

Integrated and Networked Physical Security:

***How to achieve greater levels of functionality
while reducing cost and complexity***

Table of Contents

1. Introduction	3
2. The Current State of the Physical Security Market	3
2.1 Drawbacks of Traditional Security Systems: The Piecemeal Approach	3
2.2 Issues with Custom Integration	4
3. The Unified Approach Emerges	5
4. Core Components of a Unified, Networked System	6
4.1 Video Management Software	6
4.2 Access Control	6
4.3 Video Analytics	7
4.4 Intrusion Detection	7
5. Additional Features	7
5.1 Map Interfaces	7
5.2 Reporting Capabilities	8
6. Key Benefits of the Integrated Approach	8
6.1 Ease of Deployment Leads to Lower Costs	8
6.2 Reduced Complexity and Cost of Maintenance	9
6.3 Seamless Scalability	9
7. Taking Integration Further	10

1. Introduction

A traditional security system is composed of a variety of subsystems such as video surveillance, access control and intrusion detection alerts. By themselves, each of these systems is a critical component of a sophisticated security infrastructure. But for the most part, these platforms operate as separate components without the ability to communicate with each other. This inability to share critical security information between devices and platforms leads to missing data, which can result in security hazards and lapses.

Over the past decade, the focus of security has shifted from analog based systems to IP based solutions. IP security devices enable quicker access to critical data than analog systems because information can be accessed instantly over the network. Yet until today, IP systems fell short in that they had no inherent way of connecting the disparate systems. To combat this, integrators and installers were called upon to bring these siloed platforms together. In combining these separate systems – video surveillance, access control, analytics, intrusion alerts and more – into a single interface, users can take advantage of a higher level of situational awareness to more effectively detect and deter potential security threats. However the process of merging these systems was expensive and complex because the products were not designed for intelligent integration.

Today emerges the next generation of security systems that are designed from the ground-up as completely integrated, networked systems. These solutions minimize the complexity of integration and leverage the power of the network. Video management, video analytics, intrusion detection and access control are combined into a single platform. Because all components are provided in one package, the unified approach is cost effective and easier to install, use and maintain.

This white paper outlines the benefits of these pre-bundled solutions. It will explore the key components of a sophisticated security system, the advantages of correlated information from multiple subsystems, and the cost and time savings associated with this approach.

2. The Current State of the Physical Security Market

2.1 Drawbacks of Traditional Security Systems: The Piecemeal Approach

Traditional security systems include a number of various ‘moving parts’ including video management, access control, intrusion alerts, remote connectivity, video analytics, intercom audio, and more. In the past, these separate systems had no inherent way of communicating without custom and time-consuming integration. Even with custom integration, the system was never truly whole. The following are just some of the drawbacks to the piecemeal system:

- ▶ *Different user interfaces:* When purchased separately, each system component - access control, intrusion detection and video management platforms – would each have different user interfaces, making it difficult for security personnel to effectively

manage events. For example, a security operator who receives an alert on the access control interface that a door has been forced open must then switch over the video management interface to locate the corresponding video.

- ▶ *Storage requirements and energy consumption:* Security components by themselves require many pieces of equipment – cables, servers, storage devices, etc. This additional equipment is expensive to procure, complex to install and consumes a lot of energy as well as physical space.
- ▶ *Critical data are not correlated between systems:* Basic, custom integration allows various devices to communicate but not in an intelligent way. A security system that is designed from the ground-up as an integrated and networked solution leverages the power of the network to combine, trend, and index events and alerts from various security subsystems in one interface.
- ▶ *Cost:* IP systems, when purchased separately, can be very expensive with the result that many smaller businesses forgo critical components such as IP access control or intelligent video analytics. It is not cost-effective for smaller businesses to purchase an entire IP-access control system when they have only a few doors to secure. When a comprehensive security system is built from the ground-up, the software for each subsystem is already built into the interface with the result that small door counts are affordable because the only cost is the purchase of the lock. Likewise, video analytics are expensive when purchased separately because businesses incur licensing and per channel fees. Yet in an all-in-one solution, analytics are an integral part of the system.
- ▶ *Proprietary, analog technologies:* Unfortunately, many existing security systems do not take advantage of IP networks. Both LAN and WAN are extremely prevalent today, and networked-based products offer multiple benefits for businesses of all sizes, especially users who have multiple facilities that need to be managed centrally. In general, large customers are often the first adopters of IP-based devices; smaller customers need ways to optimize the use of their existing infrastructure and take full advantage of IP networks in a cost-effective manner.

2.2 Issues with Custom Integration

In order to address the shortcomings of traditional security systems, integrators and manufacturers develop interfaces that allow the disparate devices to communicate by taking the data generated by one subsystem and transmitting it to the other. While such interfaces enable users to gather more information from the entire system, there are many problems associated with this solution. Complexity is increased when disparate systems are configured independently and then interfaced together. While some information is exchanged between the systems, they do not share common databases, which means that some critical data or functionality is lost within the customized integration. In addition, supporting these systems is time-consuming and costly since issues can involve both the manufacturers and the integrators and it is difficult to keep the different versions of different products in sync. Lastly, the different systems require unique or independent infrastructure. For example, if the VMS platform requires a server with a different spec than the access control system, two servers have to be purchased and supported.

Interfacing can be done physically (e.g. by using alarm inputs, dry contacts, etc.) or logically, by using software interfaces (SDKs, APIs, etc.). While integration at the software level can potentially achieve a higher level of integrated functionality, it requires more expertise, longer lead-times and requires continuous monitoring to keep the different systems/applications compatible.

Interfaced systems fall into three broad categories:

- ▶ *Access-centric*: An Access-centric system is one in which video surveillance and intrusion detection are added on to the existing access control interface. Unfortunately, there are a host of reasons why this integration is unsuccessful. First, most access control systems are proprietary, closed systems without the tools and interfaces necessary to support integration. Second, IP-based video surveillance is advancing much more rapidly than access control so the high-level functionality of the video system is often lost. Third, video surveillance systems require more sophisticated user interfaces compared to access control applications.
- ▶ *Video-centric*: Incorporating access control and intrusion detection functionality into a video surveillance application also falls short of achieving optimal integration. Traditional DVRs are not designed to offer this functionality and most of the integration is done by video management software applications. These applications were primarily built for video management and as such, are not event-driven, which is the basis for access control and intrusion systems. Some platforms have added event-management integration capabilities but lack the critical piece to interface with legacy access and intrusion systems.
- ▶ *Third-party applications*: These refer to software applications that integrate information from various security subsystems together. These applications, generally referred to as PSIM (Physical Security Information Management) systems, are expensive, complicated to implement and difficult to maintain, making them unsuitable for small- and medium-sized business users.

3. The Unified Approach Emerges

Addressing the need for an integrated security system requires a platform that is designed from the ground-up as both integrated and networked. These advanced, unified systems:

- ▶ Provide enhanced security through integration and intelligence, both in real-time and forensically.
- ▶ Are easy to deploy because they do not require configuration and custom integration.
- ▶ Are cost-effective with lower power consumption rates because they require fewer additional pieces of hardware.
- ▶ Are easily scalable because adding additional infrastructure components such as door locks or cameras does not require a re-configuration of the existing system.

A unified, networked security solution needs to be cost-effective, yet high in performance level and easy-to-use - a challenging combination. But today's unified networked security solutions meet these needs. One way is through an intuitive user interface (UI). The user interface is the heart of any security system. The UI is easy-to-use and presents information in an integrated manner, enabling officers to easily access information for investigation and analysis.

4. Core Components of a Unified, Networked System

4.1 Video Management Software

Video management functionality is the most critical aspect of any security system. Some of the key capabilities of an advanced VMS system built into a unified platform include:

- ▶ Display virtual matrix of multiple cameras automatically highlight a particular camera if there is an event.
- ▶ Access live, high quality video from any camera.
- ▶ Playback video from one or multiple cameras at various speeds; playback is possible by time stamps, bookmarks or particular events that are clearly displayed on a timeline.
- ▶ Control all camera features such as PTZ, tours, presets, frame rates and resolutions from anywhere over the network.
- ▶ Apply standards-based protocols for interfacing with cameras (PSIA and ONVIF), streaming and storing video (H.264, MPEG-4, MJPEG), networking (TCP/IP, IPv4&v6, UDP, etc.), security and authentication (802.1x, HTTPS, etc.) and auto-discovery/provisioning (DHCP, DynaDNS, etc.).
- ▶ Auto discovery and provisioning for faster, easier deployment.

4.2 Access Control

In a unified, networked security solution, access control functionality is completely integrated with the video management system and share the same events database, which is essential for detecting potential risk behaviors such as tailgating or piggybacking, and for generating consolidated reports.

Important features of an integrated access control system include:

- ▶ Complete access control from anywhere over the network including locking and unlocking doors.
- ▶ Schedules for locking and unlocking doors.
- ▶ Auto discovery and provisioning of access control components for faster, easier deployment.
- ▶ Easy integration with legacy components.
- ▶ Policies and roles to simplify and standardize door programming and access rights.
- ▶ Digital card access saves on rekeying costs.
- ▶ Alerts on real-time events to on-site operators, remote computers or mobile devices.
- ▶ Peer-to-peer communication in multiple locations.
- ▶ Shared events database with VMS for video confirmation.
- ▶ Events such as door forced open are time stamped for faster search.

4.3 Video Analytics

Video analytics automatically analyze surveillance video to gather information that is useful for alerting operators of possible security threats or for collecting statistical information. Important video analytics include tripwire, entry and exit monitoring, loitering, detecting objects left behind or removed and people counting.

In a unified, networked platform, video analytics are an integral part of the system. They run on the same hardware and the user interface is fully integrated with the other components. Video analytics work best when events are correlated with information from other systems such as access control. For example, video analytics can identify behaviors such as tailgating which can then be communicated to the access control system, generating the appropriate alarm. Video analytics are also useful for analyzing business procedures, compliance, operations and resource allocation. A bank could use people counting to identify the number of customers that enter a branch within a two-hour time period, for example; these data could then be used to determine appropriate staffing levels.

4.4 Intrusion Detection

A traditional alarm system is also tightly integrated into a unified, networked security solution. Some important capabilities include:

- ▶ *Easy integration of alarm panels:* For facilities that have existing alarm systems, it is essential that the security system incorporate these devices to control them through a unified interface.
- ▶ *Central station integration:* When intrusion alarms are generated, the central station operators can take advantage of the integrated security platform at the end-user site to correlate the alarm with information from the access control and video systems.

Integrating the comprehensive range of functionality as described above is achieved by sophisticated software that is able to bring together information from the different systems, correlate it and report on it. Other elements bring even more critical data to enable the user to have a comprehensive view of security and business operations.

5. Additional Features

5.1 Map Interfaces (MI)

User-interfaces are traditionally displayed in a list and matrix format. However, a map interface in which security devices such as cameras or door locks are displayed on top of a map of the building or campus has proven to be a much more intuitive way of navigating through a sites many security devices. To build MIs, users import digital schematics of facilities into the system and then place icons of the devices at the appropriate locations. Rather than scrolling through a long list of data to find a particular camera, by simply clicking on or hovering over an icon of the device users can pull up its specific information or controls. For example, security operators can click on a camera to pull up its controls and then use the PTZ functionality or playback surveillance footage, right from the same

interface. MIs are especially useful for controlling multiple facilities or sites from a central location.

5.2 Reporting Capabilities

Correlated information provides advanced reporting capabilities, helping businesses better understand their security operations. Types of reports include:

- ▶ *Incident reporting:* Reports are generated by type of incident, time, location or a host of other methods. This information helps determine locations or times of the day that pose potential threats. Incident reports also help operators gauge the impacts of changes made to the security system. Trend analysis helps users understand whether certain security issues are getting better or worse over time.
- ▶ *Case management:* Cases are easy to document since recorded events include information from all devices including door locks, intrusion alarms, surveillance footage and more. Cases are stored with a timestamp so they can be easily searched and retrieved in the future.
- ▶ *Dashboarding:* Dashboards present important information visually to track overall trends. Dashboards not only display critical data but also highlight areas that need attention. Rather than sifting through all data from a system on a regular basis, operators can look at the dashboard to view the most important information.
- ▶ *Multi-site analysis:* For users that manage multiple facilities or site, an integrated system is ideal for comparing information to determine where to focus attention and allocate resources.

6. Key Benefits of the Integrated Approach

6.1 Ease of Deployment Leads to Lower Costs

Achieving a high level of integration and functionality with a piecemeal security system is complex and costly to install. The integrated solution eliminates the complexity. The level of automation provided in an integrated platform makes it easy for security installers with limited networking knowledge. Some key features include:

- ▶ *Auto-discovery of edge devices:* Auto-discovery makes installation faster and easier because the system will find most edge devices such as cameras and IP-door locks. While not all edge devices have self-discovery protocols, there is an increasing trend towards incorporating them.
- ▶ *Auto configuration and remote configuration:* Installing a complete system is made easier by pre-provisioning the systems with configurations needed at a particular site, or connecting the systems to the network and configuring remotely.

- ▶ *Leverage existing networks:* Unified, networked solutions are designed to easily work with the user's existing network infrastructure with minimal configuration. If the site has a wireless network, the system detects it and prompts the user to provide the appropriate security credentials. Once plugged into the network, the system is automatically detected and ready for remote management.

6.2 Reduced Complexity and Cost of Maintenance

Traditional security systems have a relatively high cost of ownership over time because maintenance of disparate pieces of equipment and software is required. Different components, especially software, can become incompatible as new versions are released, which makes the maintenance of the system an arduous and expensive task. An integrated platform is relatively easy to maintain and has a much lower cost of ownership over its lifespan because the entire system is operated over a single software interface. Other features that reduce cost and complexity include:

- ▶ *Browser-based application:* Traditional systems access control and video surveillance systems are built around applications that run on specific hardware and software configurations. For example, a VMS software application may only run on a particular version of Windows on a computer with a particular hardware configuration. This leads to added cost and complexity since different hardware and software configurations may become incompatible with the applications. To avoid these issues, new applications run on Web browsers (IE, Mozilla, Firefox, Safari), making them independent of the operating system and particular hardware configurations.
- ▶ *Software upgrades:* In traditional systems, software upgrades are challenging because of compatibility issues. In a tightly integrated system, upgrading any part or feature of the system is a seamless process because there is one integrated piece of software to upgrade.
- ▶ *Remote management:* Remote management capabilities make maintenance easier and reduce the risk of losing data due to system failure. System health indicators are gathered on an on-going basis so that some failures can be predicted before they happen. Managing the system remotely reduces the number of on-site visits, lowering maintenance costs.

6.3 Seamless Scalability

A unified, networked security system accommodates growth with seamless scalability. When additional edge devices are added, the system automatically recognizes and incorporates them (if possible). Cameras, for example, are automatically discovered and configured to the parameters already set for existing cameras. Similarly, new access points are automatically configured with the same permission levels as the others in place. Once configured, edge devices are automatically incorporated to appear in the UI and the databases.

Back-end system expansion is also seamless which happens when the number of edge devices supported by the system appliance is exceeded. A unified, networked system will back up current system configuration and replicate them for the new appliance without disrupting the working system which is critical for avoiding security lapses. Furthermore, the load is evenly shared so that the resources are optimally utilized.

7. Taking Integration Further

There is a growing demand for integrated networked security systems to incorporate other systems such as HVAC, fire alarms, lighting controls and HR databases. When the networked system is integrated to building management, it can reduce energy costs. An ideal example is an employee's office lights and computer turn on when they swipe their security badges at the front door in the morning, and turns them off when they swipe on the way out.

Today's customers demand solutions that leverage the benefits of the IP network and integrate multiple devices. These solutions need to be cost effective, feature rich and easy-to-use, and combine the performance, sophistication and functionality of an enterprise-class security system into a compact, integrated package. Most importantly, the integration of access control, video management, video analytics and intrusion detection into a single platform is a more effective security solution that enhances the overall safety of an organization.