WHITE PAPER

Enhancing physical security through system unification

Genetec™

genetec.com

Executive Summary

While organizations look to incorporate video surveillance and access control systems that provide greater interoperability as part of their security strategy, the majority of security manufacturers have continued to provide disparate systems, with limited communication between systems.

With the recent advancements in software technologies, and the ongoing partnerships between security manufacturers, integration has become a popular substitute for traditional interfacing. However, even integration has its limits. The answer can be found in a single software platform that can manage access control, intercom, intrusion, and video devices, while offering a unified interface to monitor the entire system. Such a system goes above and beyond the basic functionalities of interfacing and integration, while offering end-users an efficient, flexible and cost-effective option to system unification not available with highly customized and expensive solutions like PSIMs.

Building Security Solutions That End Users Want

Even today, with all the technologies available, the industry is struggling to fully succeed at building security solutions that fulfill the users' true needs—a cohesive video and access control system that is efficient, non-proprietary, and cost effective. It is important to recognize that without these basic criteria, a unified video and access control system may not seem advantageous to customers and thus, not generate enough demand for manufacturers to justify developing such a product.

Efficiency Gains Matter

The priority of any security staff will be to spend time on performing their core tasks such as monitoring, investigating and responding to incidents to ensure the security of the organization. Their ability to perform these critical tasks should not be impeded by time spent managing technology. In other words, the security technologies they use should help them be more efficient and effective, while not slowing them down.

In one of his articles, Rich Anderson, CTO of Razberi Technologies, and previously VP of Marketing for GE Security and VP of Enegineering for CASI-RUSCO, illustrates the common problem with today's disparate systems with the following statement: "Access control systems in particular generate alarms for invalid badges, door-forced and door-held events. Those events need to be investigated, but the task of doing so with a standalone surveillance system is painful. Receive an alarm on one system, and your operator has to move to another completely different system to investigate. This surveillance system has a different user interface and so he/she has to "switch gears." Then, which camera do you call up to view the scene? An experienced operator will know, but that "experience" costs you a lot in terms of training." [2]

Mixing and Matching Best-of-Breed Technologies

The PC industry has succeeded in building interoperable products. Anyone can buy a PC today, and down the line, add new hardware like a printer, web cam, gaming device, or even install a new hard drive that processes information twice as fast as the previous one. Almost anything can be done without changing the entire PC or operating system.

However, the same cannot be said about, or achieved in, the security industry. A user cannot simply decide to buy the latest high-tech wireless door controller and add it to an existing access control system. Or buy the latest and greatest IP cameras and connect them to a video management system (VMS) without first verifying that the specific model is supported. For these and many other reasons, the security industry is far behind the PC industry.

[2] Video and Access Control Integration, SecurityInfoWatch.com, Rich Anderson, 03-25-2009

In fact, it might never be possible to achieve what the PC industry has in terms of interoperability. Making a commitment to proprietary technology can be a costly decision. When a new technology emerges, the option to incorporate it becomes more of a question about whether or not to forego existing investments and start over from scratch with a new investment.

On the other hand, having the ability to mix and match best-of-breed products from different manufacturers, and having the option to incorporate the latest advancements in technology into a security system ultimately provides more flexibility and the added assurance that your investment is future-proof.

Managing Investments

A solution that is entirely customized to fit with all existing business systems and infrastructure might be very efficient and attractive, but as with any customized approach it will likely be expensive as well. Take for example ERP systems (enterprise resource planning) deployed by many companies. An ERP system can be customized to adapt to virtually any business model and environment by specialized ERP system integrators. Although the cost of customizing such a system is very high, there is usually a significant productivity gain realized after deployment to justify this investment.

In similar respects, investments in security departments and equipment are always considered an expense and it is unlikely that security systems could be adapted to every internal process. Since these systems rarely generate revenue, budgets are traditionally tightly controlled. Completely overhauling a system, regardless of the technology employed, is entirely dependent on budget availability and management's buy-in. Often, even discussions of upgrading or replacing a system occur out of pure necessity (e.g., aging system or security flaw) and the process of sourcing and implementing a system could span months, if not, years.

Therefore, it is crucial, more than any other factor, that the total cost of ownership of a cohesive video and access control system be justified.

Integrated Systems

With the recent advancements in technologies, and increased collaboration between manufacturers, integration has become a popular substitute for traditional interfacing.

"In information technology, systems integration is the process of linking together different computing systems and software applications physically or functionally." [3]

Specifically in the security industry, the most popular integration methods involve network protocols and software development kits (SDK).

Network protocols are very powerful as they support a mix of operating systems and allows you to manage your applications in real-time. However, integrating two systems through a network protocol requires more time than an SDK, or it may require a shared database between two systems. Network protocols are popular for edge-device integrations like IP cameras or door controllers but are even more commonly used between two software applications. Network protocols are simply deemed more effective.

An SDK, also referred to as application programming interface (API), consists of a DLL package created and distributed by software manufacturers to allow other software developers to integrate to their system.

SDKs simplify the integration by hiding complex mechanisms from developers such as authentication, decoding video, complex network protocols, and so on.

Because they simplify a software integrator's task, most DVR, NVR and access control manufacturers offer an SDK or API instead of a network protocol.

The majority of video surveillance manufacturers offer an SDK that can be used to integrate live and playback video within any application. For example, some access control manufacturers use the SDK from DVR vendors to link an access control alarm to the associated video for quick playback. The majority of access control software manufacturers also offer an SDK so VMS systems can receive access control events from their system. Some access control vendors even allow video manufacturers to integrate some of their functionality inside the access control system's user interface.

Regardless of the method of integration that is chosen, integrated systems definitely start to give users the tools to become more efficient. It is very common for an integrated access control and video solution to display live or playback video associated with an access control event from the access control user interface.

[3] Systems Integration Course Syllabus, Georgia State University, webpage, retrieved June 27, 2007

Also, integrated solutions offer another advantage for users: not having to rely on a single manufacturer for the entire security system. In some cases, it might be beneficial to deal with two independent vendors, each having multiple technology partners of their own. In this case, users who do not like their current video surveillance solution might be able to switch to another manufacturer, as long as it is compatible with the access control system.

Although lowering end user switching costs and using an SDK or API to achieve a deeper level of integration amongst products has its benefits, integration can also carry a few pitfalls.

Most of these integrations still require operators to use two systems in parallel because neither the video nor the access control system offers all the required functionalities in one user interface.

A few limitations can include:

- The access control system does not support camera sequences
- Not easy to search through all recorded video recording with access control
- No motion search capabilities in the access control system
- Pan-tilt and zoom (PTZ) functionalities are limited in access control as compared to the video system

Another common drawback to consider with an integrated system emerges from future maintenance and configuration of said system. Since the administrator has two or three independent systems to configure and keep synchronized, maintenance of multiple systems will require more time.

Also, many of the required configurations are redundant, forcing the administrator to repeat the same work on all systems.

Here are a few examples:

- Independent alarm management configurations
- User management: for each operator, the security manager must create two accounts and specify privileges in two systems
- Each new camera requires configuration in two independent systems

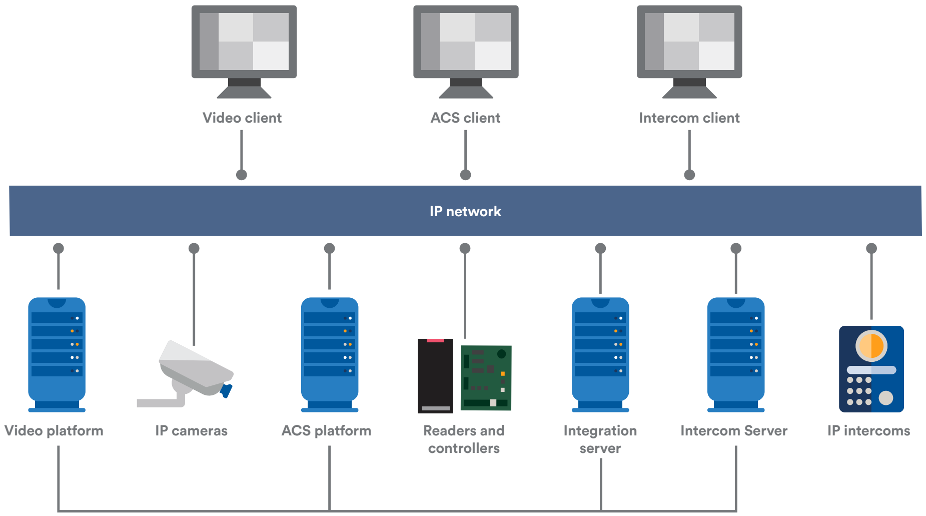


Figure 1 - Integrated solutions

Finally, conducting upgrades and getting support for an integrated system can be challenging. As a newer version of an application is released, changes to the software may break compatibility of an integration between two systems, delaying an organization's ability to upgrade their system or requiring them to invest in custom work to re-integrate the two systems.

Manufacturers constantly change their software to support new functionalities and with that, might also change the way existing integrations work, especially when they change their SDK or API.

Considering an upgrade to the latest software version of one system that is part of an integrated solution may impact the integration, the installer is responsible for ensuring that the latest VMS software is still fully compatible with the access control software. Before taking an end-user's system down and upgrading it, many integrators will prefer building a test system in their lab to validate the integration.

Seeking support for an integrated solution can also become a complicated affair. As there are two separate systems involved, each likely from two different vendors, when a problem occurs, it takes more time to resolve. Both manufacturers, and often the integrator, have to investigate and figure out which system is not behaving properly. The time it takes to resolve the issue in question is also dependent on the relationship between the two software manufacturers.

So, although there are many advantages derived from an integrated system in comparison to traditional interfacing, there are still many issues with this level of integration that emerge.

Open Platform Systems

Open-platform products, as referred to in the security industry, integrate with different hardware manufacturers without necessarily using industry standards like open-architecture systems.

Open-platform manufacturers develop, test and maintain the integration with every single device supported by the product. Open-platform products tend to support a wide variety of manufacturers that offer similar functionalities and products that are commoditized. Manufacturers of such systems do so by building a generic integration layer that provides the most common functionalities and then by developing a driver for each specific product the system integrates with. This strategy works well for specialized appliances because they have fixed and well-defined functionalities.

The open platform VMS concept, for example, is well established in the market because IP cameras or IP encoders all offer common features.

These types of systems offer huge benefits to end users because they now have the freedom to change software or hardware vendors without having to discard all invested equipment.

The access control industry however, has traditionally been built on proprietary solutions, including single manufacturers for the door controllers and the management software. Today, it is easier for vendors to build closed access control systems. The reasons being that offering a closed system reduces complexity, simplifies testing efforts, and increases the revenue per customer by selling both the hardware and software. But this closed architecture removes a lot of flexibility for the end user.

Because of the success in video surveillance, and because end users are demanding more freedom, similar open-platform products are beginning to emerge in the access control industry. Today, IP-based door controllers are offered by manufacturers that do not even offer access control software. These hardware manufacturers publish their wired protocol or provide an SDK to communicate with their controllers. Other hardware companies are also offering more and more wireless IP locks bundled with readers that reduce the installation costs.

A Cut above The Rest: The Open-Unified Platform

With the open-platform concept already established in the video surveillance industry, the new trend toward non-proprietary door controllers in the access control industry, and emerging security standards, a unified security platform is now achievable.

A unified platform is a comprehensive software solution that manages access control, intercom, intrusion and video functionalities through non-proprietary security appliances.

A unified platform goes above and beyond tagging or bookmarking video when an access control event occurs or unlocking an access controlled door from the video surveillance user interface. It is a unified user interface that offers seamless integration between video, intercom, access and intrusion systems with built-in reporting and alarm management functionalities.

With this type of solution, it is possible to configure and manage video cameras, access controlled doors, print badges, monitor intrusion panels, and have everything at the security personnel's disposal to ensure the level of security of a facility within a single consistent software suite.

An open-unified solution protects the end user's investment through interoperability, meets the user's security needs, and is affordable to buy and maintain.

An open-unified platform is a product that targets the mass market by providing built-in support for commoditized security products such as IP cameras, DVRs, door controllers, alarm panels, intercoms, badge printers, active directory for authentication, and card management without requiring customization for every installation.

This type of solution targets the mass market offers out-of-the-box interoperability and tends to be less expensive than a custom-integrated solution.

Since a unified platform supports commoditized products, hardware investments are also protected. Therefore, if the end user is not satisfied with the unified software solution, he can change software components without having to reinvest in specialized appliances.

Nevertheless, something to keep in mind is that even if customization is not mandatory to deploy a unified platform, it must still allow for third-party integration and customizations through an SDK or API. Such tools must be available to allow end users to design and maintain the custom integrations beyond their video and access control applications, and not rely solely on the unified platform manufacturer for these initiatives down the road.

The Unified Server Infrastructure

A truly unified platform optimizes resources by sharing common servers and databases for:

- Authentication and permissions
- Licensing
- Configuration settings
- Alarms and events
- Audit and activity log
- Video recording
- Access logs

This type of architecture is easier to install and manage because it consists of a single software suite to learn, configure, upgrade, and backup unlike the integrated system where these tasks must be done for all implicated systems.

A centralized server infrastructure also simplifies the end user's life because the user only needs to connect to a single server by using a single login. From that connection, they have access to all services offered by the unified platform. They no longer have to connect to different servers while conducting both video and access control investigations.

Unification from the server all the way up to the interface offers advantages beyond the end user's initial needs such as:

- Greater efficiency through the use of a single interface
- Automated event correlation across systems
- Cost-effectiveness from shared configuration and maintenance

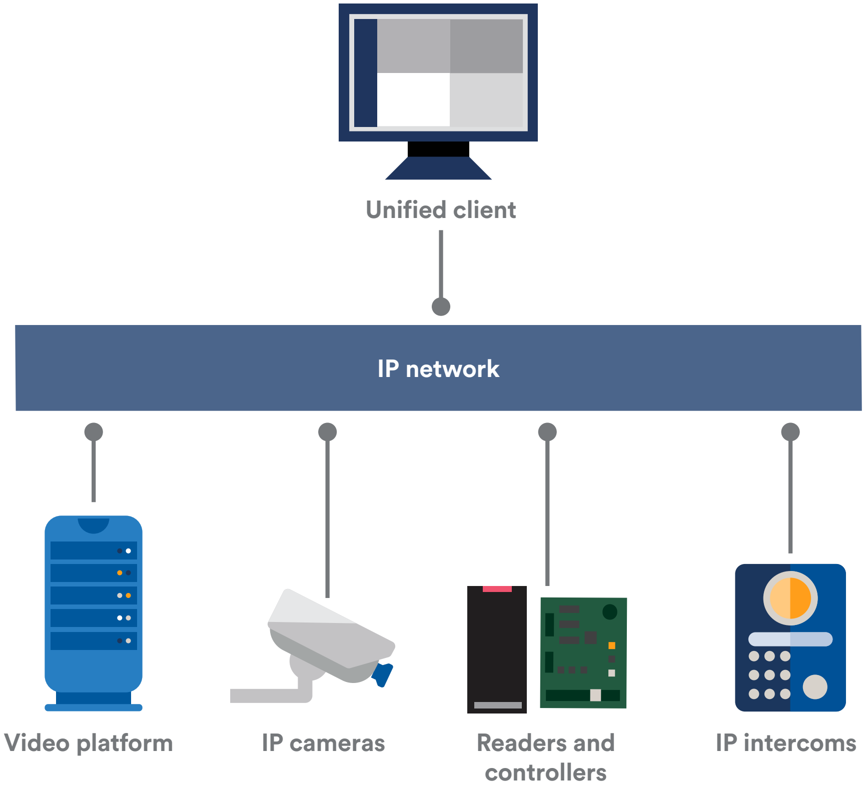


Figure 2 - Unified platform architecture

The User Experience

A single user interface for multiple security applications allows operators to easily and efficiently move from one security task to another within the same interface, thus avoiding complicated workflows and interface manipulations to reach the required window.

The user's workflows are consistent between the video and access control tasks so the user becomes more familiar with the system, experiences self-learning, and gains more confidence in their ability to use the system.

More so, the total number of workflows to understand is reduced by having common core functions. For example, alarm management, event to action, reporting, investigation, and incident-related workflows are all the same regardless of whether it is for video, access control, or voice communications.

As unified systems share a common user interface, switching from one application to another is seamless, and less time is required to train new operators on individual systems.

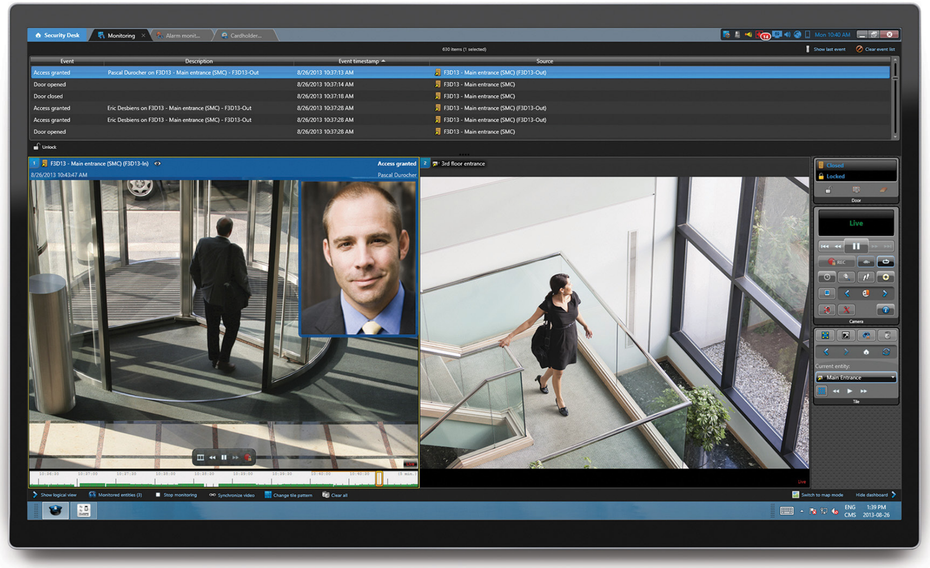
Event Correlation

A unified system is designed to offer event correlation because events and alarms are managed by a single server infrastructure. Access and video events are correlated to allow operators to rapidly review alarms in the system. For example, an operator can quickly validate a cardholder's identity when an access event occurs, in order to ensure the authenticity of a credential.

A unified platform with good event correlation can significantly reduce investigation time by filtering out false alarms.

Ease of Maintenance and Support

With a unified system, only a single software platform needs to be upgraded and maintained unlike an integrated solution where multiple individual systems must be addressed. This greater convenience allows integrators to
save time when upgrading the security system, and also enables them to coordinate with a single manufacturer should support be required. This also allows end-users to minimize system downtime during upgrades, and ensures a quicker response time to address the requirements of their system.



Event	Description	Event timestamp	Source
Access granted	Pascal Durocher on F3D13 - Main entrance (SMC) - F3D13-Out	8/26/2013 10:37:13 AM	F3D13 - Main entrance (SMC) (F3D13-Out)
Door opened		8/26/2013 10:37:14 AM	F3D13 - Main entrance (SMC)
Door closed		8/26/2013 10:37:18 AM	F3D13 - Main entrance (SMC)
Access granted	Eric Desbiens on F3D13 - Main entrance (SMC) - F3D13-Out	8/26/2013 10:37:28 AM	F3D13 - Main entrance (SMC) (F3D13-Out)
Access granted	Eric Desbiens on F3D13 - Main entrance (SMC) - F3D13-Out	8/26/2013 10:37:28 AM	F3D13 - Main entrance (SMC) (F3D13-Out)
Door opened		8/26/2013 10:37:28 AM	F3D13 - Main entrance (SMC)

What about PSIM?

Physical security information management (PSIM) is a software product able to supervise multiple distinct systems. The primary function of a PSIM is to manage information coming from different systems and present them inside a single user interface.

As opposed to a unified platform, a PSIM does not generally have a built-in access control, intrusion, or video surveillance solution. Instead, it integrates different systems through proprietary SDKs and APIs. Compatibility challenges could also arise when one of the sub-systems requires an upgrade or maintenance. Additionally, every system integrated within a PSIM has to be configured separately and there is a great degree of redundancy and duplicated effort (e.g., configuring users within a PSIM and the underlying access control, video, voice communications, and intrusion systems).

On the other hand, a PSIM integrates with a wider range of products because they custom-build the system on top of multiple security systems within a corporation. Nonetheless, opting for a PSIM can be difficult and expensive.

The disadvantages of custom integrations within a PSIM and the associated long-term costs to maintain support for a range of highly customized products, have to be objectively considered when selecting the best security technology for an organization's needs.

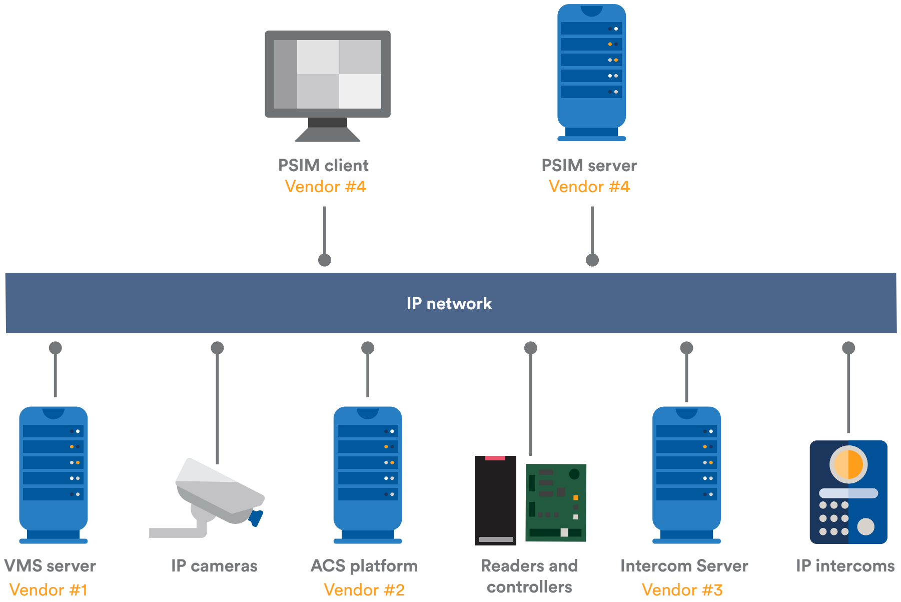


Figure 3 - Disadvantage of a PSIM architecture vs. a unified platform architecture

Choosing a Solution

Are you being efficient, flexible and cost-effective in the way you approach video and access control integration?

As you've read in the previous pages, there are many ways to deploy a physical security system that includes both video surveillance and access control. Although interfacing and integration are the most commonly deployed methods, open-platform unification offers the most efficient, flexible and cost-effective video and access control applications.

That is why it is important to take a moment to see if you are employing the most optimal method of unifying your video and access control systems. The answer could help you save time and reduce costs.

About Genetec

Genetec™ develops open-platform software, hardware and cloud-based services for the physical security and public safety industry. Its flagship product, Security Center, unifies IP-based video surveillance, access control and automatic license plate recognition (ALPR) into one platform. A global innovator since 1997, Genetec™ is headquartered in Montreal, Canada, and serves enterprise and government organizations via an integrated network of resellers, integrators and consultants in over 80 countries. Genetec™ was founded on the principle of innovation and remains at the forefront of emerging technologies that unify physical security systems. For more information about Genetec™, visit: genetec.com

Find out why Genetec fits.

genetec.com

Genetec™