Universal Library of Business and Economics Original Article

ISSN: 3064-9951 | Volume 1, Issue 2

Open Access | PP: 63-65

DOI: https://doi.org/10.70315/uloap.ulbec.2024.0102012

# Pavel Mishchenko on "Seamless" Integration: How to Make Video Surveillance, Access Control Systems and Security Systems Work as a Single Whole

**Pavel Mishchenko**

Specialist in IT Infrastructure and Integrated Security of Critical Facilities.

## Abstract

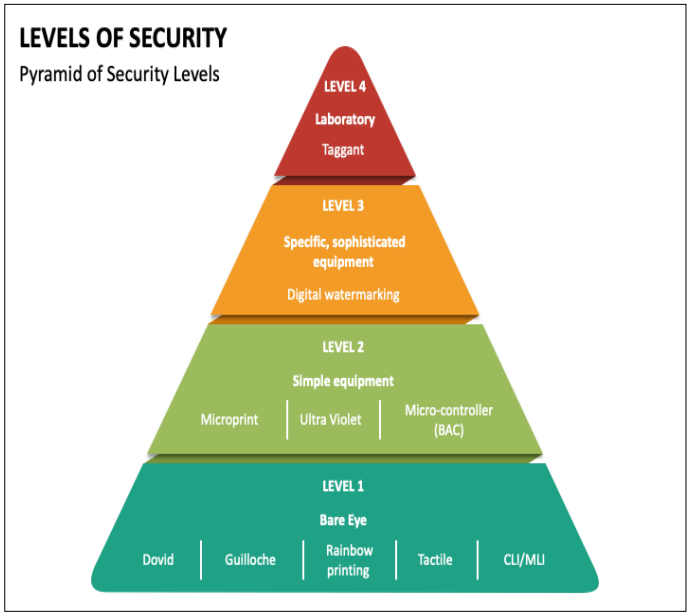
*The article considers the problem of fragmentation of corporate security systems and analyzes approaches to their "seamless" integration. The purpose of the study is to systematize methodologies and technological solutions for creating a single, synergistically operating complex of video surveillance, access control and management (ACS) and security alarm systems. An analysis of various integration levels is carried out: from hardware to platform, with an emphasis on the use of software interfaces (API) and specialized physical security management platforms (PSIM). The study found that complex integration increases situational awareness, automates response procedures and significantly reduces the operator's decision-making time. The practical significance of the work lies in the formation of a sound approach for security managers and IT specialists in the design and modernization of security systems at critical facilities, which allows moving from a reactive model to proactive incident management.*

**Keywords:** *Integrated Security Systems, PSIM, Video Surveillance, ACS, Security Alarm, Situational Awareness, Incident Management, Critical Infrastructure.*

Ensuring the security of critical facilities in modern conditions requires the use of comprehensive measures, including video surveillance, access control and alarm systems. However, in practice, these components often function as isolated, "island" solutions from different manufacturers. This fragmented approach creates serious obstacles for effective monitoring and rapid response to threats, as the operator has to work with several unrelated interfaces, and comparing data from different systems takes up valuable time. The relevance of the topic is due to the increasing complexity of threats and the need to reduce the response time to incidents. The purpose of the article is a systematic analysis of methodological and technological approaches to creating a single security contour through the seamless integration of video surveillance, ACS and security systems.

## The Concept and Levels of Security System Integration

Traditionally, security systems have operated autonomously. The video surveillance system recorded video, the ACS controlled the access points, and the burglar alarm system recorded unauthorized intruders. The integration of these systems implies the creation of logical links between them, allowing them to exchange data and run automated scripts. Experts in the field of IT infrastructure identify several levels of integration.




The initial level is hardware based on the use of "dry contacts" (relay outputs). For example, the door opening sensor of the security system closes the relay, which, in turn, activates the recording on the surveillance camera. This method is reliable, but has limited functionality.

The next level is software, which involves the interaction of systems through the SDK (Software Development Kit) or API (Application Programming Interface). This approach allows

you to implement more complex scenarios, for example, to transfer data about the cardholder from the ACS to overlay this information on the video stream. As M.L. Garcia notes, the effectiveness of a physical protection system depends on its ability not only to detect, but to classify and verify threats, which is practically impossible without software communication between subsystems [1].

The highest level is platform integration. It is implemented using high-end video management systems (VMS) or specialized physical security information Management Platforms (PSIM).

## Technological Implementation and Interaction Protocols

The practical implementation of seamless integration directly depends on the protocols used. For a long time, the development of the market was hindered by the use of closed, proprietary protocols by manufacturers, which made it difficult to combine equipment from different brands into a single system. This has changed with the advent of open industry standards such as ONVIF for IP video cameras and OPC (Open Platform Communications) for industrial automation and security systems. The use of standardized protocols guarantees basic device compatibility.

Modern systems are increasingly providing developers with a RESTful API, which provides virtually unlimited opportunities for deep customized integration. This allows not only to link security systems together, but also to connect them to corporate business systems such as ERP and HRM [2]. Choosing hardware and software with open and well-documented APIs is a fundamental prerequisite for building a flexible and scalable integrated system.

**Synergetic effect:** automated scenarios

The main value of integration is to create a synergistic effect in which the capabilities of the combined system exceed the sum of the capabilities of its individual parts. This is achieved through automated scripts (macros) that are triggered when a certain event occurs.

Let's take a practical example. The motion sensor of the security system is activated on the perimeter of the facility. In an isolated system, the operator will hear a signal and will have to manually find the right camera on the object's diagram in order to assess the situation. The following happens in an integrated system:

1. The signal from the sensor is instantly transmitted to the PSIM platform.

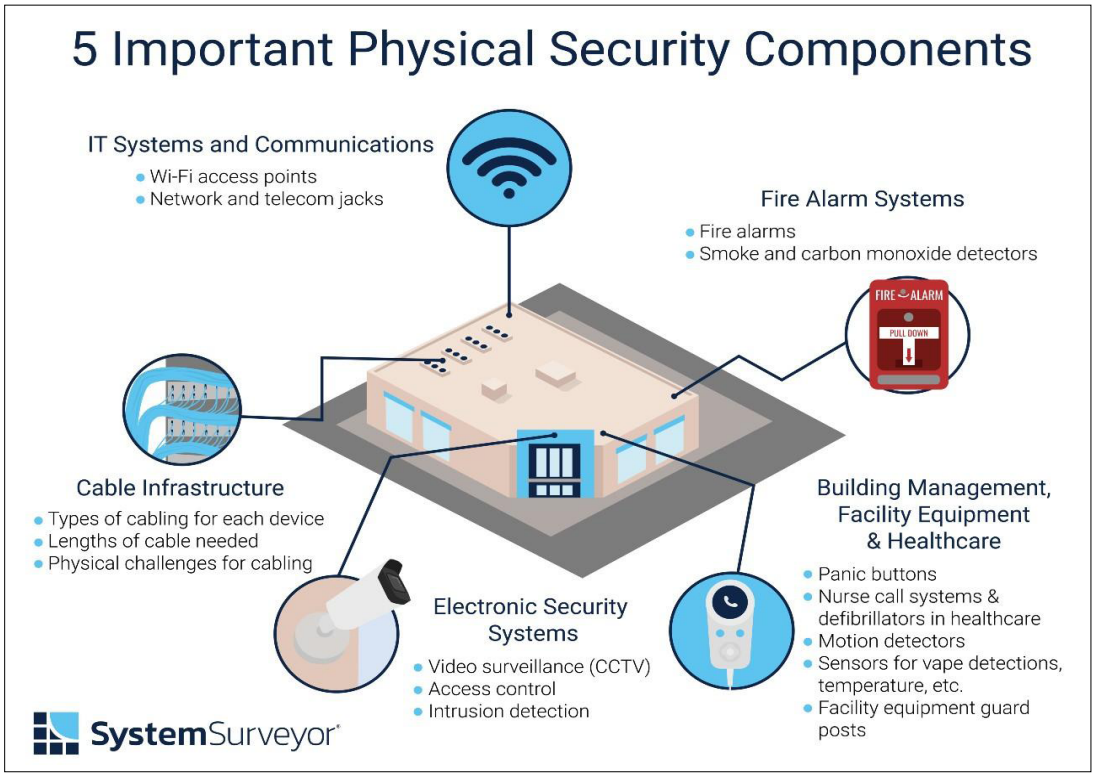
The system automatically displays an image from the nearest camera on the operator's alarm monitor.

2. If the camera is rotary-tilt (PTZ), it is automatically aimed at the operating location.

The system can automatically block the nearest access points of the ACS to isolate the intruder.

3. Instructions with a step-by-step action plan appear on the operator's screen.

This level of automation minimizes the influence of the human factor, reduces reaction time from minutes to seconds, and allows the operator to focus on decision-making rather than on routine interface manipulation [4].



## Platform Approach: PSIM as the Central Core

PSIM (Physical Security Information Management) class systems represent the pinnacle of the integration approach. These are software platforms designed not to manage individual devices, but to aggregate and analyze information from all connected security systems [3].

The PSIM platform collects events from ACS, security sensors, video analytics, fire alarm systems, and other sources. It then correlates these events, screening out false alarms and identifying complex threats. All information is presented to the operator on a single graphical interface, usually on an interactive map of the facility. The most important function of PSIM is incident management. The platform provides the operator with standardized workflows (SOPs) that guide him through the steps necessary to resolve a specific situation. This ensures uniformity and predictability of reaction even under stressful conditions.

An analysis of the principles of security system integration shows that the transition from isolated subsystems to a single platform is a necessary stage of evolution to ensure an adequate level of protection for critical facilities. The seamless integration of video surveillance, ACS, and alarm systems allows for a synergistic effect, which is reflected in increased situational awareness, drastically reducing response time, and reducing the burden on operators.

The technological basis for such integration is open protocols and programming interfaces (APIs), and the highest form of its implementation is platforms of the PSIM class. Despite the higher initial investment compared to the deployment of disparate systems, the integrated approach provides significantly higher efficiency and pays off by reducing risks and optimizing the work of security personnel. For modern enterprises, the creation of a single safety management circuit is not a technological option, but a strategic necessity.

## REFERENCES

1. Garcia, M. L. The Design and Evaluation of Physical Protection Systems. – 2nd ed. – Butterworth-Heinemann, 2007. – 360 p.
2. Zachariadis, M., Ozcan, P. The API Economy and Digital Transformation in Financial Services: The Case of Open Banking // SWIFT Institute Working Paper No. 2016-001. – 2017. – 28 p.
3. Security. The Rise and Fall and Rise of PSIM. – 2024. URL: https://memoori.com/the-rise-and-fall-and-rise-of-psim/
4. How Integrated Security Approaches are Transforming Physical Security. – 2020. URL: https://www.owlknows.com/how-integrated-security-approaches-are-transforming-physical-security/

**Citation:** Pavel Mishchenko, "Pavel Mishchenko on "Seamless" Integration: How to Make Video Surveillance, Access Control Systems and Security Systems Work as a Single Whole", Universal Library of Business and Economics, 2024; 1(2): 63-65. DOI: https://doi.org/10.70315/uloap.ulbec.2024.0102012.