smart cities

MDPI

Article

Converged Security and Information Management System as a Tool for Smart City Infrastructure Resilience Assessment

Martin Hromada [1,*], David Rehak [2], Bartosz Skobiej [3] and Martin Bajer [1]

[1] Faculty of Applied Informatics, Tomas Bata University in Zlin, Nad Stranemi 4511, 760 05 Zlin, Czech Republic; bajer@utb.cz
[2] Faculty of Safety Engineering, VSB—Technical University of Ostrava, Lumirova 13, 700 30 Ostrava, Czech Republic; david.rehak@vsb.cz
[3] German Aerospace Center, Institute for the Protection of Maritime Infrastructures, Fischkai 1, 27572 Bremerhaven, Germany; bartosz.skobiej@dlr.de
* Correspondence: hromada@utb.cz; Tel.: +420-576-035-243

Abstract: Current research on smart cities is primarily focused on the area of applicability of information and communication technologies. However, in the context of a multidisciplinary approach, it is also necessary to pay attention to the resilience and converged security of individual infrastructures. Converged security represents a particular security type based on a selected spectrum of certain convergent security types of, assuming the creation of a complementary whole. Considering the outputs of the analysis of security breaches manifestations, this kind of security makes it possible to detect emerging security breaches earlier (still in the symptom stage), thus providing a more efficient and targeted solution suitable for building smart city infrastructure. In its essence, the article refers to the practical application of the converged security theoretical principles presented in the publication to a functional sample, deployed and tested in practical conditions in context of selected smart city infrastructure protection and resilience. Considering the nature of the practical application, the convergence of a wider spectrum of smart security alarm systems in the resilience assessment context is defined. In the beginning, the general principles of security/safety and the need for their convergence are presented. In this context, the mathematical model called Converged Resilience Assessment (CRA) method is presented for better understanding. Subsequently, Physical Security Information Management (PSIM) and Security Information and Event Management (SIEM) systems are described as a technological concept that can be used for resilience assessment. The most beneficial part is the structural, process, and functional description of the Converged Security and Information Management System (CSIM) using the concept of smart security alarm systems converged security.

Keywords: converged security; resilience assessment; smart security alarm systems; PSIM; SIEM; Converged Security and Information Management System (CSIM)

Citation: Hromada, M.; Rehak, D.; Skobiej, B.; Bajer, M. Converged Security and Information Management System as a Tool for Smart City Infrastructure Resilience Assessment. *Smart Cities* **2023**, *6*, 2221–2244. https://doi.org/10.3390/smartcities6050102

Academic Editors: Katarzyna Turoń and Andrzej Kubik

Received: 1 August 2023
Revised: 17 August 2023
Accepted: 21 August 2023
Published: 25 August 2023

1. Introduction

A smart city is a concept of city operation that uses digital, information and communication technologies in order to make more efficient use of its infrastructure, reduce resource consumption and overall costs, and fulfil the goals of industries [1,2]. However, to achieve such goals, a high level of security and protection of key infrastructures, which are designated as critical [3,4], is necessary.

1.1. The Importance of Security

Security in its nature is one of the important phenomena of today's society in its wider context. In the last decades, security is starting to be considered a scientific field with its own subject of investigation, goals, and methods. Security is ultimately ensured in society through individual types of security where a type of security can be perceived

as a measures catalogue associated with the need to ensure security within the selected reference object and its environment. Currently, the basic types of security/safety include international, physical, cyber, economic, energy, personal, informational, administrative, personnel, fire safety, product safety, or safety and health protection at work [5].

The common ambition to shape and develop the scientific field of security is inherently connected and conditioned by the security theory development [6]. The issue of security theory is relatively new, but it can be stated that currently there are already sets of theoretical knowledge that are used by individual security types, are proven and implemented in practice and fit into the mosaic of security theory. It is therefore clear that the security theory itself focuses on a systemic understanding of security, realizes the framing of the security problem by describing what a security breach is, in what general forms and what types of security breaches occur, what they depend on and how it is possible to prevent or minimize the impact level [7]. As stated, the increasing demand for security is pragmatically connected with the need for practice and therefore also with the security of infrastructure systems.

1.2. Smart City Infrastructure Resilience

The security and protection of the smart city infrastructure (SCI) is often connected with the fact that individual infrastructures are interconnected horizontally and vertically, which represents to some extent the system of systems concept [8]. Concerning the interconnectedness, it is also possible to discuss their mutual dependence (interdependence), where the mutual dependence of SCI created a prerequisite for the classification of the linkages typology. It is therefore possible to consider physical, cyber, logical, or geospatial linkages as basic linkages. This statement points to the fact that one of the basic characteristics of SCI is its network nature [9]. In connection with the issue in question, the network character needs to be perceived in a broader context, where it is not only technical networks such as e.g., transport, logistics, communication and energy, but also abstract economic, financial, social and knowledge networks [10]. It is therefore obvious that an isolated and limited understanding of security and protection has only a limited effect and it is necessary to relate this understanding to the security convergence of individual infrastructures.

In this context, however, it is necessary to determine a uniform indicator by which this security will be measured. In the case of critical infrastructures, the level of resilience of these infrastructures has been used for this purpose for a long time [11]: *"Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event"*. Based on this definition, it can be stated that infrastructures with a high level of resilience are a prerequisite for the successful construction of smart cities [12,13].

1.3. The Importance of Converged Security in the Context of Smart City Infrastructure Resilience

Converged security in the context of resilience does not differentiate between Safety and Security [14]. In both cases, it is the aforementioned joining (convergence) of aspects and measures of individual security types into a complementary whole, which reflects prerequisite for increasing resilience in related security types. This approach reduces to a certain extent the disadvantages of isolated and closed use of the Safety and Security measures spectrum [15]. At the same time, the use of the convergence philosophy in the resilience context makes it possible to consider the network nature of SCI. This is based on the sense of cascading and synergistic effects [16]. Considering the scientific activity of the authors, the security and protection of SCI elements will be perceived with a specific link to physical security and therefore smart security alarm systems use in the context of increasing the efficiency and effectiveness of physical protection systems [17]. Another point of view is the creation of an integral security system in connection with resilience determinants, the influence of cascading and synergistic effects and the final security convergence and resilience aspects of SCI elements [18]. The benefit of converged security in this context is

the convergence of relevant security types into a functional system. This can be seen as a prerequisite for increasing resilience in related security types [19].

Convergence issues in the context of security were solved in the past in connection with a holistic approach to risk management. In this context, however, there is a convergence of entities and thus participants and attributes entering and responsible for optimizing risk management in broader contexts [20–22]. Aspects of convergence were subsequently linked primarily to issues and needs of information security. In its nature, however, there was not a convergence of several selected types of security, but a convergence of selected approaches within one type of security [23,24].

The logical evolution of the issue in question was the expansion of convergence approaches by the aspect of physical security as a basis for ensuring the functionality and security of information systems and thus the security of information assets [25–27]. The extension of convergence approaches to other types of security occurs sporadically in professional texts, but there is some indication of a significant potential to combine individual types of security into a complementary whole. However, it is clear from the articles in question that despite the effort to converge selected types of security, one dominant type of security is almost always determined, to which more space is devoted [28–30].

The convergence of security in its essence is connected with the correlation and processing of a large amount of sensory and system data and even in case when we put converged security and resilience into context. This fact and the presentation of systemic approaches to solving this challenge is not such a common topic. However, there is a limited spectrum of works devoted to it [31,32]. Considering what has been presented, it can be concluded that the ambition of the article is the convergence of equal types of security into a functioning complementary whole in the figurative sense of assessing and increasing the resilience of assets using an information system, enabling information and situational management of the security situation.

1.4. Smart Security Alarm Systems Convergence

A wide group of authors dealt with the security systems convergence issue. As an example, article [33] discussed approaches linked to a comprehensive understanding of cyber security. Another theoretical model was presented in [27,34]. The convergence of cyber security and just security using smart security alarm systems is elaborated in the publication [28] where the need for convergence physical access controls and cyber security was presented. Technologically more advanced approaches were subsequently presented in a publication [35], where AI and IoT approaches were converged.

A more specific connection to alarm systems was subsequently elaborated within the article about visibility and security in the smart home [36], where current security threats were reflected, including in the context of COVID-19. The convergence of a wide range of security solutions connected via IoT was simultaneously the subject of the monograph Convergence of Artificial Intelligence of Things [37]. Linking these systems to early warning systems as an added value of security systems convergence is presented in the publication Intelligent disaster safety warning system through risk level analysis [38].

Based on the analysis of current approaches, it is obvious that convergence with the use of smart security alarm systems is not a new issue, but it often works with the dominance of cyber security. In view of the stated, the aim of the article is to reverse this dominance and focus on converged security from the physical security perspective to which alarm systems belong. For this purpose, the authors created the Converged Security and Information Management System (CSIM), which enables an interconnected assessment of individual types of security, primarily physical, operational, and cyber. Based on this process, it is possible to determine the level of resilience for individual smart city infrastructures.

2. Materials and Methods

The text of this section will in principle be based on the general classification of security types, which can be understood as a model expression of the issue in question.

2.1. Classification of Security Types

In the security environment, the premise is accepted to a certain extent that security is a state when threats are reduced to the lowest possible level and the risks of the selected asset are minimized to the lowest possible level or acceptable level, and when the asset is effectively equipped for these minimization [39]. This premise to a certain extent points to the security indivisibility as a scientific field. In general, however, the opinion can be taken that security measures belonging to the Safety group reflect unintentional security threats, and security measures belonging to the Security group reflect intentional security threats and the risks resulting from them [40]. However, it is necessary to admit the fact that in security practice there would be examples that might not fully confirm this claim or would be a combination of both groups of measures.

The aspect of security threats and the risks resulting from them is therefore a fundamental basis for the definition and determination of security types. Therefore, the formulation of security types reflects to a certain extent the basic classification of security threats, which according to [41] is categorized into external threats (i.e., political, economic, social, technological, legislative, and ecological) and internal threats (i.e., procedural, personnel, and material).

Article [42] described another philosophical view on the classification of security types from the security models' point of view. Security models are understood in this context as "conceptual models" that describe the essence and method of ensuring the reference object security using verbal and visual methods. The model reflects the essence of measures through which security is ensured. Security can be ensured by a system of measures of a logical or physical nature. Logical measures include rules, management, education, negotiation, prediction, deterrence, encryption, etc. These measures are based on information and work with them. Physical type measures include barriers (fences, walls), shock absorbers, physical security, forces and assets of the armed forces, warning and alarm systems, supplies, etc. Basic security assurance models include mode model, proactive model, barrier model, preparedness model, model of collective security/common interest, reactive model, rule enforcement model, and deterrence model.

However, it should be noted that in a few models the essence of ensuring security is implemented in several ways. Therefore, they include several model variants. The rule enforcement model and the deterrence model are specific models and are auxiliary in their nature. When ensuring security itself, one the type of security model is used only in rare cases. Usually, security is ensured by a combination of measures falling under the agenda of several security models [43].

From the security type defining point of view in the context of converged security, security type represents a set of measures solving a specific group of security problems. This is a certain continuity of solving negative phenomena associated with security breaches. The goal of the introduced and implemented measures is to prevent damage or at least minimize the effects caused by security breaches. An example of a type of security is physical security, information security, occupational health and safety, road traffic safety and international security. Converged security combines operational security, physical security, and cyber security [19].

2.2. Converged Resilience Assessment

Assessing the resilience of infrastructures or individual elements can currently be implemented using a number of important methods, e.g., refs. [44–47]. However, a significant limitation of these methods is that they can only be used for assessing individual security threats. This means that they cannot be used to assess the resilience of two or more related threats. Considering the specifics and importance of the SCI and the relevant need to reflect the correlation of current security threats, the Converged Resilience Assessment (CRA) method [19] was selected for next work.

The added value of this method is the use of the security convergence philosophy for the needs of objective resilience assessment. In this context, there is a selected security types convergence, which are the most important from the selected infrastructures functionality

ensuring point of view. These are physical, cyber and operational security. The mentioned CRA method uses information and situational management, integrating sensors systems and their data flows into an effective managing and solving security events system. This methodology can be used for the individual assets that the evaluated SCI element contains and at the same time for the strategic level of electricity supply ensuring. The resulting value is subsequently expressed by the aggregation of individual resiliencies [19].

The added value of the CRA method is the ability to identify the resulting value of the selected SCI elements protection system resilience in context of converged security by determining the resilience indicator of the reference object R. The resilience indicator therefore reflects the security level of the reference object assets in relation to the identified risks and in relation to their convergence. The value of the dimensionless resilience indicator ranges from 100 to 0, where the value 100 reflects the upper limit and the value 0 the lower resilience limit.

It is clear from practice that converged security is related to several security types and simultaneously to several assets, logically, resilience must be assessed for each security type referring to the selected asset. Aggregation will then make it possible to determine the resulting resilience indicator for a different type of security (physical, cyber operational). The determination of the resulting resilience indicator for the reference object is subsequently based on the arithmetic mean of the individual asset's resilience indicator. The connection between the above variables is expressed in Equation (1):

$$R = \frac{1}{n}\sum_{i=1}^{n} S_i = \frac{1}{n}\sum_{i=1}^{n}\left(\sum_{j=1}^{m} A_{pj}\sum_{j=1}^{m} A_{cj}\sum_{j=1}^{m} A_{oj}\right) \quad (1)$$

where R = reference object resilience indicator; S_i = i-th security type resilience indicator; n = converged security types number; A_{pj} = j-th variable of asset physical security resilience; A_{cj} = j-th variable of asset cyber security resilience; A_{oj} = j-th variable of asset operational security resilience; m = assessed assets number.

The presented approach enables aggregation through individual assets, which is the basis for computing the final value of resilience indicator. The final value of reference object resilience indicator R is made up of the resilience indicator of all assets. For these purposes, the arithmetic mean of converged resilience expressed by the following computation method is used in Equation (2):

$$R = \sum_{j=1}^{m} A_j v_j \quad (2)$$

where R = reference object resilience indicator; A_j = j-th asset converged resilience indicator; v_j = j-th normalized weight of the j-th asset; m = assessed assets number.

The resulting resilience indicator of the assessed object R is expressed as an abstract value taking on a value in the interval from 0 to 100 points. For computation purposes, the initial resilience value is set at 100 points. It is based on the assumption that this value reflects an ideal state and thus the reference object protection system achieves and fulfils all the required measures and no penalizing factor is currently acting on it. The real state and value of the resilience indicator is in practice conditioned by the action of the penalty factor, which reduces the initial 100-point value. The lower limit and value of the resilience indicator was set at 0. This state then reflects the fact of the required measures absence or the state of penalizing factors action. Likewise, this situation is unlikely in practice, even considering the small probability of the simultaneous occurrence and action penalizing factors.

The value of the reference object assessed asset converged resilience I is expressed by the aforementioned aggregation, based on the selected security types resilience value, i.e., A_p, A_c, A_o. Considering the formulation of the previous conditions, even in this case the value of the indicator ranges from 0 to 100 points. Also, in this case, the computation is conditioned by the action of penalty factors and the reduction of the initial value. In

practice, penalization factors are divided into static and dynamic factors, i.e., factors that consider static penalization obtained for measures that the protection system should have but does not have at the given time, and dynamic penalization, which is obtained by the action of the intruder, non-compliance with regime measures or failure states of individual protection system components. The value based on the dynamic factors subsequently adjusts the value of the static penalty.

Subsequently, the indicator of converged asset resilience is computed, through the reference object selected assets resilience indicators arithmetic aggregation for selected security types (see Equation (3)).

$$A = \frac{A_p + A_c + A_o}{3} \tag{3}$$

where A = asset converged resilience indicator; A_p = asset physical security resilience indicator; A_c = asset cyber security resilience indicator; A_o = asset operational security resilience indicator.

Logic and visualization of the actual computation of the asset resilience indicator with respect to the selected security types A_p, A_c, A_o is expressed in Figure 1.

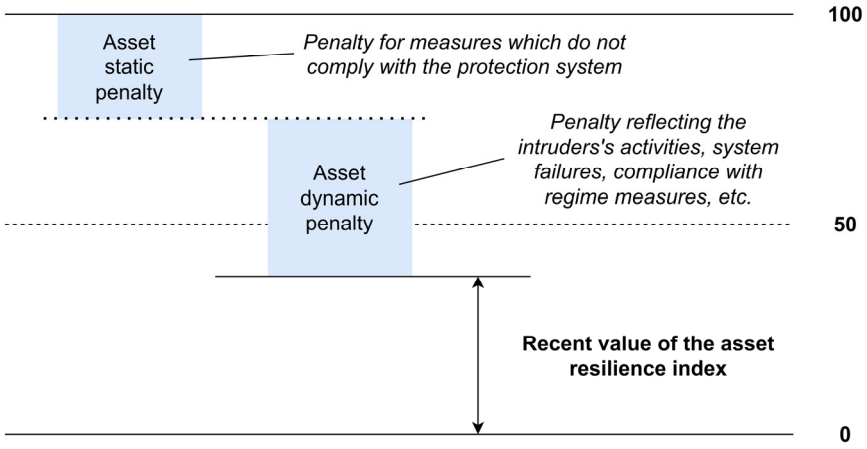

Figure 1. Asset resilience indicator computation for individual security types [19].

The mathematical model for asset resilience indicator computation will be presented in the introductory part of the article fourth chapter as a certain form of algorithmization of system and sensory data into Converged Security and Information Management System computing core.

2.3. PSIM/SIEM Category Systems Convergence as a Data Source for Resilience Assessment

The previous section explained the issue and importance of assessing the protected asset resilience and described a new resilience assessment approach using penalty factors. The aim of this section is to seamlessly follow up on the previous topic and to focus especially on the resilience level change issue based on information from technological means through dynamic penalty factors. For these purposes, it is most appropriate to use sophisticated additional smart security alarm systems, which are used in security monitoring centres for security management, and which can provide a lot of important information [48].

The world trend of recent years is the process of globalization, and it is no different in the field of security and security systems. This trend provides new approaches, possibilities, and above all the effort to integrate individual types of security. Currently, add-on systems of the Physical Security Information Management (PSIM) category are among the most advanced and sophisticated smart security alarm systems on the market. They are suitable for large-scale applications with a significant number of integrated physical, operational, and cyber security subsystems [49]. Add-on and very advanced analytical systems for

cyber security include systems of the Security Information and Event Management (SIEM) category. The mentioned systems integrate a few subsystems from which they receive data. They analyse, correlate, evaluate and transform these data into meaningful information that can be effectively used in resilience assessment [50].

In the previous part of the text, there was a logical division of penalty factors into static and dynamic factors. This division considered partial security and therefore physical, cyber and operational as well as converged security. Thanks to the static penalty factors and the subsequent application of the resilience assessment algorithm, the immediate value of the protected asset resilience can be determined. This value corresponds to the immediate security level and the asset's ability to withstand the specific risk manifestation. Data from technological means do not affect static penalty factors, and therefore it is not necessary to use technological means to determine resilience, apart from the program itself, which computed resilience. Static penalty factors are thus manifested during the introduction of means for assessing the protected asset resilience or in regular iterations, when new risks and newly created measures are evaluated. Therefore, if a resilience assessment system is deployed, for example, for a protected asset of a railway station, it is necessary to use the existing object risk analysis or to carry out a security audit so that individual penalties can be applied in relation to the risk. In this phase, as part of the resilience assessment, it is decided, for example, whether an evacuation plan is created for the railway station or whether one of the physical security technical protection systems protects it [51].

If a resilience assessment is to be effective and meaningful, resilience must be addressed over time, and if, for example, smoke is detected in a railway station and the electronic fire signalization system raises an alarm, there must be some reduction in resilience. In the event of the occurrence of this type of alarm, the relevance of this alarm must be assessed. The response to the event and overall resilience then depend on the relevance of the alarm. The relevance of an alarm can be confirmed based on the correlation of multiple events. For example, if a fire in a building is spreading, information comes from other fire detectors in the building, and it is therefore evident that it is not a false alarm. Or the relevance is verified by the operator based on the view from the camera or by the service in the location. For that reason, dynamic penalty factors have been introduced, which are linked to data from technological means and thus enable the resilience to be reduced according to how the situation develops over time. In the event of such a serious event as a fire, there is a cascading effect and a link to other security types—for example, the failure of operational technologies, information systems, disruption of mechanical prevention systems and other means to ensure the security/safety and operation of the organization. For that reason, additional related dynamic physical, cyber, and operational security penalty factors are applied that affect the overall converged security resilience [52].

In order for resilience to be reduced using dynamic penalty factors, information about which dynamic penalty factor is to be applied must be transferred to the software module for resilience assessment. For that reason, it is essential to find suitable means that will provide this information. Resilience assessment over time has two approaches:

- Continuous resilience reduction based on the resilience recomputation when applying individual dynamic penalty factors (for example, at each alarm from individual fire signalization);
- Leap resilience reduction based on an already assessed and categorized event with a certain severity, for example "High" or "Critical", possibly based on sub-events that are related to the occurrence of this event, for example "Outage of information passenger system", "Radio outage", etc.

In the case of continuous resilience reduction, a large amount of data is processed, which is not suitable to be left to the software for the resilience assessment. Superstructure security systems of a higher category, i.e., PSIM or SIEM, are intended for mass data processing, and their use is therefore very effective for processing and assessing data from subsystems and subsequent linking to dynamic penalty factors [53].

2.3.1. PSIM Systems

Systems of the PSIM category are add-on information security systems that enable the integration of a few diverse security systems and sensors, information systems and specialized business systems from different manufacturers under a unified operational view. Incoming data from various sources correlates with each other, determines their meaning and optimizes the response speed to emerging situations [54]. This can be a crisis, a security event (incident) or a solution to technological malfunctions and routine activities. Crises occur rarely. Security events can occur several times a week or even daily depending on the type of organization or industry in which the system is deployed. Solving technological malfunctions and routine activities is the order of the day. The goal of PSIM systems is to ensure the continuity of the activity of the given organization or segment in which they are applied.

When dealing with security incidents, timely information of all security forces and stakeholders plays a vital role. If information spreads quickly, dispatchers can reduce the time it takes to get an incident under control and reduce the time it takes to resolve it. Among the first questions when a security incident occurs is "What happened? Where did it happen? How should I react to that?".

And it is to these questions that PSIM systems answer. They correlate information from various security systems and sensors, including operational information, which they interpret in real time on clear map bases, display relevant cameras and thus provide a better overview of the current situation. They filter redundant information and thus create a comprehensive overview for an effective response. Individual malfunctions, security events or crises then have pre-prepared scenarios in the system that enable the system to react automatically, while operators are assigned specific tasks that help manage the given situation. Comprehensive situation management detailed reporting and retrospective analysis of security situations and routine activities is ensured. The Figure 2 shows the workplace of a security dispatcher who uses the PSIM system.

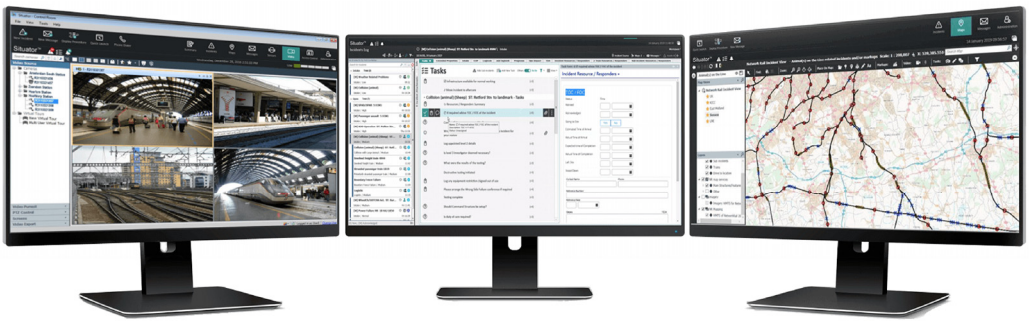

Figure 2. Workplace of the PSIM system security dispatcher [55].

The most important part of the PSIM category systems is the correlation core, which makes it possible to compare information from different integrated sources. A simple example can be a situation where it is necessary to respond to an event only at the moment when several sensors from different security systems report an alarm for a specific time period at the same time. Before this defined time elapses, the alarm system displays but does not attach importance to them in the form of a security event and does not burden the operator. A security event occurs only when the conditions are met. Systems in this category respond to the needs of organizations where lower category systems are not sufficient and a more robust solution is needed.

As can be seen in the Figure 3, data from embedded technologies comes into the correlation core, where it is assigned attributes such as time, location, data type (such as a sensor-triggered alarm), and priority. On the basis of data correlation (e.g., an alarm from a camera system and a simultaneous alarm from a fire system), pre-prepared workflows (scenarios) are triggered. Workflow, in the context of PSIM systems, is a set of automatic

interrelated activities in which PSIM uses pre-defined procedures. The operator whose task it is to solve the problem interprets meaningful information at the security workplace. Alternatively, it is possible for the system to assess the information independently, react using automatic operations, and not burden the operator. This results in an effective response to the given situation and the reaction time is significantly reduced. All system and operator steps are available for audit or investigation of unsatisfactorily resolved security events.

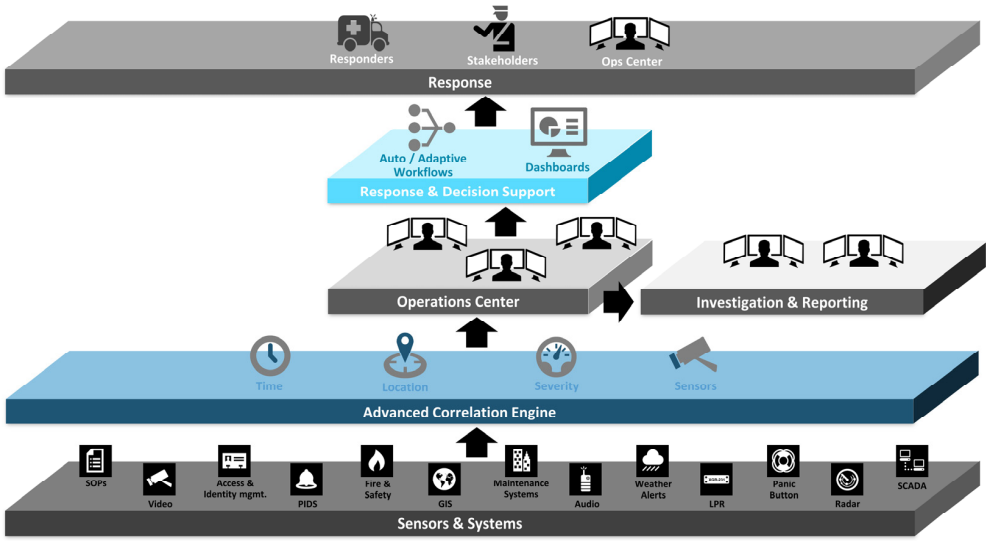

Figure 3. PSIM system structure [55].

The PSIM system assess security situations from a global perspective based on the data correlation obtained from diverse systems. It puts this data into context and starts automatic operations and workflows based on it. This is a diametrical difference compared to earlier approaches, when the system only interpreted the raw data from the subsystem to the operator without any context. It was then up to the operator to interpret the data for informational value.

The input contains disparate data, which are normalized and correlated in the next step. Using situational analysis, they are assigned to procedures that trigger appropriate user workflows (scenarios)—operators are shown relevant maps, cameras, work procedures and perform automatic operations using supporting decision-making systems. All these activities provide operators with a comprehensive situation overview, the so-called Common Operational Picture (COP) for the needs of incident resolution.

The aforementioned workflows represent the capital I of the PSIM system—"Information". All work manuals, procedures, guidelines and corporate regulations can be implemented into the system using clear workflows. In the event of an emergency, the operator can fully concentrate on solving partial tasks, as the system will offer clear work procedures. The system then enables overall archiving of the incident resolution process, both for evidentiary material and for the need for retrospective control and streamlining of processes and maintaining the continuity of the organization's activities. It ensures that information reaches the right people at the right time and that information is regularly updated. In this way, COP is obtained not only by all system clients (dispatch workplaces, field workers), but also by other interest groups (Integrated rescue system, police, superior components, service components, maintenance workers, companies, etc.) who are informed using data messages to their own information systems or obtain information by phone, email, SMS or through specialized early notification systems.

Without the use of the PSIM system, the security events prediction is almost zero or is solved at the tactical level, where measures are built in advance to minimize the exposure probability to the threat to the lowest possible level. Prediction in this case is a situation where the system is able to draw attention to any deviations from the normal state. For example, on the basis of information about the weather at approaching tropical

temperatures, it is possible to predict the occurrence of a fire, overheating of a certain technology, increased workload of employees, the probability of an accident, etc.

The system also draws on knowledge from the past. A number of events can be eliminated thanks to the system. If an incident occurs, chaos, misinformation can occur without the use of superstructure systems, and it takes some time before at least a certain consistent idea of the situation is formed. In contrast, the PSIM system will provide all available information, start the appropriate workflow and, thanks to this, make this process more efficient and significantly reduce its duration. It also provides sophisticated tools for managing and managing the situation. After closing a security event, it generates detailed reports, every step is recorded, and no additional resources need to be spent to investigate the event.

2.3.2. PSIM Systems and Data Sources for Smart Security Alarm Systems

Systems that provide data sources for smart security alarm systems and therefore can be integrated under PSIM can be categorized into security systems and sensors, localization system, graphic systems, information and database systems, control and operational systems, business systems and communication systems [53]. In order to effectively connect subsystems, the PSIM system must address and connect all supervised systems and devices into a unified platform, which is then processed by the system's control core. This integration method is usually provided with the help of appropriate software interfaces.

Security Systems

Basic security systems that can be integrated into PSIM systems include the following [56]:

- VSS with video analysis and specialized video analysis tools—means for monitoring events in real time using cameras including the ability to detect different events types;
- I&HAS—I&HAS control panels, evaluating various types of motion, shock, contact, linear light, radio types of intrusion detectors and other types of means to ensure comprehensive technical protection against unauthorized entry into objects and systems for triggering an intentional emergency alarm;
- ACS—systems for controlling access to objects, using various types of identification technologies, such as magnetic cards, Radio Frequency IDentification (RFID) chips and biometric data. Access control systems may be used even for location determination;
- EFS—electrical fire signalization control panels evaluating and controlling various types of fire detectors and devices;
- Perimeter systems—perimeter protection systems in the form of detection cables, infrared barriers, microwave barriers, etc. with specialized software for perimeter detection;
- Radar and sonar systems (as part of I&HAS)—systems for searching and determining the assets various types location (e.g., people and means of transport) with specialized software.

Location Systems

Localization systems are an important means for the PSIM system to be able to interpret the position of individual forces and resources (persons, vehicles, etc.) on map data. The localization systems that are commonly integrated into PSIM can be divided into [56]:

- Systems for external localization—systems based on GPS;
- Systems for localization inside the building—systems based on the technology of active RFID tags and suitably placed fixed or mobile RFID readers or radio localization systems.

Graphics Systems

All the outputs from the integrated subsystems are interpreted on map data in the form of a map visualization platform. The map visualization platform can be interpreted using [56]:

- Geographic Information Systems (GIS)—sophisticated systems that work with spatial data and which make it possible to locate all PSIM system entities (assets, sensors, available forces and resources) on map bases;

- Computer Aided Design (CAD)—project drawings of various types buildings;
- Vector/raster graphics—map materials in the vector or raster graphics form;
- 3D—some types of PSIM systems also work with 3D models for the graphic materials presentation.

Database Systems

The PSIM system enables integration with various types of corporate and specialized information and database systems according to the segment in which the PSIM system is implemented. The system makes it possible to draw data from these information and database systems, evaluate them and write them back. Bidirectional communication between PSIM systems and these types of subsystems is therefore ensured.

Control and Operating Systems

PSIM systems should not primarily interfere with control systems. Only in exceptional cases, when dealing with specific security events that immediately require this intervention. However, they can integrate data outputs from control systems and correlate that data with other outputs, evaluate them and create effective responses based on that. A typical example of control systems is Supervisory Control and Data Acquisition (SCADA)—specialized systems for supervision, control, and data collection with use, for example, in energy and other industries. Another segment is operational systems such as measurement and regulation, systems in buildings, elevators, etc. In operational systems, communication is usually two-way.

Enterprise Systems

Enterprise systems are specific systems with which PSIM systems can have integrated two-way communication. In this way, it is possible to contribute to ensuring the continuity of the activity of the given organization. An example can be integration with the corporate Service desk system, which primarily serves as a means of solving technical failures. If the PSIM system detects a specific technology technical failure, it automatically creates a dynamic form with information about the failure and sends it to the Service Desk system. The latter takes responsibility for solving the problem and, after solving it, informs the PSIM system about the solution of the matter. The PSIM system is therefore a means for solving the clearance of the malfunction, but the Service desk fulfilled the greater part of it. PSIM systems commonly integrate business systems such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), help desk/service desk, etc.

Communication Systems

Communication systems represent an important element for PSIM systems, as timely information of interest groups plays an important role. PSIM systems can be connected to various communication systems, such as [53]:

- early notification systems—ensure mass notification of people by calls means or SMS, providing functionalities such as Text to Speech or Speech to Text, etc.;
- radio stations—they enable the playback of predefined announcements to certain system branches and ensure a certain degree of automation in the distribution of information in the locality;
- SMS gateways—systems for sending SMS;
- IP telephones and dispatch terminals—these devices enable the control workplace to initiate telephone calls directly from the PSIM system workplace and create complex conferences, ensure communication with radio resources, etc.

It makes sense to integrate all the above subsystems from the effective security management point of view in the organization if the organization is equipped with them. Each subsystem provides a series of data that the PSIM system logically processes and uses. Not all data are suitable for resilience assessment. Therefore, in the last subsection of this article,

the options of selected subsystems and examples of important information for the resilience assessment are presented.

2.3.3. SIEM Systems

One of the subsystems of PSIM can be SIEM category systems, the issues of which are presented in this subsection. With this integration, PSIM systems can be upgraded to systems for converged security, the so-called Converged Security and Information Management System (CSIM). This is a new, modern approach to security management, where emphasis is placed on the interconnectedness of individual security types, mainly physical, operational, and cyber. From the resilience assessment point of view and the link to dynamic penalty factors, it is possible to use these systems independently, but it depends on each organization concept.

SIEM systems are superstructure security systems in the cyber security field. It is therefore not a clearly defined protection functionality, such as an antivirus or firewall, but a system that detects intrusions, warns of possible problems and collects information that gives ICT administrators a comprehensive overview about the current situation. In real time, these systems can analyse both the logs themselves and data from various applications, e.g., Intrusion Prevention Systems (IPS) or Intrusion Detection Systems (IDS), as well as from firewalls or switches. A comprehensive overview makes it possible to put individual events in a logical context and create models of relevant correlations. Today's networks tend to be quite heterogeneous, and although individual elements (from different manufacturers) generate reports about their operation, these reports are usually available in different formats and need to be unified. The unified overview provided by these systems significantly simplifies the following evaluation and other follow-up actions, e.g., early warning, security audit [57].

The main objectives of SIEM systems include:

- more flexible and faster response to any anomalies and threats in the ICT infrastructure;
- more successful detection of these anomalies and attacks;
- streamlining of ICT infrastructure management.

Systems in the SIEM category are relatively new technologies. The security information management and events in the ICT structure arose as a natural response to the ever-increasing risk of threats within the cyber environment.

The mentioned SIEM technology originally arose from two already established and well-known technologies:

- Security Information Management (SIM)—technology dealing with the long-term storage of events, their analysis and reporting of problems;
- Security Event Management (SEM)—technology dealing with infrastructure monitoring, event correlations and creating alarms in real time.

The merger of the two technologies was mainly due to the increasing costs of each of them and the demands on the complexity of the solution.

Therefore, SIEM systems provide the possibility of monitoring, storing, and managing security events represented by log records that are collected from defined devices located in the ICT infrastructure of the organization. Using analytical functions, SIEM can identify security threats that can become the basis for security incidents. The graphical interface of SIEM makes it possible to centrally assess events from many heterogeneous sources, among which we can include operating, database, application and network systems and devices. SIEM products also include archiving modules that can be used to store collected logs for forensic analysis purposes. In Figure 4 shows an example of logs from individual ICT systems, which the SIEM system analyses, assess, and categorizes based on its own algorithms.

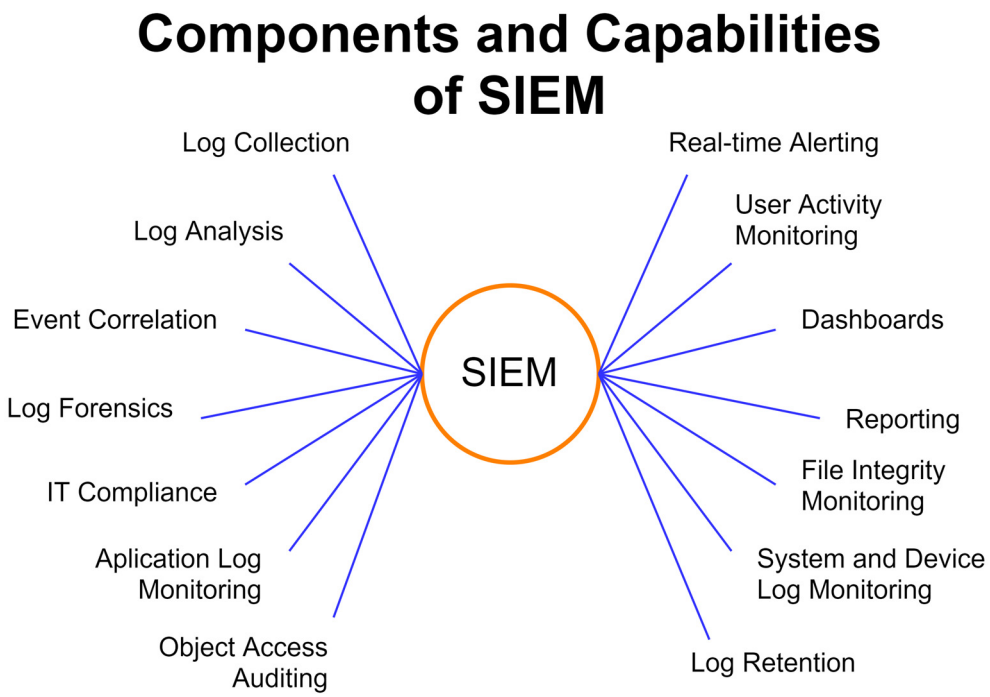

Figure 4. SIEM system structure [58].

With the help of SIEM systems, organizations can also make conceptual decisions about the further development of their infrastructure, deployment of new tools, applications, etc. Information from SIEM systems therefore represents an important basis for the organization's management when deciding on future investments.

3. Results

The development of the Converged Security and Information Management System as a complex system is conditioned by the establishment of a mathematical and logical framework. The mathematical framework to a certain extent algorithmizes the different steps of asset resilience indicator computation and thus enables the correlation and implementation of system and sensory data. The logical framework subsequently creates a way of processing, presenting and visualizing data for a specific user and thus gives the overall logic of the functioning of the system as such.

However, before describing this system, it is still appropriate to briefly describe the profile of the smart city for which this system is designed. The system can be used for small and medium-sized cities of regional character up to 400 thousand. resident. The system is primarily designed for assessing the resilience of technical infrastructures, i.e., energy, digital infrastructure, transport, drinking water, and waste water. However, it can also be used for assessing the resilience of some socio-economic infrastructures, e.g., health and emergency services. From the point of view of complexity, the system is able to assess the resilience of even complex infrastructure elements of European importance, e.g., transmission system electrical station 400/220 kV.

3.1. Mathematical Framework for Converged Security and Information Management System Development

As it was stated at the end of the second chapter, the pragmatic connection of the scientific and technological solution based on Figure 1, is the technical implementation of the systems and sensory data algorithmization represented by Equation (4), which creates a mathematical model for asset resilience indicator computation.

$$A_{p,c,o} = \left(100 - A_{sp} \cdot 100\right) \cdot \left(1 - A_{dp}\right) \quad (4)$$

where $A_{p,c,o}$ = given security type asset resilience indicator (i.e., physical, cyber or operational); A_{sp} = variable of asset static penalty; A_{dp} = variable of asset dynamic penalty indicator.

The calculation of the resilience index itself is carried out using penalty factors in such a way that the decrease in resilience caused by the penalty factors is subtracted from the initial value. The static part reflects the obtained penalty for measures that the protection system should have and does not have at a given time. The dynamic part of the formula then reflects the penalty obtained by the activity of the violator, malfunctions, non-compliance with regime measures and dynamically corrects the value of the static penalty.

The method of computing the variable of asset static penalty is indicated by the Equation (5):

$$A_{sp} = \frac{\sum P_{sa}}{\sum P_s} \tag{5}$$

where A_{sp} = variable of asset static penalty; P_{sa} = value of active static penalty factor variable in a given security type; P_s = maximum value of static penalty factor variable in a given security type.

The sum of all the required static penalty factors specified in the phase of the initial security audit of the object determines the maximum level of the default resilience of the object, which is valid for the entire monitoring period of the object, during which there were no changes to its default security measures.

The method of computing the variable of asset dynamic penalty value is indicated by the Equation (6):

$$A_{dp} = \frac{\sum P_{da}}{\sum P_d} \tag{6}$$

where A_{dp} = variable of asset dynamic penalty; P_{da} = value of active dynamic penalty factor variable in a given security type; P_d = maximum value of dynamic penalty factor in a given security type.

The occurrence of each expected dynamic penalty factor means a reduction in the immediate monitored object resilience by the value defined by this dynamic penalty factor for the period during which the dynamic penalty factor occurs. After the occurrence of an active dynamic penalty factor, the object resilience increases by the value defined by this dynamic penalty factor.

In order to understand the logic of the mathematical framework, the text is supplemented with general principles for creating a catalog of assets, risks and penalty factors. From the point of view of the overall clarity of the results, it is advisable to choose only a minimal set of the most important assets that fundamentally affect the security behavior of the assessed reference object, because the determination of security risks and reference object resilience will always be carried out separately for each asset. The resulting resilience of the entire reference object is obtained as a weighted average of the resiliencies related to individual assets.

In the common literature, the list of general threats is usually divided into several typical categories. Each specified asset in the monitored object can be affected by a different subset of threats with a different probability, i.e., different a subset of risks. The set of identified risks must be continuously modified over time, most often due to the appearance of new technologies, which can be affected by either other types of risks or original risks with a changed impact.

As already mentioned, for the creation of risk catalogs, which serve to determine the resilience of objects, the penalization method was used, which can be defined as a procedure for evaluating the resistance of objects from the point of view of converged security. The penalization method is therefore a tool for monitoring the status of measures and thus the degree of assets protection. Penalization from the point of view of assessing the objects resilience has the following characteristics:

- penalization refers to individual factors (external and internal factors),
- the penalty represents a number whose size reflects the degree of severity of the factor's influence (the level of positive or negative effect) on the reference object and its assets,
- the penalty is determined separately for individual types of security,
- the penalty can be applied both to individual assets and centrally to the entire reference object.

From the point of view of penalty, we distinguish between two factors—static penalty factor and dynamic penalty factor:

- static penalty factor specifies such influences (measures) that have a long-term effect on the protection system and will not be removed or appear by themselves. The invalidity of the relevant static penalty factor is mostly due to the non-existence of processes necessary to manage security, non-existence of physical security elements, non-compliance with valid legislation, unimplemented checks, revisions, etc.
- dynamic penalty factor represents factors (risks) that themselves change over time, and the duration of their action cannot be accurately estimated. This includes the detection of events and incidents in which it is necessary to determine the monitored time effect of the factor that contributes to the reduction of the object resilience. After the duration of its action, the relevant dynamic penalty factor is deactivated, and the object resilience will increase again.

An overview of possible static penalty factors and dynamic penalty factors is processed in the general catalog of penalty factors, which presents an overview of the main potential external and internal factors (factors) that affect the resistance of a group of objects or industries for which the general catalog was created. An example of static penalty factors for the physical security is presented in the Table 1.

Table 1. An example of static penalty factors for the physical security.

Characteristics of the Factor	Default Penalty		
	PS	**CS**	**OS**
There is a detection function in front of the perimeter	50	10	10
The area in front of the perimeter can be monitored	40	10	10
The perimeter can be monitored	60	10	10
The external controlled space can be monitored	60	10	10
The building envelope can be monitored	80	20	10
The internal controlled space can be monitored	80	20	10

Legend: PS—physical security, CS—cyber security, OS—operational security.

For a better understanding of the indicator of converged asset resilience calculation process, the calculations of the individual steps of the mathematical framework are presented in the following text.

The method of computing the variable of asset static penalty value is indicated by the Equation (5). The results of computing are presented in Table 2.

Table 2. The results of computing the variable of asset static penalty.

Characteristics of the Factor	Default Penalty		
	PS	**CS**	**OS**
$\sum P_{sa}$	140	120	130
$\sum P_s$	850	715	655
A_{sp}	0.165	0.168	0.198

Legend: PS—physical security, CS—cyber security, OS—operational security.

The method of computing the variable of asset dynamic penalty value is indicated by the Equation (6). The results of computing are presented in Table 3.

Table 3. The results of computing the variable of asset dynamic penalty.

Characteristics of the Factor	Default Penalty		
	PS	**CS**	**OS**
$\sum P_{da}$	90	20	10
$\sum P_d$	2308	3050	2737
A_{dp}	0.038	0.006	0.003

Legend: PS—physical security, CS—cyber security, OS—operational security.

Mathematical model for asset resilience indicator computation by Equation (4). The results of computing are presented in Table 4.

Table 4. The results of computing the security type asset resilience indicators.

A_p	A_c	A_o
80.3	85.1	86.2

Legend: A_p—asset physical security resilience indicator, A_c—asset cyber security resilience indicator, A_o—asset operational security resilience indicator.

Subsequently, the indicator of converged asset resilience is computed, through the reference object selected assets resilience indicators arithmetic aggregation for selected security types (see Equation (3)). Reference object asset converged resilience indicator A reached a value of 83.9. In this regard, it is possible to think about the fact that the owner of such an object, based on the determined levels of resilience, can subsequently establish a qualitative assessment of the level of resilience and thus subsequently state that the resilience is high or low or critical.

The presented example computes the converged resilience indicator for one selected asset. If the converged resilience indicator of the entire reference object should be computed, it is necessary to determine the importance and therefore the weight of the individual assets and then use Equation (2). If the user would like to express the level of the reference object resilience indicator through the resulting resilience indicator for a different type of security (physical, cyber operational), he will use Equation (1).

This approach creates a more detailed view of individual types of security and the need to supplement measures in the type of security, which achieves the lowest level of resilience. The presented system allows both methods of computation to make situational management more efficient.

3.2. Logical Framework for Converged Security and Information Management System Development

The functional architecture and capabilities of SIEM systems indicate that these are systems designed to process a huge data volume on all possible activities taking place in the organization's ICT infrastructure. This can be, for example, the monitoring and recording of user access to individual systems, network traffic or external attacks on operating systems, etc. The main result that these systems then provide to their users is clear information about functional operation and all anomalies that have the potential to harm the organization through cyberspace. In addition, the elements from which these systems draw data have a very close connection with other elements of converged security, whether it is physical, information or operational security. An example could be the use of unauthorized infected media by an employee with administrative access to a terminal computer station that is part of the company-wide network. At the same time, this employee is registered in the given organization entry control system, his movement may be monitored using a camera system, there may be biometric or other personal data about him, and last but not least, he directly or indirectly participates in determining the availability of services provided by the organization. By properly setting up the correlation of all available data and information, the PSIM category superstructure systems enable the necessary response

to threats, including those originating in cyberspace, to be initiated. From this point of view, SIEM systems represent one of the important inputs for superstructure PSIM systems, which covers the already mentioned cyber security. Therefore, some global manufacturers of PSIM systems are already working with the concept of converged security which they call the Converged Security and Information Management System (CSIM).

3.3. Function Blocks of CSIM

From the conceptual architecture point of view, the CSIM is divided into individual so-called functional blocks, which characterize the functionality of the entire module. Figure 5 describes these blocks in a comprehensive manner, which are then characterized in detail in subsequent subsections.

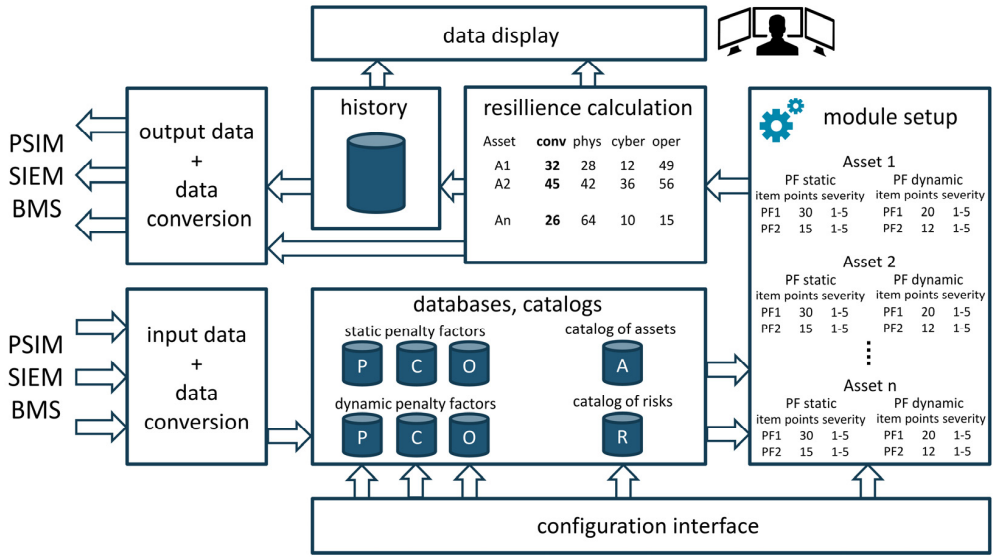

Figure 5. Functional architecture of CSIM system.

In principle, the entire CSIM module enables work in two basic modes, i.e., offline and online. In the first mode of operation, the CSIM is designed to determine or compute the so-called static resilience level of the selected SCI reference object, or assets. Static resilience refers to the general ability of the SCI reference object to withstand relevant potential security threats and the risks arising from them. In this case, the possibility of an ad hoc disruption of the asset in real time based on the security incident occurrence (or extraordinary event) that significantly affects this capability is not considered. This computation reflects the normal idle state of the asset, i.e., the SCI reference object and its initial properties, especially from the point of view of the protection system. In contrast, the second mentioned mode is intended precisely for the possibility of correcting the resilience static level as a result of the actual security incident (or emergency event) occurrence at a given moment. In such a case, the resulting real resilience level will be different from the static resilience level, as it will be lowered by the negative effects (forces) of a disruptive security incident acting on the SCI reference object and its protection system or asset.

3.3.1. Block: Databases and Catalogues

Databases and catalogues represent one of the CSIM model basic blocks. Within this block, the reference object selected data is accumulated into three group entities, i.e., Catalogue of assets, Catalogue of risks, and Catalogue of penalty factors.

Catalogue of Smart City Infrastructure Assets

This catalogue contains a list of the individual protected interests and values (so-called SCI assets) of the organization or reference object for which a resilience level is being considered. An asset is therefore understood to be anything that has a value for the SCI

reference object that can be diminished by the threat occurrence. The reference object itself can be an asset. Most often, the determination of assets is based on a generally perceived market price or a subjective importance (criticality) assessment for a given SCI reference object, or a combination of both mentioned approaches. This catalogue can be internally structured according to a number of aspects, e.g., according to the nature and species affinity of the asset, according to procedural significance within the SCI reference object.

Catalogue of Risks

In general, this catalogue presents an overview of all threats and the resulting risks for the defined assets of the SCI reference object, see Asset Catalogue. From the preserving the relational affiliation point of view of the asset and the risk, it is appropriate that each risk contains an attribute determining this relationship. This means that each risk should clearly define for which asset it is relevant and which it has the potential to disrupt. It should be considered that one and the same risk can be linked to several assets or one risk can potentially threaten several assets. Risk analysis and mapping must be done in both internal and external SCI environments [59]. In this case, the external environment is the territory in which the SCI is located.

Catalogue of Penalty Factors

The catalogue of penalty factors is a list of all possible factors that influence the asset (or SCI reference object) resilience level and its protection system. Depending on their nature and purpose, individual penalty factors are linked to risks, see Catalogue of risks, to a specific asset, see Catalogue of assets. These factors are divided from the following several points of view:

- The point of view of the application of individual factors when determining the initial or static resilience (off-line mode) it is in question on the use of so-called static penalty factors, and when determining the real resilience (online mode), the so-called dynamic penalty factors are also used;
- Aspect of security jurisdiction which includes physical security category penalty factors, cyber security category penalty factors, and operational safety category penalty factors.

The inputs to the Database and catalogues block are Input data and data conversion block (obtaining data from superstructure systems of the SCI reference object to compute the real resilience level based on additional penalty factors) and Configuration interface block (obtaining basic necessary data from the environment of the SCI reference object). This is mainly a list of assets and relevant risks that have the potential to endanger or disrupt them, and an overview of basic penalty factors and importance weights.

The output from the Database and catalogues block is Module Setup block. That is necessary grouping or setting the relevant parameters for the subsequent resilience computation to the selected asset(s) of the SCI reference object.

3.3.2. Block: Module Setup

The module setup is also one of the basic functional blocks of the CSIM module. In this block, the necessary parameters are selected procedurally for the subsequent resilience level computation to the selected asset, or to the SCI reference object asset group.

When determining the static resilience (off-line mode), the relevant asset is selected from the asset catalogue. For this asset, relevant risks that have the potential to disrupt it are assigned from the Risk Catalogue. Given the fact that static penalty factors are tied in this case to uniform risks, these factors are automatically assigned to the selected asset. Individual factors carry with them a set point value, which is the starting point for the subsequent resilience computation.

Importance weights are also assigned to the individual penalty factors, i.e., weights determining the importance of the penalty factor in relation to the selected asset (e.g., in the range of values 1–5, with the value 5 being the most important for the asset and the value

1, on the contrary, the lowest importance for the asset). Ultimately, it will be considered optimal when the individual scales are set by the user (CI security liaison officer) in direct cooperation with the end user, through the Configuration Interface block.

When determining the real resilience level (online mode), the procedure for determining the static resilience is based on the above-mentioned technique, but with the fact that so-called dynamic penalty factors also enter the whole process. This type of factor is represented, for example, by information about security incidents (or extraordinary events) from reference object automated systems and sensors that affect the resilience of the asset. The weight of importance is also assigned to these factors, similarly as in the previous case.

The inputs to the Module Setup block are Database and catalogues block (obtaining the necessary data of the assets type, risks, or relevant penalty factors of the reference object) and Configuration interface block (obtaining the necessary data such as the weight of the penalty factors importance in relation to the assessed asset). Furthermore, the incoming input data correlation is set within the configuration interface from integrated subsystems and a specific asset to determine the list of additional penalty factors for the given asset.

The output from the Module Setup block is Resilience computation block. Here the actual process of computing the Resilience of the SCI reference object selected asset(s) takes place.

3.3.3. Block: Resilience Computation

This functional block represents the core of the computation and therefore the determination of both the static and real resilience value of the SCI reference object asset(s). This involves substituting the individual parameters of the given asset. The result is the acquisition of the resilience indicator value of the SCI reference object or resilience in relation to individual security types (physical, cyber, and operational). The input to the Resilience Computation block is Module Setup block. Determination of structured data necessary to computing the resilience of the SCI reference object selected assets.

The outputs from the Resilience Computation block are Data display block (here the results obtained by applying the CSIM module are interpreted in the event that the reference object does not have a superstructure system, which would primarily be intended to display the acquired data). History block (common storage of all acquired SCI reference object resilience values, not only the real ones, but also the historical ones, since the deployment of the CSIM module in the given environment of the SCI reference object), and Output data and data conversion block (a unified communication format for transferring data obtained from the CSIM module to superstructure systems implemented in the environment of the SCI reference object for the resulting presentation of this data and its further use).

3.3.4. Block: Configuration Interface

The Configuration interface block represents the gateway (environment) for importing or manually entering the necessary data such as assets, risks, penalty factors and weights, including their necessary attributes (e.g., point valuation, determination of relational dependence).

The outputs from the Configuration Interface block are Database and catalogues block (here the necessary data of the SCI reference object asset type, risk, or relevant penalty factors), and Module Setup block (necessary data such as the penalty factors importance weight in relation to the assessed asset(s) is stored here).

3.3.5. Block: Data Display

This block is intended for the final interpretation of the obtained results in the form of determining the SCI reference object (asset)resilience. If the CSIM module is deployed in the environment of a reference object that has a superstructure system (e.g., the PSIM system), the resulting interpretation will be implemented directly in the superstructure system. This block is primarily intended for implementations without the possibility of

using superstructure systems in order to ensure a clear and unambiguous presentation of the achieved values, not only the current ones, but also the historical ones.

The inputs to the Data Display block are Resilience computation block (this is a data source of computed current SCI reference object/asset resilience values), and History block (this is the source of all data, i.e., historical SCI reference object/asset resilience values).

3.3.6. Block: History

The History block represents a common repository of acquired resilience values. All data computed by the CSIM module are recorded here. This is not only the current real-time resilience data for SCI reference object individual assets, but also all historical data obtained from the module deployment at the reference object to the current state. In some cases, add-on systems can replace the functionality of this functional block.

The input to the History block is Resilience computation block, i.e., a data source of the computed SCI reference object (asset) resilience value.

The outputs from the History block are Data Display block (here the results obtained by applying the CSIM module are interpreted in the event that the SCI reference object does not have a superstructure system, which would primarily be intended to display the acquired data) and Output data and data conversion block (a unified communication format for transferring data obtained from the CSIM module to superstructure systems implemented in the environment of the SCI reference object for the resulting presentation of this data and its further use).

3.3.7. Block: Input Data and Data Conversion

Data Input and Data Conversion is a function block that is designed to provide collection and providing aggregated data needed for resilience assessment from systems implemented in the environment of the SCI reference object (e.g., in PSIM systems, SIEM) to the CSIM module. The synchronization of this data into a uniform communication format is an integral part of this block.

The inputs to the Input Data and Data Conversion block are outputs from systems implemented and used in the environment of the SCI reference object, e.g., already evaluated data in the form of a specific event from a superstructure system of the PSIM or SIEM category, or an evaluated alarm from a BMS.

The output from the Input Data and Data Conversion block is Databases and catalogues block (filling defined catalogues and databases with the necessary data from the environment of the reference object, including their possible correction).

3.3.8. Block: Output Data and Data Conversion

Output Data and Data Conversion is a functional block that ensures the structured transfer of the resulting SCI reference object the asset(s)resilience values back to the system, implemented in the environment of the SCI reference object (e.g., in PSIM systems, SIEM) for necessary interpretation and further use. An integral part of that block is the synchronization of these data into a uniform communication format.

The inputs to the Output Data and Data Conversion block are Resilience computation block (this is a data source of computed current resilience values of the SCI reference object/asset) and History block (this is the source of all data, i.e., SCI historical reference object/asset resilience values).

The outputs from the Output Data and Data Conversion block are systems implemented and used in the environment of the SCI reference object, e.g., superstructure systems of the category PSIM, SIEM.

The CSIM aims to determine the resilience value of selected assets and then monitor it in real time. To compute the resilience value, it uses input static and dynamic information and catalogues of penalty factors, which are created according to the assets types on which the CSIM is used. CSIM module draws source data for its real-time operation from associated superstructure security systems of more complex types or directly from

partial security systems. The above decomposition of the CSIM into individual functional blocks describes the actual functionality of this module, including a schematic way of mutual positioning and individual blocks linking. The user of the CSIM tool can be any organization that needs to assess the security status of its infrastructure, predict possible threats, and create appropriate measures to limit the consequences.

4. Discussion

The primary goal of the article was to pay attention to converged security from a more complex security perspective. For this purpose, the authors created the Converged Security and Information Management System (CSIM). This system enables an interconnected assessment of individual types of security, primarily physical, operational, and cyber. In this context, it is necessary to state that the correlation of physical, cyber, and operational security in the case of using CSIM brings a very powerful tool for predicting security events and for managing security as such [20]. Previous research in this area has been oriented mainly to the field of cyber security [21]. However, this is currently no longer sufficient, as the security and protection of smart city infrastructures requires a comprehensive approach [26].

The secondary goal of the article was to present the suitability of using CSIM to assess the resilience of smart city infrastructures (SCI). From a resilience assessment perspective, CSIM represents a comprehensive tool that can provide information for the resilience assessment module and in turn respond to the computed resilience value [18]. Previous research in this area has been oriented towards the development of methods and tools for assessing static and dynamic resilience, but only in the context of one group of threats [47].

Based on the above, it can be concluded that the use of CSIM to assess the resilience of SCI brings several significant benefits. Through this system, it is possible to implement an interconnected assessment of individual types of security against different groups of threats. Furthermore, it is obvious that it is not appropriate to use all the information from the connected subsystems of the PSIM or SIEM systems for recomputing the overall resilience of the SCI reference object and the protected asset. For this reason, dynamic penalty factors catalogues were created, in which there is a list of suitable information that should influence the resilience assessment.

On the other hand, it is necessary to draw attention to some shortcomings of the CSIM system. Specifically, his focus on technical and some socio-economic systems. In the same way, the convergence of only physical, cyber, and operational security or the assessment of resilience tied to one specific threat or the scenario of its development over time can become a disadvantage. These shortcomings could be improved, for example, through the convergence of other types of security and/or the creation of a common catalogue of static and dynamic penalty factors for a group of threats.

5. Conclusions

The aim of the presented article is the presentation of the Converged Security and Information Management System (CSIM) using the smart security alarm systems converged security. concept The essence of this system is the creation of an information interface for online monitoring of the status and behaviour of elements of physical, operational, and cyber security, the use of mutual links between elements and, based on this, the assessment of the given reference object resilience (and its assets). This should enable the prediction of a possible potential threat. The source data will be drawn from superstructure security systems (i.e., PSIM, SIEM) and application of the created mathematical and logical models (CRA). The user of such tool will be any organization that needs to assess its security status, predict possible threats and create (activate) appropriate measures. The primary goal of resilience assessment is converged security, but it is not excluded to use the software for the assessment of physical, operational and cyber security separately.

The use of the CSIM system in building smart cities significantly helps to strengthen the resilience of such infrastructures, which are absolutely necessary for the concept of

smart cities, i.e., primarily energy and ICT. The high level of resilience of these infrastructures enables the creation of a reliably functioning smart city that can fully focus on the development of other technologies. Another advantage of this system is the continuous supervision of individual SCIs and the possibility of reassessing resilience after the implementation of security measures. At the same time, however, it is necessary to draw attention to the fact that the CSIM system is based on the mathematical model of the Converged Resilience Assessment method and the PSIM and SIEM systems. For this reason, working with the CSIM system requires knowledge of these input methods and systems.

Currently, the CSIM system is materialized in the form of a functional sample, which has already been successfully tested in practice on selected infrastructures of two regional cities, i.e., Ostrava (290 thousand inhabitants) and Zlín (75 thousand inhabitants). The results of the testing confirmed the ability of the system to assess the physical, operational, and cyber security of selected smart city infrastructures. The result of this assessment was the determination of the level of resilience for individual infrastructures and the identification of the most vulnerable of them. Based on the findings, it is recommended that further research focus especially on the possibilities of integrating other types of security into the assessment process. For this reason, the functional sample will be modified and deployed on other specific infrastructure systems, also in changing security environment and threats view However, the presentation of any more detailed outputs and results would be contrary to the protection of sensitive data of selected SCI operators.

Author Contributions: Conceptualization, M.H., D.R., B.S. and M.B.; methodology, M.H. and M.B.; software, M.B.; validation, D.R. and B.S.; formal analysis, M.H. and D.R.; investigation, B.S. and M.B.; resources, M.H. and D.R.; data curation, B.S. and M.B.; writing—original draft preparation, M.H., D.R., B.S. and M.B.; writing—review and editing, M.H., D.R., B.S. and M.B.; visualization, D.R.; supervision, M.H.; project administration, D.R.; funding acquisition, M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Ministry of the Interior of the Czech Republic, grant number VK01030014.

Data Availability Statement: Data are unavailable due to privacy or ethical restrictions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ristvej, J.; Lacinak, M.; Ondrejka, R. On Smart City and Safe City Concepts. *Mob. Netw. Appl.* **2020**, *25*, 836–845. [CrossRef]
2. Lacson, J.J.; Lidasan, H.S.; Spay Putri Ayuningtyas, V.; Feliscuzo, L.; Malongo, J.H.; Lactuan, N.J.; Bokingkito, P., Jr.; Velasco, L.C. Smart City Assessment in Developing Economies: A Scoping Review. *Smart Cities* **2023**, *6*, 1744–1764. [CrossRef]
3. Prochazkova, D.; Prochazka, J. Smart Cities and Critical Infrastructure. In Proceedings of the Smart City Symposium Prague, Prague, Czech Republic, 24–25 May 2018; Ruzicka, J., Ed.; IEEE: New York, NY, USA, 2018; pp. 1–6. [CrossRef]
4. Rehak, D.; Senovsky, P.; Slivkova, S. Resilience of Critical Infrastructure Elements and its Main Factors. *Systems* **2018**, *6*, 21. [CrossRef]
5. Lukas, L.; Urbancokova, H. Types of Security and their Convergence. In *Converged Security*; Lukas, L., Ed.; VerBuM: Zlin, Czech Republic, 2019; pp. 26–42.
6. Hettne, B. Development and Security: Origins and Future. *Secur. Dialogue* **2010**, *41*, 31–52. [CrossRef]
7. Plachkinova, M.; Maurer, C. Security breach at target. *J. Inf. Syst. Educ.* **2018**, *29*, 11–20.
8. Santos-Reyes, J.; Padilla-Pérez, D.; Beard, A.N. Modeling Critical Infrastructure Interdependency: The Case of the Mexico City Metro Transport System. *Hum. Ecol. Risk Assess. Int. J.* **2015**, *21*, 1428–1444. [CrossRef]
9. Pescaroli, G.; Alexander, D. Critical Infrastructure, Panarchies and the Vulnerability Paths of Cascading Disasters. *Nat. Hazards* **2016**, *82*, 175–192. [CrossRef]
10. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control. Syst. Mag.* **2001**, *21*, 11–25. [CrossRef]
11. National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations*; U.S. Department of Homeland Security: Washington, DC, USA, 2009.
12. Elvas, L.B.; Mataloto, B.M.; Martins, A.L.; Ferreira, J.C. Disaster Management in Smart Cities. *Smart Cities* **2021**, *4*, 819–839. [CrossRef]
13. Tzioutziou, A.; Xenidis, Y. A Study on the Integration of Resilience and Smart City Concepts in Urban Systems. *Infrastructures* **2021**, *6*, 24. [CrossRef]

14. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. A Survey of Approaches Combining Safety and Security for Industrial Control Systems. *Reliab. Eng. Syst. Saf.* **2015**, *139*, 156–178. [CrossRef]
15. Eames, D.P.; Moffett, J. The Integration of Safety and Security Requirements. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Toulouse, France, 27–29 September 1999.
16. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T.; Novotny, P. Cascading Impact Assessment in a Critical Infrastructure System. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 125–138. [CrossRef]
17. Rehak, D.; Hromada, M.; Onderkova, V.; Walker, N.; Fuggini, C. Dynamic Robustness Modelling of Electricity Critical Infrastructure Elements as a Part of Energy Security. *Int. J. Electr. Power Energy Syst.* **2022**, *136*, 107700. [CrossRef]
18. Matola, K.E. The Convergence of Physical and Cybersecurity: The Path Forward for Secure and Resilient Infrastructure. In *Homeland Security and Critical Infrastructure Protection*; Baggett, R.K., Simpkins, B.K., Eds.; Praeger: Santa Barbara, CA, USA, 2018; pp. 347–364.
19. Hromada, M.; Rehak, D.; Lukas, L. Resilience Assessment in Electricity Critical Infrastructure from the Point of View of Converged Security. *Energies* **2021**, *14*, 1624. [CrossRef]
20. Anderson, K. Convergence: A Holistic Approach to Risk Management. *Netw. Secur.* **2007**, *5*, 4–7. [CrossRef]
21. Spears, J.L.; Barki, H. User Participation in Information Systems Security Risk Management. *MIS Q.* **2010**, *34*, 503–522. [CrossRef]
22. Aleem, A.; Wakefield, A.; Button, M. Addressing the Weakest Link: Implementing Converged Security. *Secur. J.* **2013**, *26*, 236–248. [CrossRef]
23. Christensen, J.F. Industrial Evolution Through Complementary Convergence: The Case of IT Security. *Ind. Corp. Chang.* **2011**, *20*, 57–89. [CrossRef]
24. Chang, H.; Kim, J.; Park, J. IT Convergence Security. *J. Intell. Manuf.* **2014**, *25*, 213–215. [CrossRef]
25. Schneller, L.; Porter, C.N.; Wakefield, A. Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators. *Secur. J.* **2023**, *36*, 333–349. [CrossRef]
26. Contos, B.T.; Crowell, W.P.; DeRodeff, C.; Dunkel, D.; Cole, E.; McKenna, R. *Physical and Logical Security Convergence: Powered by Enterprise Security Management*; Syngress: Oxford, UK, 2011. [CrossRef]
27. Anand, S. Convergence of Cyber and Physical Security—A must for Smart Grid Systems. *PalArch's J. Archaeol. Egypt Egyptol.* **2020**, *17*, 8055–8060.
28. Park, S.; Ko, D. Design of the Convergence Security Platform for Smart Universities. *J. Platf. Technol.* **2015**, *3*, 3–7.
29. Kang, J.; Lee, J.; Hwang, C.; Chang, H. The Study on a Convergence Security Service for Manufacturing Industries. *Telecommun. Syst.* **2013**, *52*, 1389–1397. [CrossRef]
30. Silva, R.B.E.; Piqueira, J.R.C.; Marques, R.P.; Marques, A.L.F. Physical, Corporate and Industrial Digital Security Convergence: Gaps to Close. In Proceedings of the International Conference on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, Austria, 13–17 November 2017.
31. Zahran, B.; Hussaini, A.; Ali-Gombe, A. Security of IT/OT Convergence: Design and Implementation Challenges. In Proceedings of the 2021 World Congress in Computer Science, Computer Engineering, & Applied Computing, Las Vegas, NV, USA, 26–29 July 2021.
32. Shi, L.; Nazir, S.; Chen, L.; Zhu, R. Secure Convergence of Artificial Intelligence and Internet of Things for Cryptographic Cipher: A Decision Support System. *Multimed. Tools Appl.* **2021**, *80*, 31451–31463. [CrossRef]
33. Oh, S.Y.; Ghose, S.; Jeong, Y.K.; Ryu, J.K.; Han, J. Convergence security systems. *J. Comput. Virol. Hacking Tech.* **2015**, *11*, 119–121. [CrossRef]
34. Shin, Y.S.; Han, S.H.; Yu, I.J.; Lee, J.Y. A Study on the Linkage between Intelligent Security Technology based on Spatial Information and other Technologies for Demonstration of Convergence Technology. *J. Korea Acad. Ind. Coop. Soc.* **2018**, *19*, 622–632. [CrossRef]
35. Alalade, E.D. Intrusion Detection System in Smart Home Network Using Artificial Immune System and Extreme Learning Machine Hybrid Approach. In Proceedings of the IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020.
36. Humphry, J.; Chesher, C. Visibility and security in the smart home. *Convergence* **2021**, *27*, 1170–1188. [CrossRef]
37. Upadhyay, D.; Sharma, S. Convergence of Artificial Intelligence of Things: Concepts, Designing, and Applications. In *Towards Smart World: Homes to Cities Using Internet of Things*; Sharma, L., Ed.; Chapman and Hall/CRC: Boca Raton, FL, USA, 2020; pp. 119–142.
38. Lee, B.; Jung, W.S. Intelligent disaster safety warning system through risk level analysis. In Proceedings of the 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; pp. 2187–2191.
39. Fenz, S.; Ekelhart, A.; Neubauer, T. Information security risk management: In which security solutions is it worth investing? *Commun. Assoc. Inf. Syst.* **2011**, *28*, 22. [CrossRef]
40. Straub, D.W.; Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Q.* **1998**, *22*, 441–469. [CrossRef]
41. Rehak, D. Introduction to risk management issues. In *Security Technologies, Systems, and Management II*; Lukas, L., Ed.; VerBuM: Zlin, Czech Republic, 2012; pp. 74–95.
42. Hromada, M.; Lukas, L. Security Assurance Models. In *Security Theory*; Lukas, L., Ed.; VerBuM: Zlin, Czech Republic, 2017; pp. 72–85.
43. Walt, S.M. The renaissance of security studies. *Int. Stud. Q.* **1991**, *35*, 211–239. [CrossRef]

44. Bertocchi, G.; Bologna, S.; Carducci, G.; Carrozzi, L.; Cavallini, S.; Lazari, A.; Oliva, G.; Traballesi, A. *Guidelines for Critical Infrastructure Resilience Evaluation*; Italian Association of Critical Infrastructures' Experts: Rome, Italy, 2016.
45. Nan, C.; Sansavini, G. A quantitative method for assessing resilience of interdependent infrastructures. *Reliab. Eng. Syst. Saf.* **2017**, *157*, 35–53. [CrossRef]
46. Cai, B.; Xie, M.; Liu, Y.; Liu, Y.; Feng, Q. Availability-based engineering resilience metric and its corresponding evaluation methodology. *Reliab. Eng. Syst. Saf.* **2018**, *172*, 216–224. [CrossRef]
47. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T. Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 125–138. [CrossRef]
48. Vennam, P.; Pramod, T.C.; Thippeswamy, B.M.; Kim, Y.G.; Pavan Kumar, B.N. Attacks and preventive measures on video surveillance systems: A review. *Appl. Sci.* **2021**, *11*, 5571. [CrossRef]
49. Pappalardo, A. A Framework for Threat Recognition in Physical Security Information Management. Doctoral Dissertation, University of Naples Federico II, Naples, Italy, 2013.
50. González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors* **2021**, *21*, 4759. [CrossRef]
51. Lukas, L. Algorithm for calculating the resilience of protection system from the viewpoint of converged security. In *Converged Security*; Lukas, L., Ed.; VerBuM: Zlin, Czech Republic, 2019; pp. 113–126.
52. Malik, P. Converged security and its importance. In *Converged Security*; Lukas, L., Ed.; VerBuM: Zlin, Czech Republic, 2019; pp. 43–56.
53. Kopacek, V. PSIM/SIEM category systems as a data source for resilience assessment. In *Converged Security*; Lukas, L., Ed.; VerBuM: Zlin, Czech Republic, 2019; pp. 169–183.
54. Physical Security Information Management (PSIM) and Situation Management. Available online: http://www.qognify.com/situation-management-psim/ (accessed on 13 March 2023).
55. TTC Marconi. *Technical Documentation of the Functional Sample: Analytical Software Module for Real-Time Resilience Assessment from the Point of View of Converged SECURITY*; TTC Marconi: Prague, Czech Republic, 2019.
56. Bosch, R. NICE Systems Deal Finalized, Name Changed to Qognify. Available online: https://www.securitysales.com/news/nice_is_selling_its_video_surveillance_business_for_100m/ (accessed on 25 June 2023).
57. Budin, E. *The Use of Automated Tools for Managing Information Security According to the Standards of the CSN ISO/IEC 27,000 Series*; Masaryk University: Brno, Czech Republic, 2014.
58. SIEM Technologies—Streamline Your System Security Management. Available online: https://www.wallarm.com/what/siem-whats-security-information-and-event-management-technology-part-1 (accessed on 10 July 2023).
59. Bernatik, A.; Senovsky, P.; Senovsky, M.; Rehak, D. Territorial Risk Analysis and Mapping. *Chem. Eng. Trans.* **2013**, *31*, 79–84. [CrossRef]