World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Five key mistakes in deploying security systems at large facilities: Analytics and practical advice

Pavel Mishchenko *

Specialist in IT infrastructure and integrated security of critical facilities.

World Journal of Advanced Research and Reviews, 2025, 27(01), 1337-1340

Publication history: Received on 01 June 2025; revised on 13 July 2025; accepted on 15 July 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2620

Abstract

The article systematizes and analyzes five typical system errors that occur when deploying complex security systems at critical and industrial infrastructure facilities. Based on the analysis of current scientific publications and generalization of practical experience, including the case of the El Dabaa NPP construction from Pavel Mishchenko, the study identifies weaknesses in modern approaches to design and installation. The purpose of the work is to provide engineers and project managers with a scientific and practical basis for minimizing risks and increasing the overall reliability of security systems. The article discusses errors associated with the lack of system integration, ignoring the physical level of infrastructure, underestimating the human factor, false economic optimization, and lack of planning for the full life cycle of the system. The results of the study can be applied to the development of project management methodologies in the field of industrial safety, as well as to improve the skills of technical personnel.

Keywords: Integrated Security Systems; Critical Infrastructure; Systems Integration; Risk Management; Structured Cabling Networks (SCN); Human Factor; System Life Cycle; Industrial Safety

1. Introduction

In the context of increasingly complex technological processes and rising global threats, ensuring the security of large industrial and critical infrastructure facilities has become a top priority. Modern physical security systems (PSS) are complex, multi-component structures that include subsystems such as video surveillance, access control systems (ACS), intrusion alarms, and network infrastructure. However, as practice shows, the high cost and technological sophistication of individual components do not guarantee the reliability of the overall system. The effectiveness of a PSS depends not so much on the quality of individual devices as on the proper integration and management of these components throughout the entire system lifecycle [1].

The relevance of this study lies in the existing gap between theoretical models of security system design and the practical realities of their implementation, where design and management errors often result in vulnerabilities. The purpose of this article is to identify, classify, and analyze five of the most common systemic mistakes, based on a synthesis of academic research and the practical experience of professionals particularly Pavel Mishchenko, an expert in IT infrastructure and integrated security for critical infrastructure.

1.1. Fragmented Approach vs. System Integration

The theoretical foundation of modern security system design is the concept of systems engineering, which views a PSS as a unified organism rather than a mechanical sum of its parts. Leading researchers, such as Mary Lynn Garcia, emphasize that the effectiveness of physical protection relies on the synergy between its core elements: detection, delay,

[*] Corresponding author: Pavel Mishchenko

and response [3]. However, in real-world applications, a fragmented approach often prevails where video surveillance, access control, and alarm systems are designed and operated in isolation.

This error leads to decreased situational awareness among personnel and longer incident response times. While an integrated system can automatically verify an intrusion alarm by displaying the nearest camera feed and locking down the relevant perimeter using ACS, a non-integrated setup requires the operator to manually coordinate across multiple disconnected interfaces.

Practical experience from large-scale projects such as the construction of the El-Dabaa Nuclear Power Plant confirms the critical need for deep integration. Within this project, efforts are focused on connecting equipment and protocols from various vendors, including pre-existing local systems and newly implemented Russian platforms. The objective is to create a “seamless” environment in which data from different sources is consolidated and analyzed centrally, ensuring the full and reliable operation of the entire security complex.

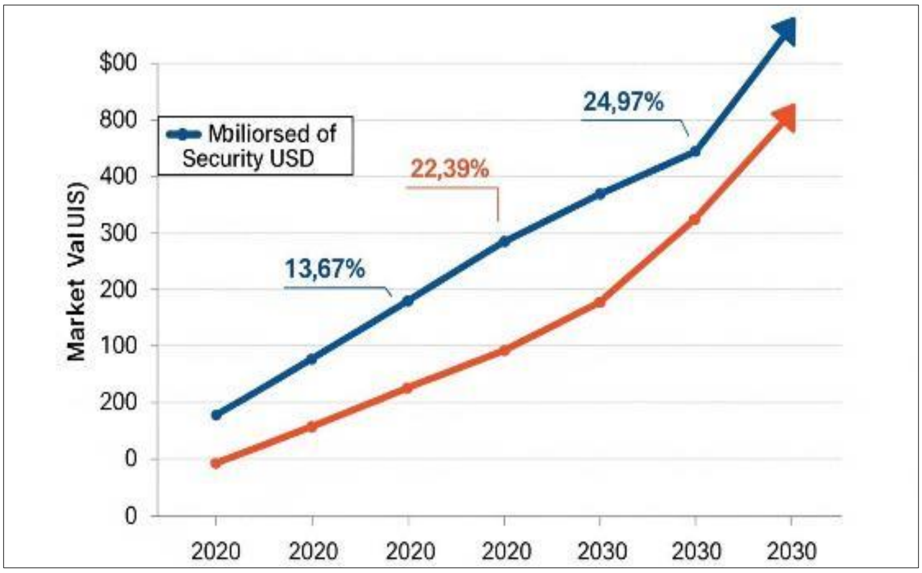


Figure 1 Global integrated security system market growth

1.2. Neglecting the Physical Layer of Infrastructure

The reliability of a hardware-software complex directly depends on the quality of its physical foundation. In many cases, during the design phase, most attention is given to the selection of servers and cameras, while passive network infrastructure in particular, structured cabling systems (SCS) is undervalued. According to analytical reports, a significant share of IT system failures is caused specifically by issues with cable infrastructure [4].

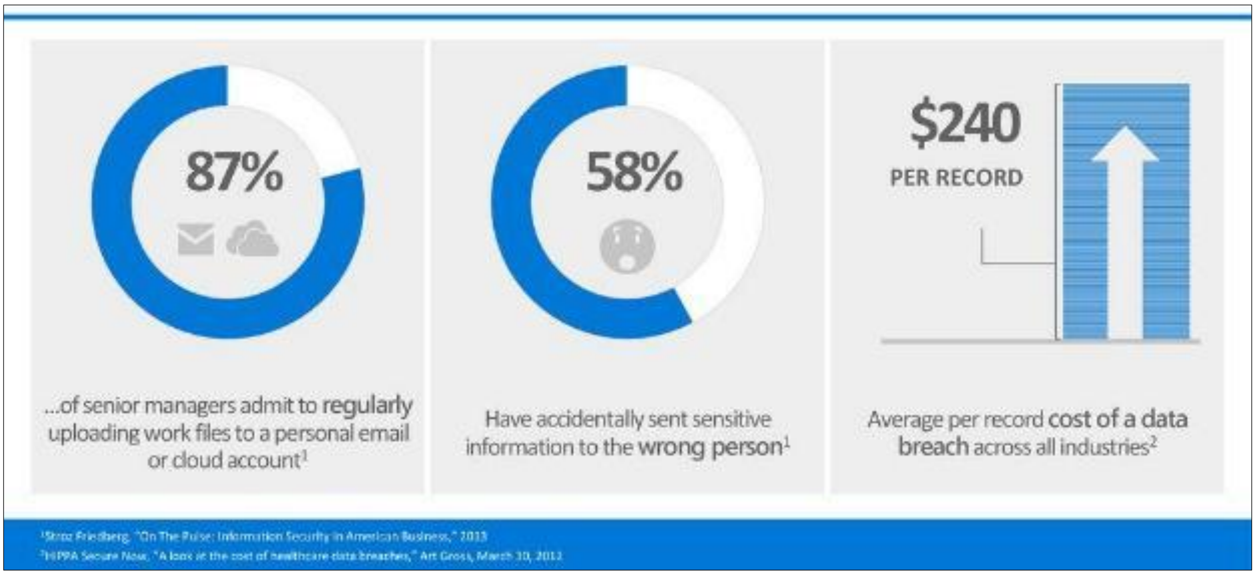
This oversight is critical, as SCS represents a long-term investment, and its replacement or repair in a functioning large-scale facility entails significant costs. A results-oriented practical approach requires that principles of high-quality installation, durability, and ease of maintenance be embedded into the design from the beginning. Using high-grade components and strictly following installation standards ensures stable data transmission and minimizes the risk of equipment failure. Cost-cutting at this stage is a false economy that leads to disproportionately high operational expenses in the future.

1.3. Underestimating the Human and Cross-Cultural Factors

Every technological system no matter how advanced is ultimately operated by people. Research in cybersecurity and physical protection consistently shows that the human factor remains one of the most vulnerable links [2]. eratorerrors, failure to follow protocols, lack of qualifications, or low motivation can completely negate the advantages of expensive equipment.

When deploying systems at international sites such as the nuclear power plant in Egypt this issue is further complicated by cross-cultural differences. Working in a team composed 50% of local personnel requires the management to develop specific approaches to communication and training. Formal instructions may prove ineffective if they fail to take local cultural specifics into account.

Experience shows that the most effective method is mentorship and knowledge transfer through joint practical work. Direct demonstration of correct practices and a focus on hands-on skills help overcome both language and cultural barriers, establishing shared quality standards within a mixed team.



[1] Stroz Friedberg, "On The Pulse: Information Security in American Business," 2013
[2] HIPPA Secure Now, "A look at the cost of healthcare data breaches," Art Gross, March 30, 2012

Figure 2 Data leakage

1.4. False Economy and Lack of Lifecycle Planning

The drive to reduce initial capital expenditures often leads to the selection of equipment and solutions that prove to be inefficient in the long term. This approach ignores the Total Cost of Ownership (TCO), which includes not only procurement costs, but also those related to installation, operation, maintenance, upgrades, and disposal. The principle of "smart economy," applied by experienced professionals, is based not on choosing the cheapest components, but on designing a system with an optimal balance of cost, quality, and durability.

Closely related to this is the mistake of failing to plan for the system's entire lifecycle. A project does not end at the installation and commissioning phase. It is essential to plan in advance for maintenance procedures, scalability, and the upgrading of outdated equipment. A system designed without consideration for maintainability will, in the future, require significant effort even for routine operations, which leads to increased downtime and higher operating costs.

2. Conclusion

An analysis of theoretical sources and practical experience in deploying complex security systems at large facilities leads to the conclusion that most failures are caused not by technological flaws, but by systemic and managerial errors.

The five identified issues fragmentation, neglect of the physical and human factors, false economy, and lack of lifecycle planning are interrelated and stem from a departure from the principles of systems engineering.

Recommendations

To improve the effectiveness and reliability of security systems at critical infrastructure facilities, it is recommended to

- Apply an integrated approach, treating all security subsystems as a unified whole throughout the design and implementation stages.
- Pay increased attention to the quality of physical infrastructure, especially structured cabling systems, incorporating principles of durability and maintainability into the project.
- Develop and implement training and motivation programs for personnel, taking into account site-specific and cultural contexts.
- Make decisions based on a total cost of ownership assessment, rather than only initial capital expenditures.
- Design systems with the entire lifecycle in mind, planning in advance for maintenance, scaling, and modernization.

The implementation of these recommendations will enable a shift from reactive problem-solving to proactive risk management, ensuring a consistent and high level of protection for critical infrastructure.

References

[1] Fennelly, L. J., and Perry, M. A. (2016). Effective Physical Security (5th ed.). Butterworth-Heinemann.

[2] Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). Wiley.

[3] Garcia, M. L. (2007). The Design and Evaluation of Physical Protection Systems (2nd ed.). Butterworth-Heinemann.

[4] Patterson, D. A., and Hennessy, J. L. (2020). Computer Organization and Design RISC-V Edition: The Hardware Software Interface (2nd ed.). Morgan Kaufmann.

[5] Blanchard, B. S., and Fabrycky, W. J. (2010). Systems Engineering and Analysis (5th ed.). Pearson.