Journal of Engineering Science *Vol. XXVII, no. 3 (2020), pp. 134 - 145*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

DOI: 10.5281/zenodo.3949684
UDC 004.056.5

REVIEW ON USE OF DECISION SUPPORT SYSTEMS IN CYBER RISK MANAGEMENT FOR CRITICAL INFRASTRUCTURES

Aurelian Buzdugan*, ORCID ID: 0000-0003-1315-6672

Moldova State University, 60 Mateevici str., Chisinau, Moldova
**aurelian.buzdugan@yahoo.com*

Received: 05. 10. 2020
Accepted: 07. 06. 2020

Abstract. This paper uses the systematic literature review methodology to identify, analyze and evaluate the state of the art on the use of decision support systems for cyber risk management in critical infrastructures. This type of activity allows us to make a reliable and unbiased analysis of existing research and identify areas that need further exploration. Existing knowledge and studies on this topic are critically analyzed in order to better position future research actions in this field. Identifying, assessing, and managing the cyber risks of information technology components in critical infrastructure has a major impact on the overall security and safety of the entity. The amount of data that is required to be processed and analyzed is often beyond the capacity of the operator or decision makers. The aim is to explore the extent to which the decision support system is currently used to overcome this limitation in cyber risk management, to present rapid and informed responses to the identified risks.

Keywords: *critical infrastructure, cyber threats, cyber risk management, decision support systems, systematic literature review.*

Introduction

Critical infrastructures are the backbone of our economy, society as well as national security. The definition of critical infrastructure refers to physical or information technology (IT) facilities such as financial systems, energy, health, communications and key government services that if disrupted or damaged could have an impact on the safety, security or economy of citizens, as well the effective functioning of the government [1]. This explanation and the elements mentioned are similar to the definition adopted in countries such as US and Canada [2, 3].

Based on this description it can be deduced that there are different domains of critical infrastructure, such as finance, banking or key government services. These might be differently classified, however are converging to the definition above.

Due to the massive digitalization processes, the cyber implication in critical infrastructure can be considered traditional nowadays. Within the sectors listed above, there can be different levels of dependency on IT systems: for example in banking or finance the IT systems play a crucial role in most processes, whereas in manufacturing the IT systems are integrated with operational technology (OT) and form the so called cyber-physical interface. Therefore, the role of IT can range from representing the main system or software, to auxiliary roles such as sensing, anomaly detection or performing certain function within the OT. The later would have a strong connection with physical systems, and IT performs functions such as monitoring, decision making or even controlling the physical components.

Historically OT systems were disconnected from IT and focused mainly on the integrity and availability of system operations. The integration of IT brings cybersecurity risks and challenges among commodity and improvements. A cyber attack on a critical infrastructure could lead to physical damages, such as draining water in dams, overloading electricity networks in smart grids or even controlling industrial (e.g. chemical, nuclear, etc.) processes with the goal to create harm. Such attacks are actual and pose risks to the economy, society and citizens, both at a national and regional level.

The following challenges result from the interaction of IT and OT:

1. Safety and security concepts have emerged into one and require the cooperation between IT and OT engineers, as well as decision makers
2. IT Security controls and concepts need to be adapted and potentially re-designed to the needs and specifics of OT
3. Managing threats upon the IT and physical system requires horizontal cooperation between the teams and analysis of large amount of different type of data.

The above challenges create a context where cyber security and facility engineers should be working together, in order to be able to correlate vulnerabilities that IT systems introduce in the OT. It also requires reverse feedback in order for cyber security experts to understand the functions and importance of the physical components. A detailed modelling of processes and infrastructure is required in order to generate an overall perspective of cyber risks in critical infrastructures for the decision makers.

In addition, the interconnection between IT and OT increases the attack surface and number of vulnerabilities which can be exploited by threat actors. A remote attack on a previously isolated network has now become possible, as many of these systems are digital and have increased connectivity, often even to the Internet. This increases the requirement to protect the sensitive, sometimes even personal data, as well as the availability and integrity of the core processes.

The current situation intensifies the need to understand each cyber risk in relation to the critical infrastructure and how to efficiently control it. Due to the complexity of this process and amount of data, the industries are now looking into IT solutions for achieving these needs.

Risk management. Cyber risks.

In this chapter we will cover the definition of the terms related to cyber risks and clarify the context for the review process that we will perform in this paper. The ISO Guide 73:2009 defines the terms risk, risk management and risk management process as following [4]:

- A risk is the effect of uncertainty on objectives, which can have different aspects (safety, financial etc.) and be applied at different levels (strategic, product, process). The uncertainty term, as per ISO, refers to the state, or partial one, of lack of information to the understanding of an event, its consequence or likelihood.

- Risk management refers to coordinated activities to direct and control an organization with regard to risk
- Risk management process is a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

Whereas the ISO risk related terminology has some specifics, we believe that many of these terms are often used with interchangeable meanings in papers, literature and media unless otherwise specified. We will take into consideration the definition of specific terms and phases, however we assume that many times the reference is made to the core meaning of a risk as the result of threat, probability and consequences.

Another common understanding of managing risks is risk reduction. Studies have shown that the overall costs are considerably lower when reducing risks to an acceptable level, compared to the cost of the incident and hazard that this risk might have caused [5]. Whereas this conclusion is from a study focused on natural hazards, we see a direct connection with our research, as cyber security incidents can lead to safety events in critical infrastructures. Therefore, we consider the cyber risk management an actual and emerging topic. In our review, we will focus on cyber risks as the threats that arise from the cyberspace or the use of IT. The notion of "cyber risk" is not explicitly defined by ISO, however it became very popular and commonly used in the industry.

Cyber threats in the modern era

The focus that we have chosen on cyber risk management is based on the emergence of these threats upon the critical infrastructures and the need to identify and control these risks. Previously OT were associated with physical systems and the physical security of an entity was considered to be the main goal of the critical infrastructure security team. With the introduction of IT, the physical and cyber security domains have converged and mandate the cooperation between experts with knowledge from two various domains. Taking this into account, we believe risk management processes for ensuring physical security are mature enough and ensure an adequate level of protection in line with the current threats and risks. Therefore, we have decided to focus in our research on the cyber risk management in critical infrastructures, as we observe that IT and the associated risks create challenges in ensuring the safety and security of a critical infrastructure. Our focus is also influenced by the continuous increase in the past decade, both in number of cyber attacks as well as potential damage on critical infrastructures [6, 7].

The status of current cyber threats is well defined and has been evaluated as being ahead of the defensive reactions in the area of critical infrastructures [8]. This requires investment in the short term solely to the deterrence of cyber threats. We believe this contours the threat level, the increased probability as well as the need to take actions in improving the cyber risk management process in critical infrastructures.

In our view the above statement is applicable to most, if not to all countries, in terms of cyber threat perception in critical infrastructures. This provides us the necessary context to extract the facts that cyber threats are developing fast and defense is one step behind. In our view actions are required in order to improve the security stance of the underlying information systems in critical infrastructures.

In addition, there are different needs and strategies adopted that refer to securing the underlying information systems of critical services that are at the basis of the critical infrastructure [9]. As example, the main goal reflected by National Institute of Standards and Technology is to ensure that IT systems are adequately reliable and secure throughout the development life cycle, provides the necessary resilience, and thus supports the economy and national security [9]. Additionally, other objectives such as system modernization, increase the use of automation, as well as standardization and optimization of systems in order to strengthen the protection for high value assets are specified.

We believe the actions and strategies described by certain countries, relate and position the cyber threats as emerging risks for critical infrastructures.

Decision Support Systems

The definition of a decision support system (DSS) is relatively easy to perceive by the meaning of each of its terms. We will consider a DSS as per the definition of Filip as an evolving information system, anthropocentric and adaptive, which is designed to simulate the functions of advising in order to support the decision makers [10]. The DSS is a potential solution in overcoming human limits in terms of solving complex decisions or analyzing a large amount of data [11, 12]. We prefer this definition as it covers the required elements in the context of our review of cyber risks in critical infrastructures. DSS relate to a range of systems which include various technologies and aim in guiding and supporting the decision-making process [12,13]. Such systems can cope with multidimensional and complex topics, and can be considered as the substitution of a team of experts with different backgrounds [11, 12].

We have selected this type of systems, due to the exponential increasing interest of DSS in research [13]. On the other side, a DSS can be linked to related terms such as decision making or expert systems. We will focus on the DSS term as we consider it is comprehensive and covers the required factors in our research. This type of system can support the focus on a long term and sustainable solution in managing cyber risks in this domain.

The opportunities provided by a DSS also relate to NIST recommendations on increasing the use of automation wherever possible, due to factors as speed, effectiveness, and efficiency of executing actions part of the risk management process. We believe a DSS could support and implement this recommendation into practice, as these systems are conceptually able to perform real time, continuous assessment and monitoring of controls for the decision maker, and also support the cyber risk management process.

Another factor for using DSS are trends that were identified in the continuous integration between entities, diversity of cultures and technologies that are interconnected, as well as the pursuit of a sustainable development [14]. In our opinion, the same trends and factors can be observed in the development and digitalization of critical infrastructures and afferent risk management processes.

Systematic literature review

In this paper we will conduct a systematic literature review in order to identify, evaluate and summarize the state of art of decision support systems for cyber risk management in critical infrastructures. A systematic literature review (SLR) is a type of secondary study that uses a pre-defined methodology to identify, analyze and interpret all existing and available studies on a specific question [15]. Even though the SLRs are used in domains such as environment or medicine, the principles can be adjusted for other fields such as IT and software engineering [16].

We have selected this type of study as it reduces the likelihood of a bias, as well as creates a comprehensive overview on the desired topic. The results of the SLR will support us in evaluating the state of art of existing studies on our research question. The repeatable steps of a SLR in identification, extraction and information aggregation are considered to be linked to scientific research.

Problem definition and protocol

In the context of this SLR our main question is to evaluate the state of art in the use of DSS for cyber risk management in critical infrastructures. The objectives that we aim for are the following:

- To summarize the existing evidence of DSS for cyber risk management in critical infrastructures
- To identify gaps in current research, and suggest areas for further investigation.
- To provide the framework in order to appropriately position new research activities.
- To empower us to make a trustworthy and unbiased analysis on the proposed research question

The criteria for inclusion are:

- Studies that discuss the combination of cyber security, risk management, critical infrastructures and decision support systems
- Studies that mention systematic analysis of the literature to assess and manage cyber risks in critical infrastructures
- The studies describe decision support systems used in cyber risk management in critical infrastructures

The criteria for exclusion are:

- Studies that are not related to the main research question
- Studies that mention the need of a DSS however are not explicitly describing the system

The specific questions that we will evaluate the final list of selected papers upon are the following:

1. Is the paper describing or proposing a DSS?
2. Is decision support system a prototype or used in practice?
3. Does the paper explicitly focus on cyber risks? If not, on which type of risks does the paper focus on?
4. What areas of risks management are discussed?
5. Is the study oriented on generic critical infrastructures or specific domains?

Conducting the review. Identification of research

The search strategy that we have chosen was refined in order to cover the main research question and identify all existing related studies. We have performed preliminary searches to see whether SLR were conducted around our research topic, however none was found. We have done multiple trials in the identification of the right query. All searches were performed using the combination of the following terms: “critical infrastructure” and "decision support system" and "risk" and "cyber". Since decision support systems and critical infrastructures can be viewed as a wide range of systems, we have not considered other specific terms for our query such as SCADA, ICS, expert systems, data mining or business intelligence.

The differences in the search query compared to the inclusion criteria created additional manual work for us, however we decided on this approach as the number of results by querying the exact terms in the abstract and keywords was initially very low. In order to ascertain that we are not missing relevant results, we have decided to include more generic keywords such as "risk" and "cyber" and evaluate manually the articles against the inclusion criteria.

The selected sources to collect the existing studies on the research question sources are ACM, Science Direct and Springer [17 - 19]. These are leading platforms hosting peer-reviewed journals in technical areas such as IT, Critical Infrastructure and Risk Management.

The number of initial articles found and the final number of articles that were preserved for the SLR is described in Table 1.

Table 1

SLR sources and number of articles identified.

Source	Description	Total number of studies found	Number of studies selected to be reviewed
ACM	The ACM Digital Library is a research, discovery and networking platform containing: the Full-Text Collection of all ACM publications, including journals, conference proceedings, technical magazines, newsletters and books; and a collection of curated and hosted full-text publications from select publishers for Computing Literature.	12	1
Science Direct (open access)	A database with more than 2,900 journals and 300,000 books.	13	0
Springer	Database of peer-reviewed journals, articles, book chapters	68	5
Total		**93**	**6**

The query was conducted on April 4th, 2020. From the initial list we removed the articles that were not relevant to the research question and were focusing on certain elements related to our query by performing a screening on the title and keywords. After this first step of the triage the number of papers to be analyzed comprised 42 (ACM – 8, Science Direct – 6, Springer – 28). The next step was diagonal reading to assess whether the study is related to DSS in cyber risk management for critical infrastructure. The final list consisted of 6 papers to be reviewed. During the initial process we have noticed that there are very few studies tackling our research topic, and that most of them were elaborated more than 10 years ago. Therefore, we have repeated the entire screening process from the beginning, to ensure that we have identified the full list of studies relevant and related to our main question.

Data extraction

The studies that met the inclusion criteria were reviewed and the specific questions were answered in Table 2. This has empowered us to easier synthetize and summarize the findings.

Table 2

Evaluation of identified studies.

Author, (Year)	Does the paper explicitly focus on cyber risks? If not, on which type of risks?	What areas of risks management are discussed?	Does the study relate to generic or specific critical infrastructures?	Number of citations	Reference
Amantini et al. (2012)	Yes	All	Generic	9	[20]
Choraś, M., Kozik, R. (2009)	No, all	Identifying, Analyzing, Evaluating	Generic	4	[21]
Choraś, M., Flizikowski, A. (2010)	Yes	All	Specific: telecommunication, energy and transportation	6	[22]
Choraś, M., Kozik, R., (2010)	No, all	All	Generic	8	[23]
Setola et al. (2017)	No, all	Identifying, Analyzing, Evaluating	Generic	6	[24]
Kozik et al. (2010)	No, all	Identifying, Analyzing, Evaluating, Treating	Yes	4	[25]

The number of citations was extracted from the platform database in which the study was initially found.

Narrative synthesis

The review was a rather complex and extensive task due to the specific topic. The initial observation that we had during the identification of relevant studies is that a large number referred to separate items from our search query, whereas very few covered in entirety the main research question. Some studies focused on interconnection and interdependency between critical infrastructures [26-28], responding to hazards in sectors such as energy grids or water dams [28 - 34], human aspect of evaluating risks and decision making, cyber threat evaluation and contextual awareness [35 - 44], and resilience or investment prioritization [45 - 48]. However only six studies have been identified to match our research question and these have been included in the scope of the SLR. The synthesis of the studies that have been selected for a qualitative analysis are briefly described below.

Choraś et.al. proposes a DSS that uses the approach of describing vulnerabilities based on the ontology logic [21]. The proposed system is focused on general type of risks and the target domain is telecommunications. This type of domain contains a lot of interconnected and heterogeneous networks and the proposed DSS would serve as a network security framework which comprises different tools and techniques for intrusion detection and tolerance.

The next four studies will be reviewed together as these have common authors and relate to the same system. Choraś and Flizikowski propose a cyber-risk focused DSS for the telecommunication, energy and transport domains [22]. The DSS is also ontology based and refers to the classification and relationships of vulnerabilities and threats upon the critical infrastructures. The DSS is designed to support the hardening of SCADA systems against cyber attacks. In another study a similar DSS is proposed, however with a focus on general type of risks with the aim to assess and simulate security in real systems [23]. Kozik et.al. proposed the addition of Bayesian network to the described DSS that is ontology based [25]. According to the author, this would improve the reasoning engine of the DSS and create new reporting such as ranking of threats and their severity. Amantini et.al. refers to the user experience interface of the same DSS and recommends that the users and experts should have IT knowledge, in order to be able to cope with more complex interfaces [20]. The described DSS is concentrating on the dependency modelling and analysis of the critical infrastructure and underlying network. It has a focus on network monitoring, detection and response (peer-to-peer overlay routing, traffic guarantee), as well as proposing an automatic fault detection and recovery architecture for SCADA.

Setola et.al. describes a DSS for emergency situation handling in critical infrastructures. This system would support the operators in the response action and the public authorities in coordination as well as contingency planning [24]. The DSS concept is to use a multitude of data sources and correlate them in order to estimate the potential damages and consequences, which would support in having an informed decision making. We also observed that the study proposes a categorization of potential consequences, such as on citizens, economy or other critical infrastructure and environment. However, the study does not explicitly tackle the cyber attack as threats, nor the impact and consequences from this type of threats.

We note that in several of the reviewed studies the focus of the DSS is not exclusively designed for cyber risk management and can be adapted to various needs and requirements. Even though there are few results that match our search query combination and have tackled our research question, we consider the findings to be valuable and transparently presenting the current status of using DSS for cyber risk management in critical infrastructures.

Conclusions

This review allowed us to better understand the research topic, as well as identify what has been already researched and in which degree.

We have noticed that the studied areas in all papers are dispersed and cover various objectives or research question. We identified a focus on resilience and contextual awareness in several papers, denoting the importance of these factors in the critical infrastructure domain. While this is not necessarily linked to the entire research question that we have tackled in this paper, it does contribute to supporting the importance in having a holistic study on the focus that we have selected.

As a result of the SLR our observations are:

- None of the studies describe a DSS used in practice – all of them describe it at the concept level or propose a prototype
- The concepts and methodologies used within the described DSS vary among ontology, Bayesian networks, interdependency modelling, categorization and correlation
- All studies have certain limitations and were not designed for all type of cyber threats
- We notice a focus on the energy sector with regards to risk management
- Less than half of the studies focus explicitly on certain type of cyber risks
- The majority of the studies that were reviewed were from 2009-2012 period and only one study was relatively recently published in 2017
- The systems described focus on various processes within risk management
- There is an assumption of security experts having both IT and OT knowledge in the field when using the DSS [20]
- Two studies relate on the importance of having cyber security principles applied in the DSS itself [20, 24].

We have identified several areas that do not have extensive coverage as well as future research topics that we believe would support the industry and research domain. The understanding of cyber risks and all the implications upon a critical infrastructure, in combination with the decision support system, would allow the operators and risk managers to make quick and informed responses towards the identified risks. We consider that a DSS focusing explicitly on cyber risks would complement and support the existing research, and is required for sustaining the long-term goals in managing emerging risks. Whereas physical events and damages in critical infrastructures were the focus for years on systems for supporting risk management in the identification, assessment and evaluation of risks, these in our opinion do not cover exhaustively the new nature of risks that the cyberspace brings. Having a DSS explicitly focused on cyber risks and developed in a way that it is seen as a component, would increase the probability to have it adopted by other systems and used in real case scenarios. We believe that such a modular system would complement the risks management processes in domains such as nuclear or healthcare [49-50].

We have also noted, that there is no DSS that takes into account all type of cyber security risks, and only a subset of them. This we believe should be concept of a future developed DSS, which would enhance the process of risk evaluation and prioritization in terms of controlling the risk.

Another result of this study is the identification of the need to build and develop a modular DSS that is easy to integrate in other DSS or risks management processes. The complexity of the identified relevant studies as well as the low number of studies in this field shows that building an entire DSS for all type of risks can be time and resource consuming. We trust that a DSS developed as a module with various interfaces for connection and data sharing would allow it to be efficiently managed, updated and used in various type of domains and systems. We have also noted a focus on the interface importance of a DSS that can be correlated to its efficiency in use by the operators or decision makers, as well as the level of IT knowledge required. We believe the context identification phase would cover the factors required to be taken into account when describing a DSSs.

These results constitute valuable insights into the possibility to use DSS for cyber risk management in critical infrastructures. This validates and confirms the actuality of the selected research question. This study has also provided us trustworthy data in understanding the current state as well as how to advance the study in the main research question from this SLR.

The knowledge gained has allowed us to identify the gaps as well as serve as the baseline for the future research agenda in this domain. These results will be supported by the identified factors for a DSS that we have identified in the previous study. We believe the dissemination of these results will be beneficial for the researchers focusing in this domain.

References

1. European Commission. *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism /* COM/2004/0702 final */.* 2004. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52004DC0702&from=EN
2. CISA - Cybersecurity and Infrastructure Security Agency. *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism /* COM/2004/0702 final */,* 2020. Available at: https://www.cisa.gov/critical-infrastructure-sectors
3. Government of Canada. *National strategy for critical infrastructure,* 2020. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf
4. ISO - International Organization for Standardization. *ISO GUIDE 73:2009 Risk management — Vocabulary*, 2009. Available at: https://www.iso.org/standard/44651.html
5. Rose, A, et al. *"Benefit-cost analysis of FEMA hazard mitigation grants."* Natural hazards review 8.4 (2007): 97-111.
6. Hemsley K., Fisher R. *History of Industrial Control System Cyber Incidents, Idaho National Laboratory*, 2018. Available at: https://www.osti.gov/servlets/purl/1505628
7. National Infrastructure Advisory Council, *Securing cyber assets – Addressing Urgent Cyber Threats to Critical Infrastructure*, 2017. Available at: https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf
8. Department of Defense, *Report of Defense Science Board Task Force on Cyber Deterrence, 2017.* Available at: https://fas.org/irp/agency/dod/dsb/cyber-deter.pdf
9. National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations, NIST Special Publication 800-37*, 2018, https://doi.org/10.6028/NIST.SP.800-37r2
10. Filip F. G. *Decision support and control for large-scale complex systems*, Annual Reviews in Control 32(1): 61–70., 2008, https://doi.org/10.1016/j.arcontrol.2008.03.002
11. Geertman S., Stillwell J. *Planning Support Systems: An Introduction*. In: Geertman S., Stillwell J. (eds) Planning Support Systems in Practice. Advances in Spatial Science. Springer, Berlin, Heidelberg, 2003.
12. Hedwig van Delden, Patrick Luja, Guy Engelen, *Integration of multi-scale dynamic spatial models of socio-economic and physical processes for river basin management*, Environmental Modelling & Software,Volume 22, Issue 2, 2007,Pages 223-238,ISSN 1364-8152, https://doi.org/10.1016/j.envsoft.2005.07.019.
13. Filip F. G., Suduc A.-M. & Bîzoi M. *DSS in numbers. Technological and Economic Development of Economy*, 20(1), 154-164, 2014, https://doi.org/10.3846/20294913.2014.890139
14. Filip F.G., *DSS—A Class of Evolving Information Systems*. In: Dzemyda G., Bernatavičienė J., Kacprzyk J. (eds) Data Science: New Issues, Challenges and Applications. Studies in Computational Intelligence, vol 869. Springer, Cham, 2020

15. Kitchenham B., Stuart C. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. 2007, Vol. 2.
16. Kitchenham B. et al., *Systematic literature reviews in software engineering – A systematic literature review*, Information and Software Technology, Volume 51, Issue 1, 2009, Pages 7-15, https://doi.org/10.1016/j.infsof.2008.09.009
17. Association for Computing Machinery (ACM), Available at: https://www.acm.org/
18. Science Direct, Available at: https://www.sciencedirect.com/
19. Springer, Available at: https://www.springer.com
20. Amantini A., Choraś M., D'Antonio,S., Egozcue E., Germanus D., & Hutter R. *The human role in tools for improving robustness and resilience of critical infrastructures*. Cognition, Technology and Work, 14(2), 143–155, 2012, https://doi.org/10.1007/s10111-010-0171-2
21. Choraś M., Kozik R., Flizikowski A., Renk R., & Hołubowicz W. *Ontology-based decision support for security management in heterogeneous networks*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, 5755 LNAI, 920–927. https://doi.org/10.1007/978-3-642-04020-7_99
22. Choraś M., Flizikowski A., Kozik R., & Hołubowicz W. *Decision aid tool and ontology-based reasoning for critical infrastructure vulnerabilities and threats analysis*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2010, 6027 LNCS, 98–110. https://doi.org/10.1007/978-3-642-14379-3_9
23. Choraś M., Kozik R., Flizikowski A., & Hołubowicz W. *Ontology applied in decision support system for critical infrastructures protection*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2010, 6096 LNAI (PART 1), 671–680. https://doi.org/10.1007/978-3-642-13022-9_67
24. Setola, R., Luiijf, E., & Theocharidou, M., *Managing the Complexity of Critical Infrastructures*. In Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach (Vol. 90, Issue Ci)., 2017, https://doi.org/10.1007/978-3-319-51043-9
25. Kozik R., Choraś, M., & Hołubowicz W. *Fusion of Bayesian and ontology approach applied to decision support system for Critical Infrastructures protection*. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, 45 LNICST, 451–463. https://doi.org/10.1007/978-3-642-16644-0_39
26. Dudenhoeffer D. D., Permann M. R., Woolsey S. Timpany R., Miller C. McDermott A., & Manic M. *Interdependency modeling and emergency response*. Summer Computer Simulation Conference, 2007, SCSC'07, Part of the 2007 Summer Simulation Multiconference, SummerSim'07, 2, 1230–1237.
27. Satumtira G., & Dueñas-Osorio L. *Synthesis of modeling and simulation methods on critical infrastructure interdependencies research*. Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering, 1–51, 2010, https://doi.org/10.1007/978-3-642-11405-2_1
28. C. Koduah S. T., & Prasad R. *The Threats of Infrastructure Obsolescence to Smart Grid: A case study*. 2020. https://doi.org/10.1007/s11277-020-07406-y
29. Panguluri S., Phillips W., & Cusimano J.,*Protecting water and wastewater infrastructure from cyber attacks*. Frontiers of Earth Science, 2011, *5*(4), 406–413. https://doi.org/10.1007/s11707-011-0199-5
30. Di Cristo C., Leopardi A., & de Marinis G. *Water infrastructure protection against intentional attacks: An experience in Italy*. Frontiers of Earth Science, 2011, *5*(4), 390–399. https://doi.org/10.1007/s11707-011-0208-8
31. Kongar I., Esposito S., & Giovinazzi S. *Post-earthquake assessment and management for infrastructure systems: learning from the Canterbury (New Zealand) and L'Aquila (Italy) earthquakes*. Bulletin of Earthquake Engineering, *2017, 15*(2), 589–620. https://doi.org/10.1007/s10518-015-9761-y
32. Enescu F. M., & Bizon N. *SCADA applications for electric power system*. In Power Systems. 2017, https://doi.org/10.1007/978-3-319-51118-4_15
33. Kureshi, I., Mangina, E., O'Hare, G., & Roche, J., *Towards an info-symbiotic decision support system for disaster risk management*. Proceedings - 2015 IEEE/ACM 19th International Symposium on Distributed Simulation and Real Time Applications*, DS-RT 2015*, 85–91. https://doi.org/10.1109/DS-RT.2015.26
34. Vamvakeridou-Lyroudia, L. S., Chen, A. S., Khoury, M., Gibson, M. J., Kostaridis, A., Stewart, D., Wood, M., Djordjevic, S., & Savic, D. A., *Assessing and visualizing hazard impacts to enhance the resilience of Critical Infrastructures to urban flooding*. Science of the Total Environment, 2020, 707, 136078, https://doi.org/10.1016/j.scitotenv.2019.136078

35. Tsai F. S., & Chan K. L. *Blog data mining for cyber security threats*. Data Mining for Business Applications, 2009, 169–182. https://doi.org/10.1007/978-0-387-79420-4_12
36. Sa C., & Hutchison D. *Theory and Models for Cyber Situation Awareness State-of-the-Art*. 2917, Vol 4, 3–25. https://doi.org/10.1007/978-3-319-61152-5
37. Khelil A., Germanus,D., & Suri N. *Protection of SCADA communication channels*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*)*, 2012, *7130*, 177–196. https://doi.org/10.1007/978-3-642-28920-0_9
38. Formicola V., Di Pietro A., Alsubaie A., Marti J., & D'Antonio S. *Assessing the impact of cyber attacks on wireless sensor nodes that monitor interdependent physical systems.* IFIP Advances in Information and Communication Technology, 2014. *441*, 213–229.
39. El-Alfy E. S. M. & Al-Obeidat F. N. *A multicriterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection*. Procedia Computer Science*,* 2014, 34*,* 55–62. https://doi.org/10.1016/j.procs.2014.07.037
40. Wagner N., Lippmann R., Winterrose M., Riordan J., Yu T., & Streilein W. W. *Agent-based simulation for assessing network security risk due to unauthorized hardware*. Simulation Series, *2015,* 47(1), 18–26.
41. Zarreh A., Wan H., Lee Y., Saygin C., & Janahi R. Al. *Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach*. Procedia Manufacturing, 38,2019, 605–612. https://doi.org/10.1016/j.promfg.2020.01.077
42. Motzek A., & Möller R. *Context- and bias-free probabilistic mission impact assessment*. Computers and Security, 2017, 65, 166–186. https://doi.org/10.1016/j.cose.2016.11.005
43. Fujita H., Gaeta A., Loia V., & Orciuoli F. *Improving awareness in early stages of security analysis: A zone partition method based on GrC*. Applied Intelligence, 2019, 49(3), 1063–1077. https://doi.org/10.1007/s10489-018-1315-y
44. De Maggio, M. C., Mastrapasqua, M., Tesei, M., Chittaro, A., & Setola, R., *How to Improve the Security Awareness in Complex Organizations*. European Journal for Security Research, 2019, 4(1), 33–49. https://doi.org/10.1007/s41125-017-0028-2
45. Uddin S., Routray J. K., & Warnitchai P. *Systems Thinking Approach for Resilient Critical Infrastructures in Urban Disaster Management and Sustainable Development*. In Resilient Structures and Infrastructure. Springer Singapore, 2019, https://doi.org/10.1007/978-981-13-7446-3
46. Stavroulakis P., Kolisnyk M., Kharchenko V., Doukas N., Markovskyi O. P., & Bardis N. G. *Reliability, fault tolerance and other critical components for survivability in information warfare*. In Communications in Computer and Information Science (Vol. 990), 2019, Springer International Publishing. https://doi.org/10.1007/978-3-030-11039-0_17
47. Häckel B., Hänsch F., Hertel M., & Übelhör, J. *Assessing IT availability risks in smart factory networks*. Business Research, 2019, 12(2), 523–558. https://doi.org/10.1007/s40685-018-0071-5
48. Hickford A. J., Blainey S. P., Ortega Hortelano A., & Pant, R. *Resilience engineering: theory and practice in interdependent infrastructure systems*. Environment Systems and Decisions, 2018, 38(3), 278–291. https://doi.org/10.1007/s10669-018-9707-4
49. Buzdugan A., Buzdugan A. *The Synergy Between Cyber and Nuclear Security. Case Study of Moldova*. In: Sidorenko A., Hahn H. (eds) Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, 2020
50. Buzdugan A. *Integration of Cyber Security in Healthcare Equipment*. In: Tiginyanu I., Sontea V., Railean S. (eds) 4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019, IFMBE Proceedings, vol 77, pp 681-684, Springer Nature Switzerland AG 2020, https://doi.org/10.1007/978-3-030-31866-6_120