VOLUME 23 | NOVEMBER 2026 | ISSUE 4 | 17 €

GIT SECURITY INTL

79 824

TY AND SECURITY – WORLDWIDE

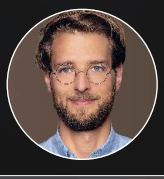


CSO INTERVIEW
Alexandra Forster: Global Threats & Crisis Management at Bayer · p 8



CRITICAL INFRASTRUCTURE
Michèle Knodt: Resilience in Times of Crisis · p 12

SMART PORTS
Port de Barcelona: Video Becomes Business Intelligence · p 42



VIP:
Ferdinand Gehringer · p 66

LivEye Cover Story page 36

More than a Video Tower

Carsten Simons: Security is just the Beginning



GIT SECURITY AWARD
The Winners 2027 · p 18

A BEST-OF IN PRINT

More news, full case studies & tech reports on www.GIT-SECURITY.com

WILEY



© TensorSpark - stock.adobe.com

SECURITY MANAGEMENT

PSIM for Critical Infrastructures

Operational Resilience: Balancing Security Management, Regulation and Auditability



© Advancis

Is a Physical Security Information Management (PSIM) system more than just an integration platform for threat alerts—namely, a building block of modern RegTech strategies for operators of critical infrastructure? An article by Dr. Jens Hartmann of Advancis.

The term "RegTech" (Regulatory Technology) originated in the financial sector and describes technologies that help companies efficiently implement regulatory requirements and, above all, ensure their transparency. At its core, the focus is less on the measure itself and more on its structured, verifiable implementation in day-to-day operations. This perspective is also becoming increasingly important in the critical infrastructure environment as regulatory requirements undergo fundamental changes.

New Regulatory Framework

With the introduction of the NIS2 Directive, the EU Critical Infrastructure Resilience Directive (CER), and national regulations such as the Critical Infrastructure Framework Act, a regulatory framework is emerging that no longer merely requires the establishment of security measures but focuses on their actual effectiveness in operation. Operators of critical infrastructure must no longer merely demonstrate that processes exist, but that these processes function in the event of an incident—and that this functionality can be reliably verified. Security is thus evolving from a conceptual discipline into an operational capability whose implementation must be verifiable.

In practice, however, it is evident that many organizations of critical infrastructures face significant challenges precisely in this area. At the conceptual level, many large operators are well-positioned. Security policies, risk analyses, business continuity plans, and incident response processes are defined and documented.

Technically as well, there is a wide range of specialized systems covering various aspects of security—from IT security solutions and monitoring platforms to physical security technologies such as access control, video surveillance, and fire alarm systems. From a formal standpoint, this means the requirements mandated by regulation are met.

Lack of Operational Consistency

However, when an actual incident occurs, the reality is often quite different. When a security-related incident occurs, a large amount of information from various systems converges within a short period of time. Multiple organizational units are involved, decisions must be made under time pressure, and processes evolve dynamically. It is precisely in these situations that gaps arise. Processes are not always implemented consistently, decisions depend on individual experience, information is fragmented, and documentation often takes place only after the fact. The actual problem, therefore, lies not in a lack of regulation or a lack of strategies, but in a lack of operational consistency and traceability.

This discrepancy between defined processes and actual practice is becoming increasingly critical due to current regulatory developments. Regulatory authorities no longer ask merely whether a process exists, but whether it was followed in a specific case. They expect traceable escalation chains, documented decisions, and the ability to fully reconstruct the course of an incident. As a result, operational implementation itself becomes the subject of scrutiny. This is precisely where a structural gap arises that many organizations have not yet closed.

This gap lies between the conceptual level of security processes and their operational implementation. Processes are defined, but their execution is not consistently system-supported. Different systems provide information but do not control the workflow. Decisions are made on a case-by-case basis, workflows vary, and documentation is not fully integrated. This separation has developed historically but is becoming increasingly problematic due to new regulatory requirements. This is because resilience is now viewed holistically. Physical events can affect digital systems, and IT incidents can trigger physical measures. Without an integrated implementation layer, this complexity remains difficult to manage.

PSIM Takes on New Meaning

This is where Physical Security Information Management (PSIM) systems take on new strategic importance. PSIM systems are traditionally viewed as integration platforms that bring together various security and hazard detection systems. They consolidate information from fire alarm systems, video surveillance, access control, and perimeter security, and display it in a unified interface. But this description falls short. The true strength of PSIM lies not only in the integration of data, but also in the structuring and control of operational processes.

PSIM digitizes, standardizes, and orchestrates security procedures in the event of an incident. An alarm is not merely displayed but is automatically routed into a defined process. Operators are guided through structured workflows, escalation levels are supported by the system, and measures are implemented consistently. At the same time, every step is automatically documented. This results in a new level of quality in operational execution. A theoretically defined process becomes an actual, reproducible workflow.

A key advantage lies in the way documentation is generated. In many organizations, documentation is still done after the fact, often manually and under time pressure. This leads to gaps, inconsistencies, and a high workload. PSIM reverses this principle. Documentation is not created after the event, but during its handling. Every step—from the initial alarm notification through decisions made to actions taken and escalations—is automatically recorded. The result is a continuous audit trail that enables complete reconstruction and is admissible for regulatory purposes. Thus, maintaining audit trails is no longer an additional task but an integral part of the operational process.

Pioneer Financial Sector

This trend is particularly evident in the financial sector, which plays a pioneering role as part of critical infrastructure. Under the Digital Operational Resilience Act (DORA), banks must demonstrate their ability to maintain operations even in the event of disruptions. This applies not only to IT systems but to overall operational resilience. Banks exemplify how strongly regulatory requirements today focus on the actual implementation of processes and how important reproducible, documented procedures are. At the same time, it is becoming clear that physical security, IT security, and organizational processes can no longer be viewed in isolation.



With the increasing use of artificial intelligence, the possibilities continue to expand. AI can analyze large amounts of data, recognize patterns, and support decision-making processes. In complex environments of critical infrastructures, this enables efficiency gains, such as through the prioritization of alerts or the detection of anomalies. At the same time, however, the requirements for transparency and traceability are increasing. Regulatory requirements demand explainable decisions and human oversight. AI may therefore support processes, but it must not become a "black box" that eludes scrutiny.

For operators of critical infrastructures, this results in a fundamental shift in perspective. Security is no longer understood primarily as a protective measure, but rather as the ability to ensure stable, traceable operational management. What matters is not only what is done, but also how consistently and thoroughly it is documented. PSIM supports this transformation by standardizing, structuring, and making operational workflows traceable. This results in reproducible processes, consistent decisions, and robust evidence. At the same time, reliance on individual decisions is reduced, and the quality of operations improves.

PSIM in the Context of RegTech

Against this backdrop, PSIM can also be viewed in the context of RegTech. PSIM is not RegTech in the traditional sense and does not replace regulatory frameworks or governance structures. Functionally, however, it fulfills a role typical of RegTech: providing technical support for verification and compliance processes. PSIM translates regulatory requirements into operational reality and makes them verifiable. This creates a link between security operations and regulatory expectations.

Regulatory developments in the critical infrastructure environments will continue to accelerate in the coming years. With NIS2 and CER, an environment is emerging in which physical, digital, and organizational security must be considered in an integrated manner. Technologies that combine operational implementation with the ability to demonstrate compliance will play a central role in this context. In this context, PSIM is evolving from an integration system into an operational resilience platform.

The initial question can thus be clearly answered. PSIM is not RegTech in the strict sense. However, in the critical infrastructure environment, it is becoming a central technological building block—not only for meeting regulatory requirements but also for consistently implementing them in day-to-day operations and providing robust evidence of compliance. GIT

Advancis Software & Services
https://advancis.net

© JK2507 - stock.adobe.com