IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 12, No. 4, August, 2022, pp. 459-465
Journal homepage: http://iieta.org/journals/ijsse

Review of Security Principles and Security Functions in Critical Information Infrastructure Protection

Prasetyo Adi Wibowo Putro*, Dana Indra Sensuse

Faculty of Computer Science, Universitas Indonesia, Depok 16424, Indonesia

Corresponding Author Email: prasetyo.adi01@ui.ac.id

https://doi.org/10.18280/ijsse.120406

Received: 18 May 2021
Accepted: 26 June 2022

Keywords:
critical information infrastructure, protection, security principle, security function

ABSTRACT

There is quite a lot of research on Critical Information Infrastructure Protection (CIIP), but what threats and vulnerabilities are considered in the security principle offered is unknow. Likewise, the security functions provided have not been measured. This study is a review of CIIP using the Kitchenham framework. From 31 scientific publications and 5 CIIP standards, it was found that there were 13 threats and 16 vulnerabilities were categorized into three security principles. As a result of measuring security functions on CIIP, we found that only 25% provide all security functions.

1. INTRODUCTION

Critical Infrastructure (CI) defines critical infrastructure as essential human-made assets related to energy, communication, and water supply that support continuity and welfare [1]. In order to maintain the continuity of a CI, we must identify and secure the Critical Information Infrastructure (CII) in it [2]. CII is defined differently by several countries [3, 4], but the similarity of these definitions is that this infrastructure is related to CI, the leading security asset. Cybersecurity guidelines define CII as a system provided or operated by CI providers [5]. It is very important to be protecting CII because CI management already uses an electronic system so that CI services depend on CII security

Currently, many countries have identified existing CII services and categorized them into several sectors [3]. There are five sectors: finance, energy, transportation, water, and food. In addition, some countries add to the defense, technology, and government sectors, but other policies incorporate these fields into other sectors [6]. Several countries have also made CII safeguard policies that consider national risks [7]. However, many have recently identified the CII sector based on national risk and let the CII Protection to the CII service operators according to existing information security standards [8].

Information security standards are different for vital infrastructure than for general infrastructure [9]. Information security standards, better known as Information Security Management Systems (ISMS), focus on business objectives with a custom domain to business processes. Meanwhile, CII Protection (CIIP) security functions, focused on Preventive, Detective, Corrective, Deterrent, Recovery, and Compensation [10].

Some information security incidents occurred on the CII, although national security policies were in place. For example, in September 2020, a hospital in Germany whose database was attacked was forced to refuse emergency patients, resulting in the death of a woman who did not make it to the nearest hospital twenty miles away [11]. Great Britain was also affected by the Ransomware WannaCry attack on many hospitals, resulting in inaccessible medical data and national service providers having to cancel more than 19,000 medical appointments [12]. The two attacks against CII above occurred because CIIP was carried out only by implementing ISMS at the operator level. Therefore, CIIP must pay more attention to threats and impacts on continuity and national welfare [7].

Several international CIIP standards provide a comparison with other standards to show their connectivity capabilities [4, 13]. Review on national standards was also conducted on the CIIP national policy as a form of evaluation in strengthening. In 2009, 20 national and five inter-country CIIP policies were reviewed [3]. The result shows similarity between the CIIP security principles and the CII strategic sectors. Despite the international CIIP standard, there is still a large CIIP gap between developed and developing countries [14]. CI with inadequate protection and unstructured protection often becomes a zombie to carry out attacks. [15].

Strengthening CIIP can also be done using research results. There is quite a lot of research on CIIP published on three reputable scientific journals in information infrastructure [16]. A review of critical information infrastructure has also been carried out specifically on the security assessment method for industrial control systems [17]. Similar research specifically reviews the measurement of risk in strategic industries [18]. However, based on the reviews conducted [19], research on CIIP has not met Reliability, Availability, Maintainability, and Safety/security parameters (RAMS). As a part of information security, it is also necessary to know whether CIIP have the same security principles with information security.

The Security Principle is a must-have trait in information security [20]. These traits can be lost due to threats or vulnerabilities. Therefore, information security principles are often used to classify threats and vulnerabilities. Common security principles namely confidentiality, integrity, and availability [10]. No one is more important than the other in these three principles. In fact, this principle can be added by other properties according to the needs of the organization.

This research is a literature review of scientific articles and standards in CIIP based on information security principles and functions. The results of this review are expected to provide information on security principles and security functions that have so far been considered problematic. Threats and vulnerabilities are looked at for each literature and then grouped according to information security principles. Threats, vulnerabilities, and security functions in each literature, is use to describe relationship between security principles and security functions in CIIP.

This article will be organized as follows: Chapter 1 will explain the motivation, problems, and research contributions. The review methodology will be explained in Chapter 2. Chapter 3 will explain the results from each literature and discuss the findings in Chapter 4. In the end, Chapter 5 will answer the research questions, limitations, and further research.

2. METHODOLOGY

Review in this study used Kitchenham's Systematic Literature Review (SLR) protocol [21]. SLR is a literature study method that identifies, assesses, and interprets findings on a research topic to answer predetermined research questions [22]. Although The Kitchenham protocol has not provided methods for synthesizing/analyzing findings, this protocol is considered ideal for describing security functions and classifying threats and vulnerabilities into security principles [23].

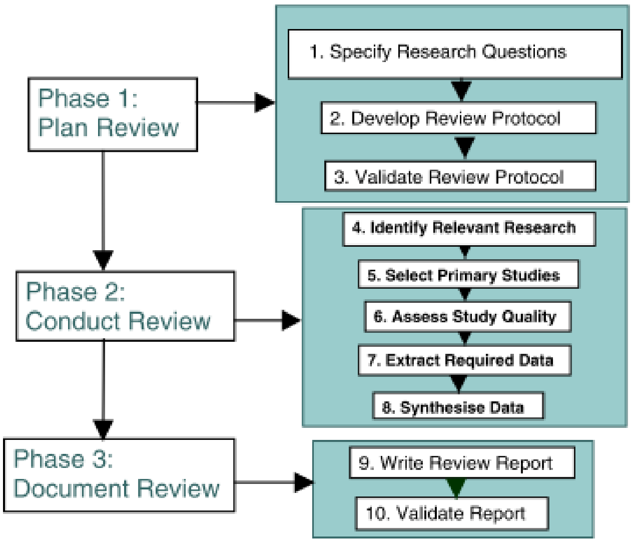

Figure 1. SLR methodology [21]

The Kitchenham SLR methodology consists of 10 steps, as shown in Figure 1. The first step to the third step is the planning stage that describes the methodology used. Steps four through Step seven describe the literature results obtained. The final stage is Step eight, which synthesizes data from the literature to answer research questions. Steps 9 and 10 relating to the Report take the form of making this scientific article.

2.1 Specify research questions

To answer the research problem as previously described, two research questions were made as follow:

RQ1: What is the security principle of Critical Information Infrastructure?

RQ2: Is the security model that fulfills the Critical Information Infrastructure Security function?

2.2 Develop review protocol

The preparation of the research protocol began by compiling the research aspects and describing them into Population, Intervention, Comparison Outcomes, and Context (PICOC) as in Table 1. Based on the PICOC aspects, the SLR protocol was compiled as in Table 2. Five publication databases were selected according to the availability of accessing the full articles on those databases. Search string are arranged based on the PICOC aspect and added with the * character to accommodate variations in word writing in the search sentence. Because information security is a dynamic technology suited to the newest attacks and vulnerabilities, the publication was selected from international conference proceedings and journals with an index of Q1 to Q3 from 2016 until 2020.

Table 1. PICOC aspect of the research

Aspect	Value
Population	Critical Information Infrastructure
Intervention	Protection, Security
Comparison	n.a.
Outcome	Model, Framework, Implementation, Application
Context	Academic Research, Applied Research

Table 2. SLR protocol

Rules	Content
Keywords	Critical Information Infrastructure Protection
Database	ACM, IEEE Xplore, Scopus, SpringerLink, ScienceDirect
Search string	Critical* AND information* AND infrastructure* AND (Protection* OR Security*) AND (Model* OR framework*)
Inclusion Criteria	Publication 2016 to 2020 English publications Journal of Q1, Q2, Q3, and Proceedings
Exclusion Criteria	Not discuss sectors in the Critical Information Infrastructure Not discussing security models or frameworks Not Full-Text paper No recommendation of a specific model or framework Research literature review

2.3 Validate SLR protocol

The SLR protocol in Table 2 is the validated protocol that used in this study. Protocol validation was carried out through discussion between the authors and consultation with those familiar with CCIP. At this validation stage, the SLR protocol was revised twice. The protocol was first tested in the IEEE Xplore database to determine search sentences according to the scope of the search results. Furthermore, the Complete protocol was made, and the literature obtained was consulted, and the latest version of the SLR protocol was obtained from the second improvement.

3. RESULT

The SLR results are a series of identifying relevant research processes to extract required data. The selected literature is obtained from the identification stage of relevant research to assess the quality of the research, as shown in Figure 2. These results will be extracted and become the basis for synthesis.

3.1 Identify relevant research

This stage is carried out by searching based on the search sentences that have been compiled. The search sentence must be adjusted for searches on the Science Direct database because it cannot process star characters (*).

3.2 Select primary study

A selection is carried out at this stage based on inclusive exclusive criteria, as listed in Table 2. This stage also eliminates the duplication of publications because they appear in several databases. The primary study was selected by looking at the publication metadata, including abstracts and references. Snowball analysis was also conducted to identify new literature based on references. The results of the Snowball analysis continued to use the same inclusive and exclusive criteria as the SLR protocol.

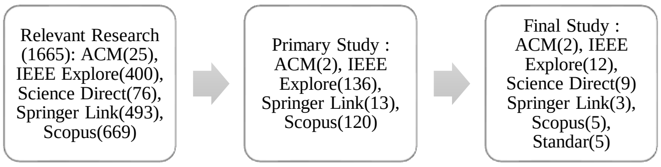
Relevant Research (1665): ACM(25), IEEE Explore(400), Science Direct(76), Springer Link(493), Scopus(669)
Primary Study : ACM(2), IEEE Explore(136), Springer Link(13), Scopus(120)
Final Study : ACM(2), IEEE Explore(12), Science Direct(9) Springer Link(3), Scopus(5), Standar(5)

Figure 2. Literature selection process

3.3 Access study quality

The literature quality assessment is carried out based on the questions as in Table 3. Literature that is declared quality is literature that meets all the existing criteria. Based on the reference list in selected literature, five international standards for information security were identified. National policies on safeguards are not included in the primary literature because not all national policies on CIIP are published in full. Based on the SLR stages carried out, 36 pieces of literature consisting of 31 scientific articles and five international CIIP standards have been obtained.

Table 3. List of quality assessment questions

Checklist	Quality Assessment Question
C1	Clearly describe the research objectives?
C2	Have a literature review, research background, and context?
C3	Show the main contribution of the research?
C4	Describe the proposed architecture or methodology used?
C5	Have research results?
C6	Provide conclusions that are relevant to the research objectives/concerns?
C7	Recommend future work or improvements in the future?

3.4 Data extraction

Data extraction was carried out for 25 scientific articles that had passed the quality test and 5 CIIP standards. The 30 pieces of literature are grouped according to the strategic sectors discussed, referring to the division of 9 strategic sectors [8] as shown in Table 4. The nine strategic sectors are government, energy and mineral resources, transportation, finance and banking, health technology and telecommunications, defense, food, and strategic industries. After data extraction, six scientific articles were found that did not specifically describe the strategic sector under study. One generic sector is added for literature that does not explicitly mention the strategic sector understudy.

From the reviewed literature, we find that many threats are considered in CIIP. Each researcher uses their terminology. If we use terminology based on the literature obtained, the CIIP threats are mostly about Cyber-attacks [24-32]. This cyber-attack can be in the form of DDoS on the Power Grid [24], Web attack [31], or attack the point of Sale (POS) [30]. Apart from cyberattacks, there are also External attacks [33, 34], Insider Threat [35, 36], Unauthorized Access [37, 38], Targeted attacks [39, 40], Hybrid Threats [41], Hazardous Event [42], Nature Disasters [43], Social Engineering [44], Falsification Attacks [45], Breach Attack [46], Data Theft [47], and Data Tampering [48] commonly found in CIIP.

Table 4. Data extraction

Strategic Sector	Related Literature
Government	[24-28, 33]
Energy and Natural Resource	[43-46, 49]
Transportation	[29, 36, 50]
Finance	[30, 31, 47, 51]
Health	[52]
Telecommunication Technology	[53]
Defense	[34]
Food	[48, 54, 55]
Strategic Industry	[32, 39]
Generic	[4, 8, 13, 35, 37, 38, 40-42, 56]

If we quote directly from the literature, vulnerability also has many terms. Many CIIPs have Poor Interoperability vulnerabilities [24-28, 33, 55]. There is a lack of connection between CII managers, so it is necessary to control safeguards to avoid risks. Other vulnerabilities found in the literature are Misconfigured Security Control [32, 37, 47], Collaborative Systems [38, 52], Financial Vulnerability [30, 31], Operator Mistakes [35, 44], Lack Traceability [48, 54], Unsecure Framework [53], Internal Turmoil [34], Unresolved Risk [42], Unknown Machine Failure [43], Manual Negotiation of Access Control [49], IoT Interconnection [45], Insecure Communication Technology [46], No Defense In-Depth [36], Sensor Misconfiguration [29], and Design Vulnerability [39].

Meanwhile, to identify CIIP needs, the theory of six security functions is used, namely Preventive, Detective, Corrective, Deterrent, Recovery, and Compensation. The security function is also not fully accommodated in the literature reviewed. Only research in the government sector [26-28, 33], strategic industry [32], dan generic [8, 37, 56] found a security model with complete security functions. In addition, CIIP standards also accommodate all security functions.

4. DISCUSSION

4.1 Threat and vulnerability on critical information infrastructure protection

Several threats and vulnerabilities found in CIIP are similar, such as cyber-attack, web attack, targeted attack, breach attack, and point of sale attack. Therefore, the classification of threats and vulnerabilities uses the Security Principles. Security principles are used to identify security issues discussed in the literature, namely confidentiality, necessity, and availability.

If each threat and vulnerability are grouped on the security principle, it turns out that the most threats and vulnerabilities are in availability, as shown in Table 5. A total of 35 of the 36-literature reviewed identified availability as a risk that needs to be considered for CIIP. In addition, 21 CIIP models were made by considering all Security Principles. In addition to this, the principle of confidentiality has not been much considered in creating the CIIP model. If we analyze further using Table 4 and Table 5, we find that the principle of confidentiality is not yet considered in the Energy and Natural Resources, Food, and Strategic Industries sectors. This happens because this sector prioritizes service availability so that other security principles, such as confidentiality, will adjust to availability needs.

To support the security function, all three security principles must be met. From the existing literature, there are 21 literatures that accommodate all security principles. The three security principles are only found in the literature [24-28, 30, 31, 33, 35, 37, 41, 42, 50-53]. Whereas for literature in the form of CIIP standards [4, 8, 13, 56], all of them have met the security principle. This means that it is expected that later 58.33% of the CIPP model can fulfill all security functions.

Table 5. Security principle of critical information infrastructure protection

Security Principle	Related Literature	Sum
Confidentiality	[4, 8, 13, 24-28, 30, 31, 33-37, 41, 42, 47, 50-53, 56]	23
Integrity	[4, 8, 13, 24-29, 30-35, 37 39, 41-56]	33
Availability	[4, 8, 13, 24-34, 36-56]	35

4.2 Security function on critical information infrastructure protection

The existing CIIP model is more focused on the Preventive function. Based on the reviewed literature, as shown in Table 6, the Preventive security function is the most accommodated, followed by Compensation, which is also an alternative to the preventive function. This condition is quite reasonable considering that CII is a strategic sector where it is hoped that risks will never occur so that the function of prevention is prioritized. However, it is unfortunate that only nine pieces of literature, or 25% of the total literature, provide a complete Security Function.

Table 6. Security function on critical information infrastructure protection

Security Function	Related Literature	Sum
Preventive	[4, 8, 13, 25-38, 41, 43-56]	33
Detective	[4, 8, 13, 24, 26-33, 36, 37, 39, 40, 45-47, 53, 55, 56]	22
Corrective	[4, 8, 13, 26-28, 32, 33, 37, 45, 47, 55, 56]	13
Deterrent	[4, 8, 13, 26-28, 32, 36-38, 41, 47, 50-53, 56]	17
Recovery	[4, 8, 26-28, 32, 33, 37, 47, 55, 56]	11
Compensation	[25-34, 36-38, 41, 42, 45-48, 52-55]	23

The sum of security functions that CIIP accommodates is too small if we compare it with all of literature that meets security principles. For example, suppose 21 CIIP models fulfil all security principles. In that case, there should also be 21 security models that provide security functions because the principles of confidentiality, integrity, and availability should be sufficient to provide all security functions. Furthermore, the security controls used in CIIP, such as encryption, access control, digital signature, hash function, and detection systems, are not a type of security control that counter other security functions.

It turns out that the CIIP standard also has a security function gap. For example, the financial security standard (PCI DSS) does not accommodate the detective, corrective, and recovery functions. Likewise, the generic security standard (CIS) did not provide a recovery function. Nevertheless, it is possible to present these security functions because several scientific articles on the sector can provide this function.

Based on the identification of security principles and security functions, the relationship among can be described in Figure 3. Based on the literature review carried out, it turns out that confidentiality has no impact on the security function. Although no principle of confidentiality was considered, security function preventive [29, 32, 38, 43-46, 48, 49, 54, 55], detective [32, 39, 40, 45, 46, 55], corrective [32, 45, 55], deterrent [32, 38], recovery [32, 55] and compensation [29, 32, 38, 45, 46, 48, 54, 55] were found. This condition is different from Integrity which has correlation with corrective and recovery, and Availability with its correlation to all security function.

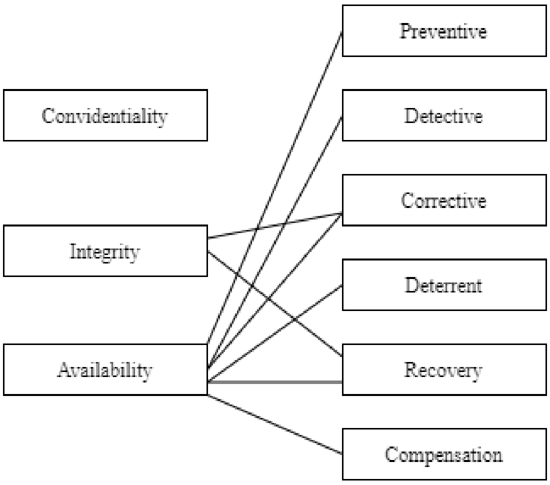

Figure 3. Relationship between security principles and security functions

5. CONCLUSION

There were 13 threats and 16 vulnerabilities considered for the CIIP model. If we classify the threats and vulnerabilities according to the Security Principle, we get it 58.33% of the security models have considered the principles of confidentiality, integrity, and availability. Although quite much of the security model considers the whole security principle, it turns out that only 25% of the CIIP security model fulfills the Critical Information Infrastructure Security function. Most security models still focus on the Preventive function, with availability as the primary security principle.

The relationship between security principles and security functions has also been identified based on the literature obtained. For further study, this relation offered can be reviewed with more literature or an information security perspective. For example, a new model that complements the standard can be proposed, which does not yet provide a complete security function. Further research can also be carried out by identifying model in CIIP.

ACKNOWLEDGMENT

I would like to thank Indonesia Endowment Fund for Education (LPDP) from the Ministry of Finance Republic Indonesia for granting the scholarship and supporting this research.

This research was supported by E-Government and E-Business Laboratory, Faculty of Computer Science, Universitas Indonesia.

REFERENCES

[1] Bailes, A.J.K., Frommelt, I. (2004). Business and Security Public – Private Sector Relationships. Solna, Sweden: Stockholm International Peace Research Institute, p. 328.

[2] Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protebtion, 8: 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

[3] Brunner, E.M., Suter, M. (2009). International CIIP Handbook 2008/2009. Zurich: ETH Zurich.

[4] Barrett, M. (2018). Framework for improving critical infrastructure cybersecurity. Cybersecurity Framework. National Institute of Standards and Technology, p. 55. https://doi.org/10.6028/NIST.CSWP.04162018

[5] ISO/IEC. (2012). ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.

[6] ENISA. (2015). Critical Information Infrastructures Protection approaches in EU. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-, accessed on Apr. 21, 2021.

[7] Keen, W. (2020). Safeguarding Critical National Infrastructure: Risk & Opportunities. Singapore.

[8] Suter, M. (2007). A Generic National Framework for Critical Information Infrastructure Protection (CIIP). Center for Security Studies, no. August. International Telecommunication Union, Zurich. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf.

[9] Białas, A. (2006). Information security Systems vs. Critical information infrastructure protection Systems - Similarities and differences. Proc. Int. Conf. Dependability Comput. Syst. DepCoS-RELCOMEX 2006, pp. 60-67. https://doi.org/10.1109/DEPCOS-RELCOMEX.2006.30

[10] Harris, S., Maymi, F. (2019). All-in-One CISSP® All-in-One Exam Guide. Mc-Graw Hill.

[11] Eddy, B.M., Perlroth, N. (2021). Cyber Attack Suspected in German Woman's Death. The New York Times, 2021. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html, accessed Apr. 21, 2021.

[12] Kaspersky. (2020). Ransomware WannaCry: All you need to know | Kaspersky. Kaspersky Resource Centre. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry, accessed on Apr. 21, 2021.

[13] Center for Internet Security. (2019). CIS Controls Version 7.1. Cent. Internet Secur., pp. 47-49.

[14] International Telecommunication Union. (2020). Global Cybersecurity Index (GCI).

[15] Ellefsen, I., von Solms, S. (2010). Critical information infrastructure protection in the developing world. In: Moore, T., Shenoi, S. (eds) Critical Infrastructure Protection IV. ICCIP 2010. IFIP Advances in Information and Communication Technology, vol 342. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-16806-2_3

[16] Scimagojr. (2015). SJR - Journal Search. https://www.scimagojr.com/journalsearch.php?q=critical+infrastructure, accessed on Apr. 22, 2021.

[17] Qassim, Q.S., Jamil, N., Daud, M., Patel, A., Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. Information and Computer Security, 27(1): 47-61. https://doi.org/10.1108/ICS-04-2018-0048

[18] Fakiha, B. (2021). Business organization security strategies to cyber security threats. International Journal of Safety and Security Engineering, 11(1): 101-104. https://doi.org/10.18280/ijsse.110111

[19] Pirbhulal, S., Gkioulos, V., Katsikas, S. (2021). A systematic literature review on RAMS analysis for critical infrastructures protection. International Journal of Critical Infrastructure Protection, 33: 100427. https://doi.org/10.1016/j.ijcip.2021.100427

[20] ISO/IEC. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and Vocabulary. ISO/IEC27002:2018. [Online]. Available: http://www.worldcat.org/title/service-operation/oclc/254028066&referer=brief_results%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf%0Ahttp://k504.kh.

[21] Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software, 80(4): 571-583. https://doi.org/10.1016/j.jss.2006.07.009

[22] Kitchenham, B. (2004). Procedures for performing systematic literature reviews. Jt. Tech. Report, Keele Univ. TR/SE-0401 NICTA TR-0400011T.1, 33: 33. http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf.

[23] Paré, G., Trudel, M.C., Jaana, M., Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. Inf. Manag., 52(2): 183-199. https://doi.org/10.1016/j.im.2014.08.008

[24] Mohammad, N. (2019). A multi-tiered defense model for the security analysis of critical facilities in smart cities. IEEE Access, 7: 152585-152598. https://doi.org/10.1109/ACCESS.2019.2947638

[25] Sung, Y., Sharma, P.K., Lopez, E.M., Park, J.H. (2016).

FS-OpenSecurity: A taxonomic modeling of security threats in SDN for future sustainable computing. Sustain., 8(9). https://doi.org/10.3390/su8090919

[26] Ramtohul, A., Soyjaudah, K.M.S. (2016). Information security governance for e-services in southern African developing countries e-Government projects. J. Sci. Technol. Policy Manag., 7(1): 26-42. https://doi.org/10.1108/JSTPM-04-2014-0014

[27] Rodríguez-Hoyos, A., Rebollo-Monedero, D., Burgos, R.T., Estrada-Jiménez, J., Forné, J., Romero, A.Á., Rodríguez, R.D. (2019). Anonymizing cybersecurity data in critical infrastructures: The CIPSec approach. Proceedings of the International ISCRAM Conference, pp. 1198-1208.

[28] Buscemi, G., Angelucci, B., Di Mascolo, M., Nardelli, M., Damiani, A. (2015). Title: Comprehensive security framework for copernicus: Free & open data access. TNC 2015 - Connected Communities.

[29] El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J., Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. Veh. Commun., 23: 100214. https://doi.org/10.1016/j.vehcom.2019.100214

[30] Catota, F.E., Morgan, M.G., Sicker, D.C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. J. Cybersecurity, 4(1): 1-20. https://doi.org/10.1093/cybsec/tyy002

[31] Martinelli, F., Mercaldo, F., Nardone, V., Orlando, A., Santone, A., Vaglini, G. (2018). Safety critical systems formal verification using execution traces. 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 247-250. https://doi.org/10.1109/WETICE.2018.00054

[32] Yamada, T., Nakano, T., Kaji, T., Tano, S. (2020). Security introduction framework for operational technologies and applying to industrial control system. 2020 59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), pp. 25-30. https://doi.org/10.23919/SICE48898.2020.9240268

[33] Slipachuk, L., Toliupa, S., Nakonechnyi, V. (2019). The process of the critical infrastructure cyber security management using the integrated system of the national cyber security sector management in Ukraine. 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), pp. 451-454. https://doi.org/10.1109/AIACT.2019.8847877

[34] Roy, S., Nene, M.J. (2016). Analysis and recommendations for network and communication security for mission critical infrastructure. ICACCS 2016 - 3rd International Conference on Advanced Computing and Communication Systems: Bringing to the Table, Futuristic Technologies from Arround the Globe, pp. 1-8. https://doi.org/10.1109/ICACCS.2016.7586382

[35] Morovati, K., Kadam, S., Ghorbani, A. (2016). A network based document management model to prevent data extrusion. Comput. Secur., 59: 71-91. https://doi.org/10.1016/j.cose.2016.02.003

[36] Nace, L. (2020). Securing trajectory based operations through a zero trust framework in the NAS. Integrated Communications, Navigation and Surveillance Conference, ICNS, pp. 1B1-1-1B1-8. https://doi.org/10.1109/ICNS50378.2020.9222912

[37] Limba, T., Plėta, T., Agafonov, K., Damkus, M. (2017). Cyber security management model for critical infrastructure. Entrep. Sustain. Issues, 4(4): 559-573. https://doi.org/10.9770/jesi.2017.4.4(12)

[38] Aali, N.A., Baina, A., Echabbi, L. (2016). Evaluation of interaction messages in trust model within collaborative system. 2016 International Conference on Information Technology for Organizations Development, IT4OD 2016, pp. 1-6. https://doi.org/10.1109/IT4OD.2016.7479262

[39] Cruz, T., Rosa, L., Proença, J., Maglaras, L., Aubigny, M., Lev, L., Jiang, J., Simões, P. (2016). A cybersecurity detection framework for supervisory control and data acquisition systems. IEEE Trans. Ind. Informatics, 12(6): 2236-2246. https://doi.org/10.1109/TII.2016.2599841

[40] Shaburov, A.S., Alekseev, V.R. (2019). Protection models of critical information infrastructure objects from targeted computer attacks. Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2019, pp. 335-338. https://doi.org/10.1109/EIConRus.2019.8656722

[41] Yevseiev, S., Aleksiyev, V., Balakireva, S., Peleshok, Y. (2019). Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy. Eastern-European J. Enterp. Technol., 3(9-99): 49-63. https://doi.org/10.15587/1729-4061.2019.169527

[42] Bialas, A. (2016). Risk management in critical infrastructure—Foundation for its sustainable work. Sustain., 8(3). https://doi.org/10.3390/su8030240

[43] Tidwell, V.C., Lowry, T.S., Binning, D., Graves, J., Peplinski, W.J., Mitchell, R. (2019). Framework for shared drinking water risk assessment. Int. J. Crit. Infrastruct. Prot., 24: 37-47. https://doi.org/10.1016/j.ijcip.2018.10.007

[44] Etigowni, S., Tian, D.J., Hernandez, G., Zonouz, S., Butler, K. (2016). CPAC: Securing critical infrastructure with cyber-physical access control. ACM Int. Conf. Proceeding Ser., pp. 139-152. https://doi.org/10.1145/2991079.2991126

[45] Pacheco, J., Ibarra, D., Vijay, A., Hariri, S. (2017). IoT security framework for smart water system. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), pp. 1285-1292. https://doi.org/10.1109/AICCSA.2017.85

[46] Menete, S., Mavee, A., Ehlers, E.M., Leung, W.S. (2017). Smart grid critical information infrasructure protection through multi-agency. 2017 Computing Conference, pp. 461-468. https://doi.org/10.1109/SAI.2017.8252138

[47] García, A., Dominguez, F., Calle, L., Martinez, J., Raymundo, C. (2018). Personal data protection maturity model for the micro financial sector in Peru. Int. J. Eng. Res. Technol., 11(4): 649-660. https://doi.org/10.1109/CATA.2018.8398649

[48] Chen, H., Chen, Z., Lin, F., Zhuang, P. (2021). Effective management for blockchain-based agri-food supply chains using deep reinforcement learning. IEEE Access, 9: 36008-36018. https://doi.org/10.1109/ACCESS.2021.3062410

[49] Ben Abdelkrim, I., Baina, A., Bellafkih, M. (2016). Automation of access control negotiation in dynamic coalitions for electrical critical infrastructures. 2016 International Conference on Electrical and Information Technologies (ICEIT), pp. 349-354.

https://doi.org/10.1109/EITech.2016.7519619

[50] Hudic, A., Smith, P., Weippl, E.R. (2017). Security assurance assessment methodology for hybrid clouds. Comput. Secur., 70: 723-743. https://doi.org/10.1016/j.cose.2017.03.009

[51] PCI Security Standards Council. (2018). Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures. pp. 1-139.

[52] Azeez, N.A., Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egypt. Informatics J., 20(2): 97-108. https://doi.org/10.1016/j.eij.2018.12.001

[53] Ptitsyn, P.S., Radko, D.V., Lankin, O.V. (2016). Designing architecture of software framework for building security infrastructure of global distributed computing systems. ARPN J. Eng. Appl. Sci., 11(19): 11599-11610.

[54] Aji, J.M.M. (2020). Linking supply chain management and food security: A Concept of building sustainable competitive advantage of agribusiness in developing economies. E3S Web of Conferences. https://doi.org/10.1051/e3sconf/202014206005

[55] Jabbar, K., Bjørn, P. (2018). Permeability, interoperability, and velocity: Entangled dimensions of infrastructural grind at the intersection of blockchain and shipping. ACM Trans. Soc. Comput., 1(3): 1-22. https://doi.org/10.1145/3288800

[56] ISO/IEC. (2013). ISO/IEC 27001:2013 Information Security Management System-Requirements. ISO/IEC 27001: 2013. International Organization for Standardization.