allows an organization to quickly identify real threats and respond intelligently has proven a complex and arduous process.



This white paper describes how Physical Security Information Management (PSIM) systems can simplify security management by consolidating security information to deliver more complete and *actionable* security intelligence. PSIM systems help position organizations to respond to security incidents more efficiently and intelligently, while reducing costs and improving compliance.

About Verint Video Intelligence Solutions

Verint® Video Intelligence Solutions™ is a leading global provider of networked video solutions designed to enhance the security of people, property and assets. Verint's award-winning Nextiva® portfolio features IP video management software, video analytics, a physical security information management system, encoders, cameras, wireless devices and intelligent network video recorders for use across a variety of vertical market environments. Open, standards-based and IT friendly, Nextiva helps organizations realize the benefits of IP video leveraging their legacy video investments.

Verint. Powering Actionable Intelligence®.

Verint Systems Inc. (NASDAQ: VRNT) is a global leader in Actionable Intelligence® solutions and value-added services. More than 10,000 organizations in over 150 countries use our workforce optimization and security intelligence solutions to improve enterprise performance and make the world a safer place. Verint is a member of the US broad-market Russell 3000 Index. For more information about Verint, visit www.verint.com.

VERINT
VIDEO INTELLIGENCE SOLUTIONS™

Securing Critical Infrastructure: Challenges Today

Heightened Threats to Security

The functioning of a nation's economy depends on the proper operation of its critical infrastructure—airports, seaports, petrochemical plants, power plants, pharmaceutical manufacturers, water treatment plants, transportation networks, bridges and tunnels, hospitals, universities as well as government and military facilities.

Yet threats to this infrastructure are considerable. In February of 2011, Senior Homeland Security department officials warned that the U.S. terrorism threat was at its highest level since 9/11/2001.[1] Threats include greater numbers of foreign terrorist groups, a sharp increase in extremists in the country, and "lone wolf" operators. At the same time, the biggest threats to security in Europe come from jihadist groups operating within Europe, as well as al-Qaeda, the Taliban, and other allied groups based in Pakistan. These groups are training to mount assaults of the type that killed 163 people in Mumbai in 2008.[2]

Growing Compliance Requirements

In the United States, the U.S. Department of Justice responded by requesting $300.6 million in program increases to strengthen national security and counter the threat of terrorism.[3] The U.S. government has also implemented numerous regulations and guidelines that require compliance. Among these are the:

- Chemical Facility Anti-Terrorism Standards (CFATS) to protect chemicals and the facilities involved in their manufacture
- Maritime Transportation Security Act (MTSA) to protect ports, vessels and related cargo
- North American Electric Reliability Corporation (NERC) to protect systems used at facilities involved in electric energy
- Clery Act/Higher Education Opportunity Act to initiate emergency response following the confirmation of a significant emergency or dangerous situation

---

`[1] "U.S. terrorism threat at 'heightened' state" by Richard Serrano, Los Angeles Times, Feb 9, 2011
[2] "Current Security Threats to Europe," by Neil Doyle, Atomic News, March 18, 2011
[3] "U.S. Department of Justice, FY 2011 Budget Request," http://www.justice.gov/jmd/2011factsheets/pdf/national-security-counter-terrorism.pdf

Siloed Systems Impede Response

Today, a myriad of security systems and sensors are used to safeguard critical infrastructure. Examples include access control, identity management, building management, panic/duress alarms, fire alarms, elevator controls, biometric scanners, video surveillance, video analytics, and more. These systems typically perform a specific task and operate in their own proprietary environments with virtually no working knowledge of each other and limited interactivity.

Increased globalization and enterprise consolidation further increase the complexity of security systems within organizations. Security systems acquired over time by different divisions in different parts of the world are unlikely to be standardized across the organization.

The result has been a piecemeal and inefficient approach to security. Bringing together information from all of these separate security systems to form comprehensive, well-coordinated security plans and responses to incidents requires considerable, often manual, effort. The overwhelming amount of information often makes it impossible for operators to know how to act effectively and decisively, especially under stress.

The Benefits of PSIM

Physical Security Information Management (PSIM) systems capture and fuse information from a variety of security, safety, and enterprise systems. These systems enable users to view and analyze information to more quickly and efficiently identify situations and persons of interest and initiate rapid, effective response, often in collaboration with first responders and outside agencies.

Leading PSIM solutions provide a single user interface that consolidates data from the organization's subsystems and sensors and:

- Aggregates, correlates, and enables analysis of data from various security monitoring systems.
- Performs 2-D and 3-D mapping and offers geospatial capabilities that dynamically locate devices, people and assets and create relationships between them.
- Performs simulations to allow organizations to perform "what if" analysis to plan a response.
- Provides standard operating procedures (SOPs) to ensure consistent responses that follow best practices.
- Furnishes reporting to enable organizations to meet regulatory requirements.

Organizations can use PSIM solutions to plan and monitor their security environment, respond effectively to events, and review event response for auditing/regulatory compliance and to improve response.

By consolidating security system planning and monitoring and providing standard operating procedures, simulations, and reporting, PSIM systems enable organizations to improve the speed, efficiency and intelligence of response, while reducing costs and minimizing compliance risks.

Improve Operator Efficiency and Lower Costs with Consolidated Monitoring

PSIM solutions create a unified command, control, and communications (C3) environment with a single coordinated set of information that supports a unified response. Operators can see information from all their security systems in one interface. Because sensors and systems automatically feed the PSIM system the geographic coordinates of any events (as shown in Figure 1), the PSIM interface can correlate data, events, and alarms to provide a situational view of data that identifies real situations. The system presents this data using a 3-D GIS view of the monitored area and any security incidents as they occur.

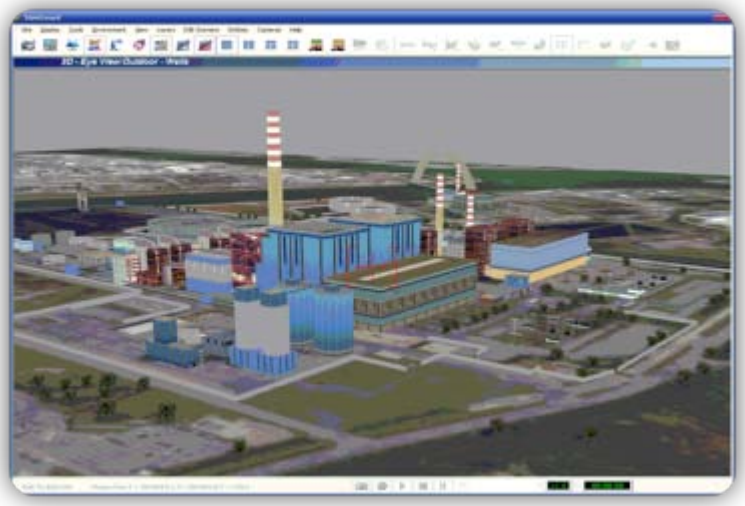


Figure 1: A PSIM system presents a 3-D view of the monitored area. Sensors and security systems feed the PSIM system the geographic coordinates of security incidents.

Take the case of an airport that uses a PSIM system to consolidate information from its radar and video surveillance systems. If a blip occurs on the radar screen, the radar system automatically provides the PSIM system with the geographic coordinates. The PSIM system instantly associates those coordinates with the location of the nearest camera and displays a video view of what the radar detected. The operator can thus see whether the blip was an animal which can be ignored, or an intruder, which requires a security response. Without the PSIM system, the operator would have to manually track down the cameras associated with the location of the radar blip.

The rules engine within the PSIM system helps determine the importance of an incident, so operators can prioritize their response. For example, an access alarm can indicate either forced entry or faulty locking hardware. An operator could set up a rule such that when an access alarm occurs, the system automatically checks the video motion detector and issues an alarm to the operator only if there's an intruder. This minimizes false alarms and the costs associated with responding to them.

The centralized C3 also gives operators access to check lists, emergency plans, and other decision support aids right from the operational display, as shown in Figure 2. The C3 distributes all this information to response personnel in the field to enable a standardized, improved response. Call trees tell operators who must be notified, and escalation trees automatically send text and email messages. This accelerates and standardizes response during an emergency by eliminating the need to rummage through paper books and manuals.

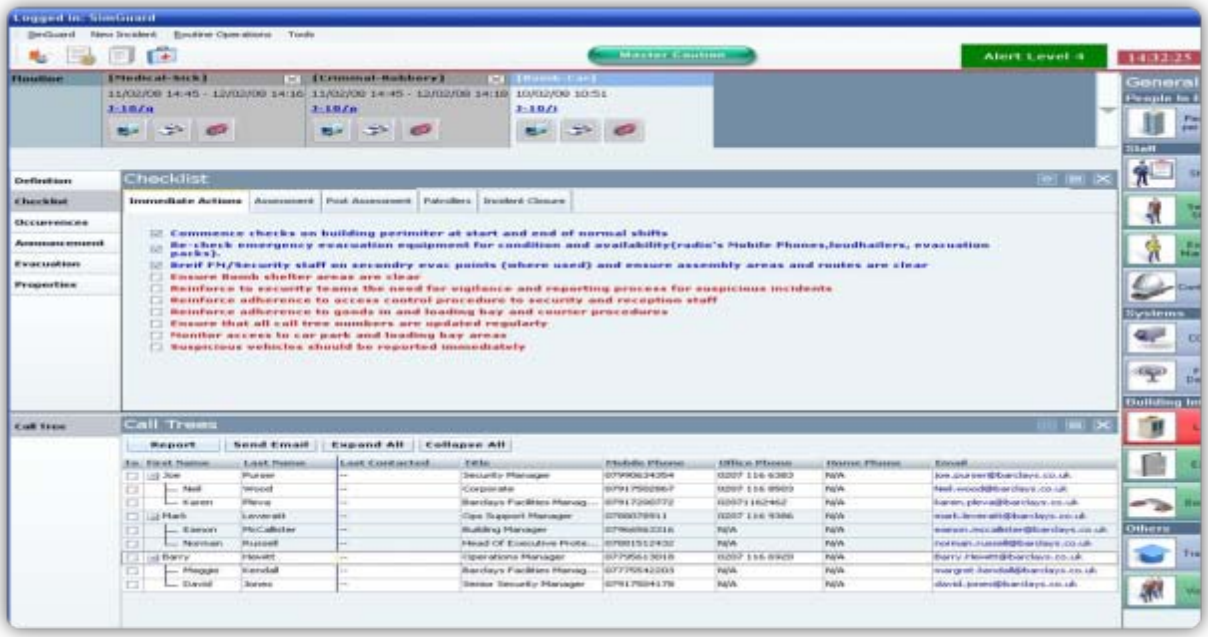


Figure 2: The C3's operational display can show checklists and call trees when necessary to eliminate the need for operators to look through books and manuals during an emergency.

Everything that transpires in the system is registered into a database. The organization can later research what happened and see exactly what each operator did during the incident. This is useful for improving future response or aiding an investigation into the incident.

Enhance Preparedness through Simulations

Simulators model a live threat environment to prepare responders for emergencies. Planners can run virtual threat scenarios that simulate crowd behavior, gas propagation, blasts, floods, and more. Realistic computer simulations enable organizations to test and practice a wide range of scenarios in a cost-effective manner.

Simulators can be used to improve numerous operations, including:

- **Device deployment.** Simulators help organizations place security devices in the best positions. For example, when a utility company places security cameras around the facility, a key objective is to minimize costs by using the fewest cameras that provide the greatest visibility. The simulator allows planners to place a camera on a 3-D map and see the coverage area, as well as anything in the environment that might obstruct the view. They can then "virtually" move the camera and elements of the environment to optimize placement.

- **Optimize security plans**. Organizations can run simulated scenarios in a virtual environment to test security plans against relevant threats to evaluate the quality of the plan and identify security gaps. Sophisticated crowd behavior algorithms enable organizations to visualize evacuation routes to determine the location of bottlenecks and estimate the time needed for evacuation.
- **Training.** Training based on real-life experiences helps establish a higher level of incident preparedness. By combining a 3-D geospatial model and scenario generators, organizations can construct and run simulated incidents. Trainees or controllers and management can rehearse different scenarios and view the consequences of corresponding actions. Scenarios can be made more challenging by changing lighting conditions, weather conditions, camera interference and more. This helps prepare key personnel to make more accurate assessments of emergency situations, improving the decision making process.
- **Real-time decision support.** Security and safety personnel can perform simulations in real time during an incident for decision support. For example, they can see the likely path of a fire or of gas propagation to help plan a response.

Respond More Intelligently with Next-Generation Technology

Next generation capabilities, such as geographic maps, multi-site and multi-zone views, and 2-D and 3-D maps, promote faster, more effective response to security threats.

- **Geographic map views.** These views allow operators to see where an incident is occurring on a map and provide the geographic coordinates, as shown in Figure 3. These maps can include 2-D and 3-D indoor and outdoor views and use multiple layers to represent streets, locations, and coverage areas for cameras and other sensors. They can also delineate threat regions and damage zones.

Figure 3: Geographic, 3-D maps allow operators to see where an incident is occurring.

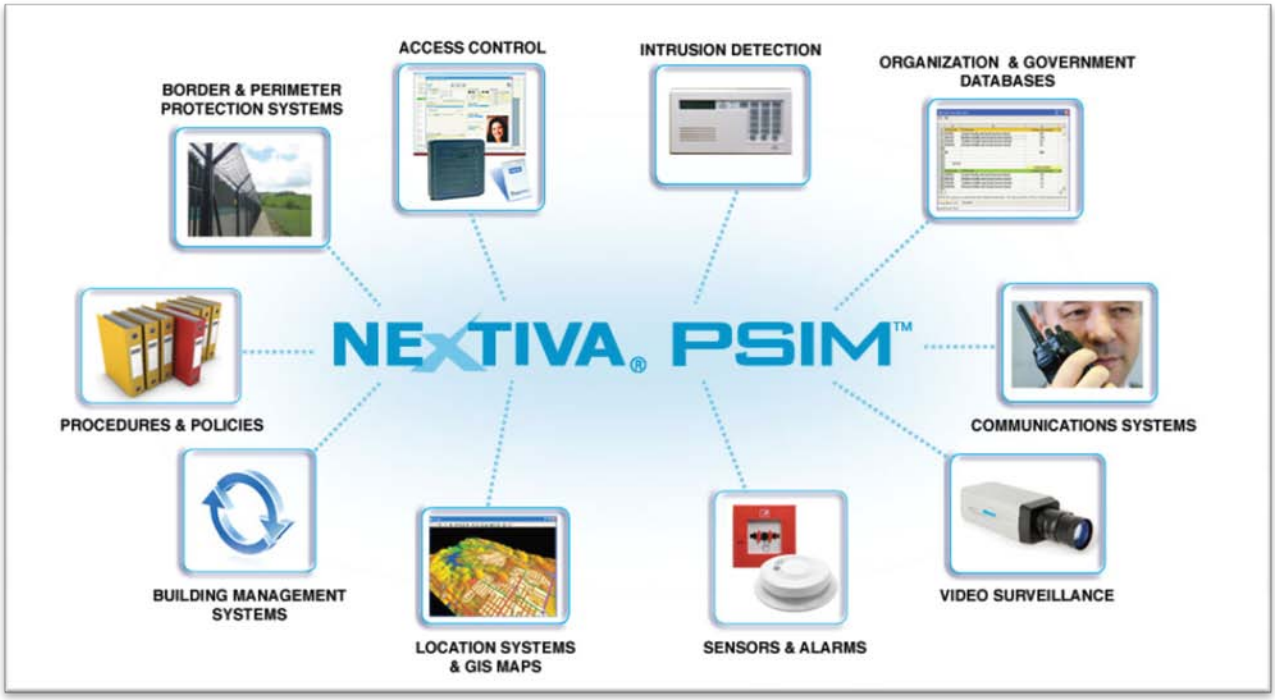
- **Multi-site view.** A single operator can monitor incidents and status at multiple sites simultaneously. For example, a utility might have multiple gas pipes and electric substations all over a city. The utility can use this capability to monitor all of these sites from one location, thus reducing security costs.
- **Multi-zone view.** This allows multiple people within a single location to monitor specific areas. For example, there may be thousands of cameras throughout a city. Multi-zone views allow city governments to assign various operators the task of monitoring specific precincts or neighborhoods.
- **Holistic 3-D video management.** A smart video management system allows operators to automatically view cameras in a selected area by simply clicking on the 3-D model of the site. For example, if someone tried to enter a secure area in an airport via an exit, the access control system could automatically provide the PSIM system with the intruder's coordinates. The PSIM system could then display the video corresponding to those geographic coordinates. As the intruder walked through the terminal, adjacent cameras could automatically track the intruder's progress. Without a PSIM system, it would take hours to manually locate the right cameras and track down the intruder, potentially leading to closure of the terminal until the suspect was located.

Facilitate Regulatory Compliance

Regulatory compliance typically comes down to developing and following standard response processes and being able to demonstrate that the organization follows these processes. PSIM systems should include industry-standard workflows and checklists to help ensure that organizations have repeatable and predictable procedures in place to respond to potential threats and incidents. These systems should record all event data and allow scenarios to be accurately re-run to present all operators' actions, so that organizations can also demonstrate compliance with standard response processes.

Nextiva PSIM: Boost Situational Awareness, Accelerate Response

Nextiva® PSIM™ generates Actionable Intelligence from vast amounts of data to increase situational awareness, improve security effectiveness, streamline system management, and optimize costs.



Nextiva PSIM captures and fuses information from a variety of security, safety, and other enterprise systems, so that users can more identify and initiate response to potential threats and other situations quickly and efficiently. The unified PSIM interface provides virtually everything operators need to monitor their environment and respond in a consistent fashion that complies with organizational policies, best practices, and regulatory requirements.

Feature Rich

Nextiva PSIM features:

- An intuitive 3-D, multi-layer user interface and indoor and outdoor 2- and 3-D maps that rapidly build situational awareness
- System-wide procedures and standards to promote more efficient and consistent event management throughout the organization
- Virtual simulations for improving training, contingency planning, and incident preparedness
- Reporting for more effective debriefing and step-by-step event/response analysis
- Industry-standard workflows to help ensure that operators respond to routine and emergency situations based on standard policies and procedures
- And much more …

Plus, Nextiva PSIM helps reduce operational costs by enabling organizations to deploy equipment and resources more efficiently and cost effectively.

Collaboration and Communication in Real Time

Built on an open, scalable architecture, Nextiva PSIM allows multiple users to view information, including events, alerts, and video, from multiple sites simultaneously. In addition, Nextiva PSIM allows operators situated in different locations to collaborate and share information in real time. An open SDK facilitates easy integration with a multitude of sensors and systems — access control, intrusion, CCTV, radar, border control, and HVAC systems, GIS, various communication media, and multiple public and private organizational databases.

Nextiva: Transforming Video into Value™

Nextiva PSIM is part of the Verint Nextiva portfolio, the industry's most comprehensive, *integrated* suite of video solutions and services. Nextiva features video management software and services, video analytics, encoders and decoders, industry-leading wireless devices, high-definition cameras, network video recorders, and a physical security information management system, plus suites for retail, banking and financial services, enterprise, and critical infrastructure. Nextiva streamlines management of large, geographically dispersed video operations and can significantly simplify video system deployment, maintenance, and migration to IP.

Since 1994, Verint Actionable Intelligence solutions have helped government and commercial organizations protect people, property, and assets. Today, more than 10,000 organizations in over 150 countries use Verint solutions to improve enterprise performance and make the world a safer place.

For more information about Nextiva PSIM or any of our solutions, visit www.verint.com or contact us at marketing.vis@verint.com.