Smart City Infrastructure Resilience

Subjects: Engineering, Civil

Contributor: Martin Hromada , David Rehak , Bartosz Skobiej , Martin Bajer

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. However, to achieve such goals, a high level of security and protection of key infrastructures, which are designated as critical, is necessary. The 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.

converged security | resilience assessment | smart security alarm systems | Converged Security and Information Management System (CSIM)

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 [1].

The common ambition to shape and develop the scientific field of security is inherently connected and conditioned by the security theory development [2]. 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 [3]. As stated, the increasing demand for security is pragmatically connected with the need for practice and therefore also with the security of infrastructure systems.

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 [4]. 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 [5]. 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 [6]. 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 [7]: *"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 [8][9].

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 [10]. 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 [11]. 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 [12]. 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 [13]. 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 [14]. 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 [15].

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 [16][17][18]. 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 [19][20].

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 [21][22][23]. 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 [24][25][26].

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 [27][28]. 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.

4. Smart Security Alarm Systems Convergence

A wide group of authors dealt with the security systems convergence issue. As an example, article [29] discussed approaches linked to a comprehensive understanding of cyber security. Another theoretical model was presented in [23][30]. The convergence of cyber security and just security using smart security alarm systems is elaborated in the publication [24] where the need for convergence physical access controls and cyber security was presented. Technologically more advanced approaches were subsequently presented in a publication [31], 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 [32], 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 [33]. 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 [34].

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.

References

1. Lukas, L.; Urbancokova, H. Types of Security and their Convergence. In Converged Security; Lukas, L., Ed.; VerBuM: Zlin, Czech Republic, 2019; pp. 26–42.
2. Hettne, B. Development and Security: Origins and Future. Secur. Dialogue 2010, 41, 31–52.
3. Plachkinova, M.; Maurer, C. Security breach at target. J. Inf. Syst. Educ. 2018, 29, 11–20.
4. 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.
5. Pescaroli, G.; Alexander, D. Critical Infrastructure, Panarchies and the Vulnerability Paths of Cascading Disasters. Nat. Hazards 2016, 82, 175–192.
6. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control. Syst. Mag. 2001, 21, 11–25.
7. National Infrastructure Advisory Council. Critical Infrastructure Resilience Final Report and Recommendations; U.S. Department of Homeland Security: Washington, DC, USA, 2009.
8. Elvas, L.B.; Mataloto, B.M.; Martins, A.L.; Ferreira, J.C. Disaster Management in Smart Cities. Smart Cities 2021, 4, 819–839.
9. Tzioutziou, A.; Xenidis, Y. A Study on the Integration of Resilience and Smart City Concepts in Urban Systems. Infrastructures 2021, 6, 24.
10. 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.
11. 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.
12. 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.
13. 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.

14. 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.
15. Hromada, M.; Rehak, D.; Lukas, L. Resilience Assessment in Electricity Critical Infrastructure from the Point of View of Converged Security. Energies 2021, 14, 1624.
16. Anderson, K. Convergence: A Holistic Approach to Risk Management. Netw. Secur. 2007, 5, 4–7.
17. Spears, J.L.; Barki, H. User Participation in Information Systems Security Risk Management. MIS Q. 2010, 34, 503–522.
18. Aleem, A.; Wakefield, A.; Button, M. Addressing the Weakest Link: Implementing Converged Security. Secur. J. 2013, 26, 236–248.
19. Christensen, J.F. Industrial Evolution Through Complementary Convergence: The Case of IT Security. Ind. Corp. Chang. 2011, 20, 57–89.
20. Chang, H.; Kim, J.; Park, J. IT Convergence Security. J. Intell. Manuf. 2014, 25, 213–215.
21. Schneller, L.; Porter, C.N.; Wakefield, A. Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators. Secur. J. 2023, 36, 333–349.
22. 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.
23. Anand, S. Convergence of Cyber and Physical Security—A must for Smart Grid Systems. PalArch's J. Archaeol. Egypt Egyptol. 2020, 17, 8055–8060.
24. Park, S.; Ko, D. Design of the Convergence Security Platform for Smart Universities. J. Platf. Technol. 2015, 3, 3–7.
25. Kang, J.; Lee, J.; Hwang, C.; Chang, H. The Study on a Convergence Security Service for Manufacturing Industries. Telecommun. Syst. 2013, 52, 1389–1397.
26. 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.
27. 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.
28. 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.

29. 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.
30. 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.
31. 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.
32. Humphry, J.; Chesher, C. Visibility and security in the smart home. Convergence 2021, 27, 1170–1188.
33. 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.
34. 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.