INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 3, PP. 1-9
Manuscript received August 12, 2024; revised June, 2026. doi: 10.24425/ijet.2026.1713

# Application of cognitive and cyber modelling for cybersecurity risk management in Automated Process Control Systems

Valerii Lakhno, Dmytro Kasatkin, Hennadii Mohylnyi, Alona Desiatko, Tetiana Zhyrova, Karyna Khorolska, and Nataliia Kotenko

***Abstract*—The growing number of cyber attacks in the world emphasises the importance of protecting critical computer systems (CCS), including automated process control systems (APCS). Ensuring the cybersecurity of CCSs becomes an essential element of resilience and reliability of modern information technologies. This paper considers the possibility of applying cognitive and cybernetic modelling and investigates the concepts that affect the cybersecurity risks of APCS. The methods of cognitive and cybernetic modelling made it possible to identify the links between the considered concepts, which made it possible to better understand the dynamics of changes in the system of APCS risk management.**

***Keywords*—cybersecurity; risks; cognitive modelling; concepts; automated control system; technological processes; cybernetic modelling; Python**

## I. Introduction

THE growing number of cyberattacks worldwide highlights the importance of protecting critical computer systems (CCS), including automated process control systems (APCS), which play a key role in managing many manufacturing, economic and other technological processes. In the face of increasingly complex and frequent threats, cyber security (CS) is becoming an essential element of information technology resilience and reliability on a global level. The cybersecurity of an CCS requires the identification of all possible threats that can cause damage to the system, including the APCS. According to studies [1, 2], the CCSs are often targets for cyberattacks because attacks on them can be used to cause economic or political damage. The connectivity of APCS s to corporate networks and the Internet increases their vulnerability to remote attacks, and the use of outdated technology and lack of up-to-date security measures make them even more vulnerable. Many governments and international organisations recognise control systems as mission-critical systems and set strict standards and requirements to ensure their cyber security. According to NIST: Cybersecurity Framework for Critical Infrastructure [3], IEC 62443: International Cybersecurity Standards for Industrial Automation Systems [4], and ISO 27001: Information Security Management Standard Applicable to Process Control Systems [5], risk assessment involves analysing potential attacks, their likelihood and possible consequences. During such an assessment, it is important to identify the most critical vulnerabilities that can lead to serious incidents, which will allow to focus resources on their elimination and risk minimisation. As shown in several works [6, 7, 8], cognitive modelling allows visualising and analysing complex relationships between different system components, threats and protection measures, which simplifies the understanding of complex systems and helps to identify weaknesses in the protection of CCS.

Using cognitive maps and cyber modelling tools, different attack scenarios and their consequences can be visualised, allowing the defence to predict developments and develop incident response strategies for the control system. This includes creating models that integrate data on current threats, vulnerabilities, and protective measures, thereby providing more accurate and responsive solutions for securing the CCS.

## II. Literature review

Note that the idea of using cognitive modelling to solve cybersecurity problems is not a new one. Over the last decade, many studies demonstrating the effectiveness of this approach have been published.

For example, in [9], the authors discuss the application of cognitive models to simulate the behaviour of attackers, defenders and users in cybersecurity scenarios. The work emphasises the use of adversarial reasoning, integration of human factors and dynamic simulations to enhance learning and decision making in cybersecurity.

In [10], a cognitive deception model that generates fake documents to prevent data leakage in networks during cyberattacks is presented. The authors propose to use fake documents to divert attackers' attention and reduce the risk of stealing real data. The model includes strategies for creating plausible fake data that can confuse attackers and improve network security.

In [11], the use of cognitive risk management to mitigate the threat of cyber attacks in smart grids is discussed. The authors propose the integration of cognitive techniques, including machine learning and artificial intelligence, to monitor and

Valerii Lakhno and Dmytro Kasatkin are with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: lva964@nubip.edu.ua, d.kasatkin@nubip.edu.ua)

Hennadii Mohylnyi is Taras Shevchenko National Universit, Ukraine, Kyiv, Ukraine (e-mail: g.mogilniy@gmail.com)

Alona Desiatko, Tetiana Zhyrova, and Nataliia Kotenko are with State University of Trade and Economics, Kyiv, Ukraine (e-mail: desyatko@gmail.com,ev, kryvoruchko@ukr.net, karynakhorolska@gmail.com, i.karpunin@knute.edu.ua )

Karyna Khorolska is with Boris Grinchenko Kyiv Metropolitan University, Ukraine(e-mail: karynakhorolska@gmail.com)

analyse data from the grid. The approach proposed in the paper enables real-time detection of anomalies and potential threats, as well as dynamic response to them, which significantly improves the defence of smart grids against cyberattacks.

In [12], the development of a "kill chain" model for cyberattacks using a cognitive approach is discussed. The authors propose to integrate cognitive techniques and multitasking processes to improve detection and neutralisation of cyberattacks. The model allows for a better understanding and analysis of the stages of cyberattacks, from initial reconnaissance to the final execution of the attack, and the application of appropriate protective measures at each stage to improve cybersecurity.

In [13], the authors discuss the development of effective cloaking strategies for cyber defence. The authors explore methods for creating deceptive strategies using human experiments and cognitive models. The focus of the paper is on how cognitive models can be used to predict and improve human responses to cyberattacks, allowing for the development of more effective methods to protect information systems.

In [14], cognitive models for dynamic decision making in autonomous intelligent cyber defence are discussed. The authors explore how cognitive models can be used to improve real-time decisions in the face of cyberattacks. The focus is on developing models that can adapt to changing threats and conditions, enabling better defence of systems. The research demonstrates how cognitive approaches can improve autonomous cybersecurity systems.

In general, reviewed and other works, e.g. [6-8, 15-17], consider the potential of cognitive modelling to simulate attacker and defender behaviour, analyse insider threats, enhance the realism of training programs and understand interactions in cyber environments.

The main drawback of the reviewed studies is that the authors did not address the issue of extending the potential of cognitive modelling using cybernetic modelling and object-oriented programming languages, which limits the possibilities of deeper and more detailed integration of various modelling aspects and the development of more complex and adaptive cybersecurity systems. Based on the above, the objective of our research was to.

## III. Aims and Objectives of the Study

The aim of the study is to investigate the possibilities of developing cognitive modelling methods using cybernetic models in the algorithmic language Python with a focus on the analysis of the mutual influence of concepts, including weakly structured ones, on the cybersecurity risks of automated process control systems.

Objectives of the study:

1. *Develop and improve cognitive and cybernetic modelling methods that will enable more effective assessment of CCS cybersecurity risks.*
2. *Create and test a cybernetic model in Python to analyse concepts related to cybersecurity risk management in CCS.*

## IV. Methods and Models

To create a scenario of changes in the cybersecurity concepts influence network, inputs include: a list of influencing factors $SI = \{si_i\}$ ; measurements for each factor it's scale(s) $X_{ij}$ ; and the current state of the information security system prior to the potential threat [18].

Thus, we determine what data we need to model and predict the change of the situation, starting from the current state of the system, taking into account the different influencing factors and their measurements.

$$X(t_0) = (x_{11},...,x_{nm}); \tag{1}$$

$$\text{MS } AM = \left|am_{ij\,sl}\right| , \tag{2}$$

Where $i, s$ is the number of the concept; $j, l$ is the number of the attribute of the judgement. For the number of judgements we have, respectively, $i \vee s$

In general, it is necessary to define a set of new factors (or - vector of feature addition - VFA) i.e.

$V(t), V(t+1),..., V(t+n)$ and track the change in the state of the cybersecurity system for the input parameters $X(t), X(t+1),..., X(t+n)$ at the moments of time $t,...,t+n$. To solve this problem, the method of successive iterations was used, during which the VFA was calculated from the following expression:

$$V(t+1) = V(t) \circ AM . \tag{3}$$

Then, the state at time $t+1$ will be characterised by the relation $X(t+1) = X(t) + V(t+1)$. In this case, each adjacency matrix (or AM) $AM = \left|am_{ij\,sl}\right|_{n\times n}$ for the positive and negative components is transformed under the following conditions:

$$\begin{aligned} &if\ am_{ij\,sl} > 0\ \ then\ \ am'_{i(2j-1)s(2l-1)} = \\ &= am_{ij\,sl},\ am'_{i(2j)s(2l)} = am_{ij\,sl}; \\ &if\ am_{ij\,sl} < 0\ \ then\ \ am'_{i(2j-1)s(2l-1)} = \\ &= -am_{ij\,sl},\ am'_{i(2j)s(2l)} = -am_{ij\,sl} \end{aligned} \tag{4}$$

to a positively defined dual matrix $AM' = \left|am'_{ij\,sl}\right|_{2n\times 2n}$ .

In a block matrix - feature addition at times *t*, columns - feature addition at the time that corresponds to the column i.e:

$$V^t = \left|V'(t+1)^T,..., P'(t+n)^T\right|. \tag{5}$$

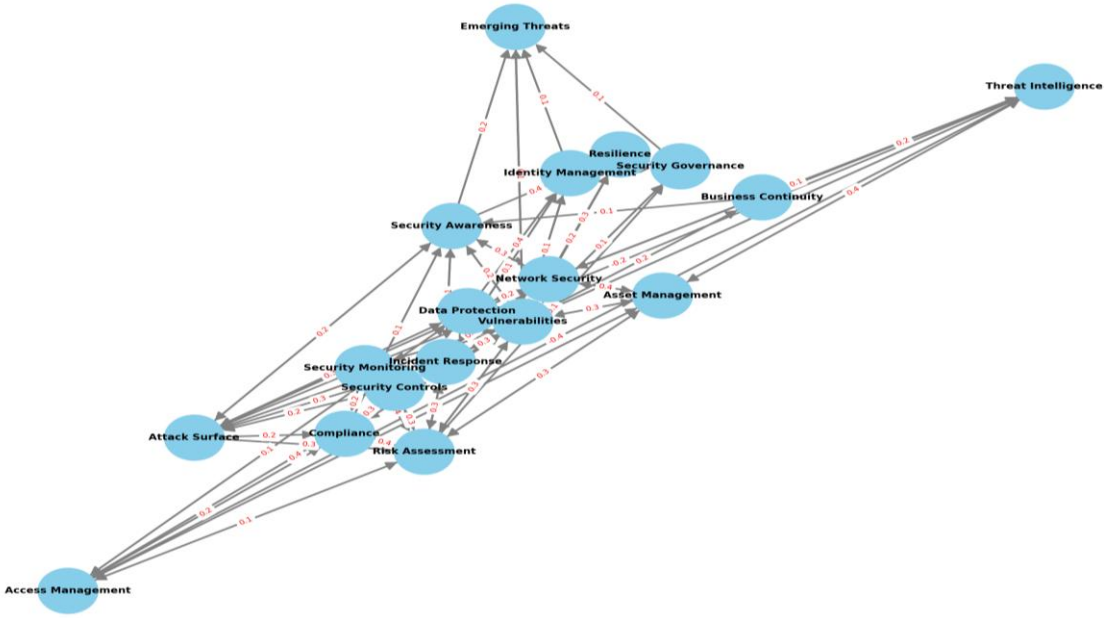
Block Matrix (BM) $V^t$ was used in the developed software product to predict the transformation of the situation of the cybersecurity facility.

As part of the solution to the problem of cognitive risk modelling for the CCS, important components are the adjacency matrix and the block matrix, which represent the interactions between the different elements of the system. The adjacency matrix is a way of describing the structure of a network in which concepts are connected by edges, i.e. interactions, e.g. as shown in Figure 1. The nodes can represent different aspects of the cybersecurity, and the edges can represent their interrelationships and influence on each other. The block matrix

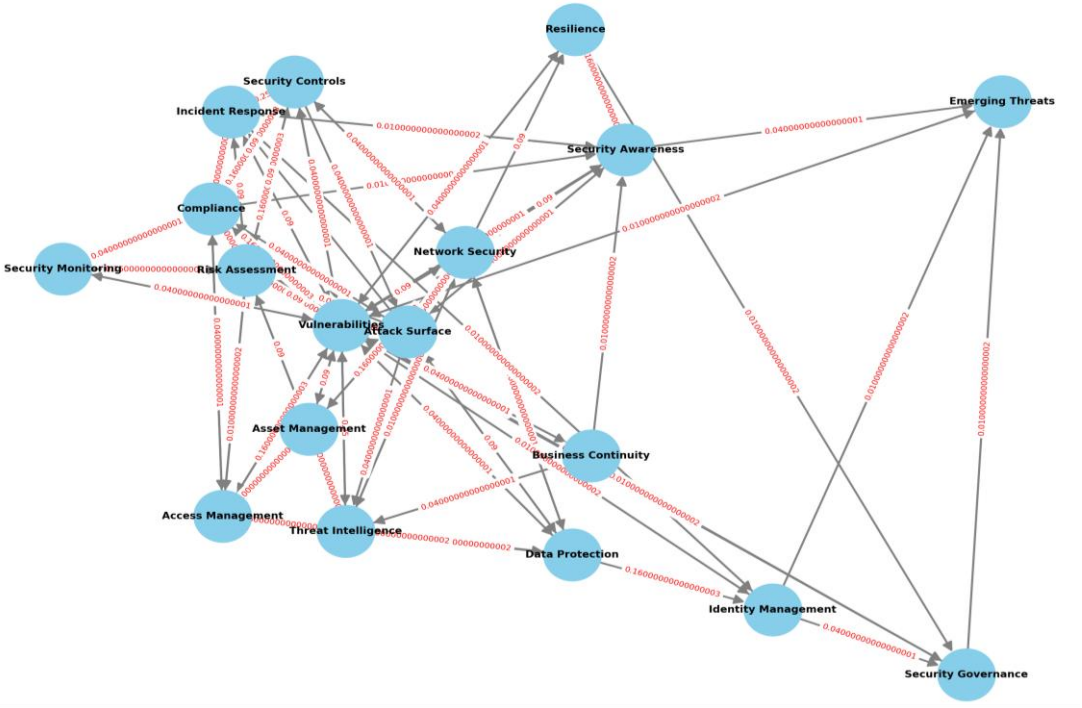
is used for more complex modelling where a system is divided into several subsystems or blocks, each of which is described by its own adjacency matrix. This allows the interaction between subsystems to be modelled and more complex interrelationships to be considered.

Using cognitive modelling techniques, such as iterative computation and simulations, we can analyse the current state and predicted changes in the CCS system based on the introduction of new factors or changes in existing relationships using the developed software product. Based on the results of the analysis, potential risks were assessed and strategies were developed to minimise them.

Eighteen concepts were used for our software model: Vulnerabilities; Threat Intelligence; Attack Surface; Risk Assessment; Security Controls; Incident Response; Compliance; Access Management; Data Protection; Network Security; Security Awareness; Asset Management; Business Continuity; Security Monitoring; Identity Management; Security Governance; Resilience; Emerging Threats, see Figures 1 and 2.




a)




b)

Fig. 1. Examples of a general network of influences for different concepts on ACS cybersecurity risks

## V. Computational Experiment

The computational experiments were aimed at investigating and analysing the mutual influence of different concepts on the risks of CCS's cybersecurity.

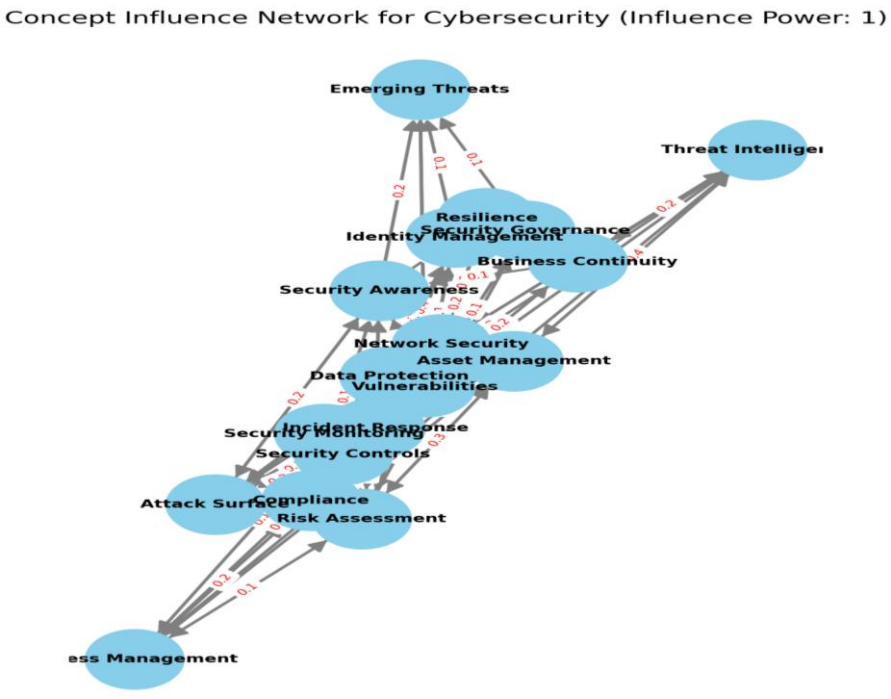
An influence matrix was constructed, see Figure 2, in which each value represents the degree of influence of one concept on another. Positive values indicate positive influence and negative values indicate negative influence. In our examples, a synthetic dataset was used because in most cases, especially in research and preliminary modelling, real data on the impact of different concepts on CCS cybersecurity risks may be either unavailable or limited due to privacy and security of information. The synthetic dataset provided the computational experiments with complete freedom to vary concept values and scenarios, allowing different hypotheses and their implications to be considered, including those that may be difficult or impossible to obtain in real-world settings. In addition, the synthetic data provided a baseline for initial validation of the cognitive model, which reduced the risk of errors and increased the reliability of the model when they were later used in real-world CCS cybersecurity risk analyses.

Using Python cybernetic modelling tools, particularly the NetworkX library, an influence network was constructed to represent the relationships between concepts. The nodes of the network represent the concepts, and the edges represent the extent to which they influence each other. Graphs and histograms were created to visualise the results, see Figs. 3-5.

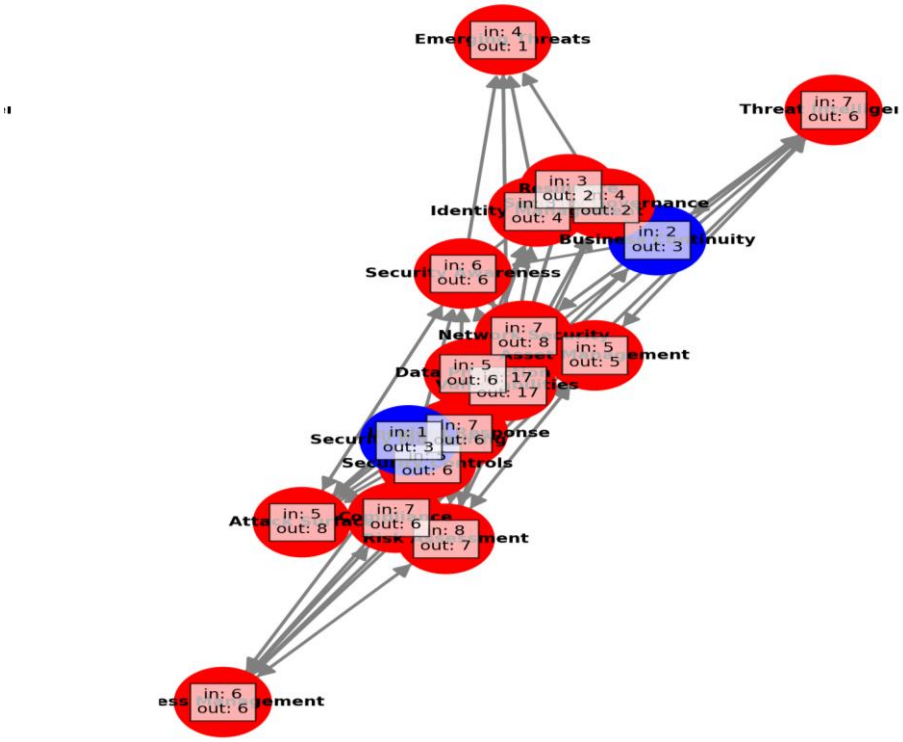
main.py

```python
import networkx as nx
import matplotlib.pyplot as plt
import numpy as np

# Create a graph
G = nx.DiGraph()

# Adding concepts (nodes)
concepts = [
    'Vulnerabilities', 'Threat Intelligence', 'Attack Surface', 'Risk Assessment', 'Security Controls',
    'Incident Response', 'Compliance', 'Access Management',
    'Data Protection', 'Network Security', 'Security Awareness',
    'Asset Management', 'Business Continuity', 'Security Monitoring',
    'Identity Management', 'Security Governance',
    'Resilience', 'Emerging Threats'
]
G.add_nodes_from(concepts)

# Influence matrix with synthetic data
influence_matrix = np.array([
    [0, 0.5, 0.4, 0.2, 0.3, 0.3, 0.4, 0.4, 0.2, 0.3, 0.2, 0.3, 0.2, 0.4, 0.1, 0.1, 0.2, 0.1],  # Impact on Threat Intelligence
    [-0.5, 0, 0, 0, 0, 0, 0, -0.4, 0.1, 0.1, 0, 0.4, 0.2, 0, 0, 0, 0, 0],  # Impact on Attack Surface
    [0.4, -0.2, 0, 0.3, 0, 0.3, 0.2, 0, 0.3, 0.2, 0.2, 0, 0, 0, 0, 0, 0],  # Impact on Risk Assessment
    [0.3, 0, 0, 0, 0.4, 0.5, 0.3, 0.1, 0, 0, 0, 0.3, 0, 0, 0, -0.1, 0, 0],  # Impact on Security Controls
    [0.2, 0, 0.2, 0.3, 0, 0.5, 0.4, 0, 0, 0.2, 0, 0, 0, 0, 0, 0, 0],  # Impact on Incident Response
    [0.3, 0, 0, 0.3, 0.5, 0, 0.2, 0, 0, 0, 0.1, 0, 0, 0, 0.1, 0, 0, 0],  # Impact on Compliance
    [0.4, 0, 0, 0.4, 0.3, 0.2, 0, 0.2, 0, 0, 0.1, 0, 0, 0, 0, 0, 0, 0],  # Impact on Access Management
    [0.4, -0.4, 0, 0.1, 0, 0, 0.2, 0, 0.1, 0, 0, 0.1, 0, 0, 0, 0, 0, 0],  # Impact on Data Protection
    [0.2, 0.1, 0.3, 0, 0, 0, 0, 0.1, 0, 0.2, 0, 0, 0, 0, 0.4, 0, 0, 0],  # Impact on Network Security
    [0.3, 0.1, 0.2, 0, 0.2, 0, 0, 0, 0.2, 0, 0.3, 0.4, 0, 0, 0, 0, 0.3, 0],  # Impact on Security Awareness
    [0.2, 0, 0.2, 0, 0, 0.1, 0, 0, 0, 0.3, 0, 0, 0, 0, 0, 0, 0.4, 0.2],  # Impact on Asset Management
    [0.3, 0.4, 0, 0.3, 0, 0, 0, 0.1, 0, 0.4, 0, 0, 0, 0, 0, 0, 0, 0],  # Impact on Business Continuity
    [0.2, 0.2, 0, 0, 0, 0, 0, 0, 0, 0, 0.1, 0, 0, 0, 0, 0, 0, 0],# Impact on Security Monitoring
    [0.2, 0, 0, 0.4, 0, 0, 0.2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],  # Impact ona Identity Management
    [0.1, 0, 0, 0, 0, 0.1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.2, 0, 0.1], # Impact on Security Governance
    [0.1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.1], # Impact on Ha Resilience
    [0.2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.1, 0, 0], # Impact on Emerging Threats
    [0.1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
     ])

# Add edges based on influence
for i, concept in enumerate(concepts):
    for j, influence in enumerate(influence_matrix[i]):
        if influence != 0:
```

Fig. 2. An example of a concept influence matrix

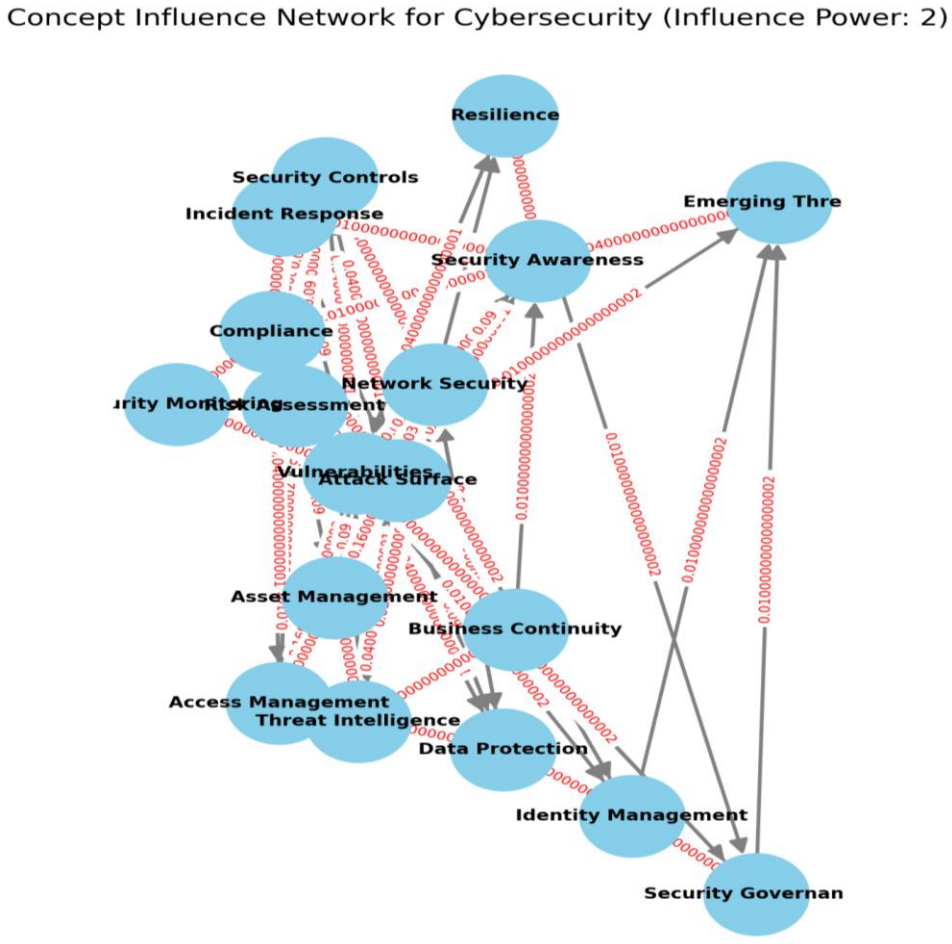



a)

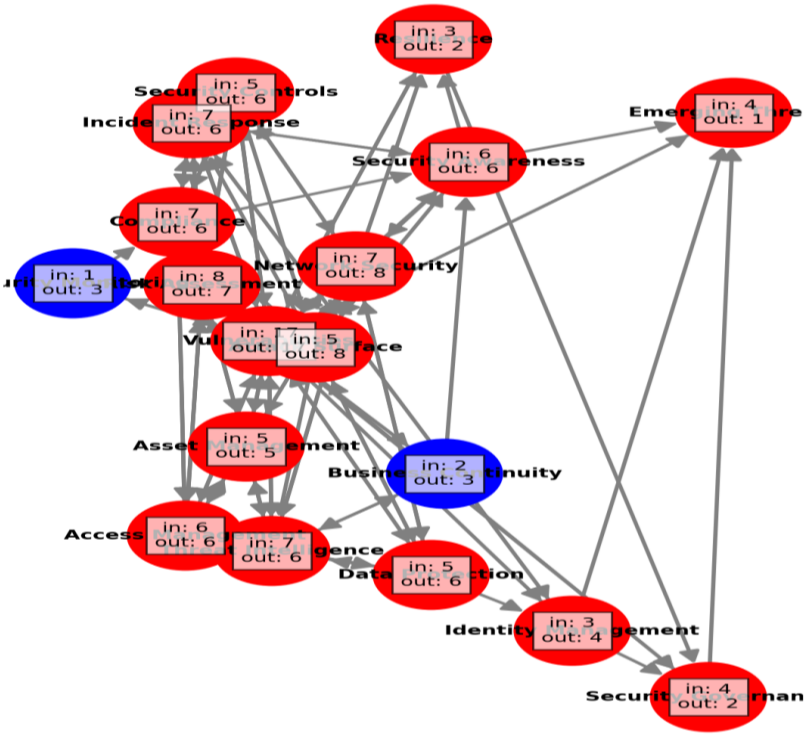



b)

Fig. 3. Results of the computational experiment

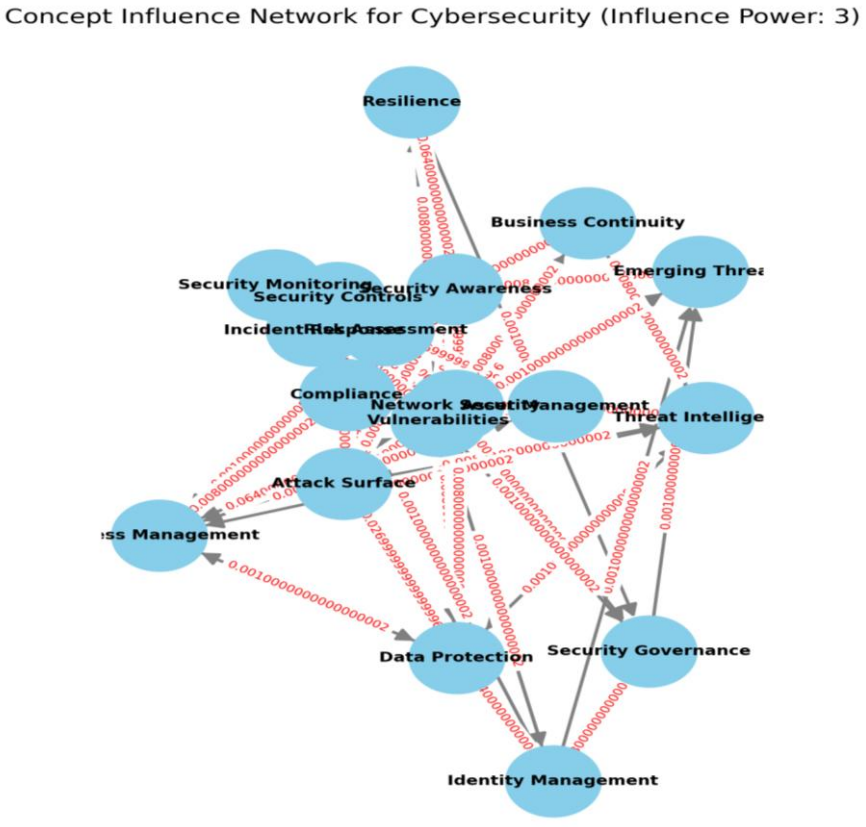



a)

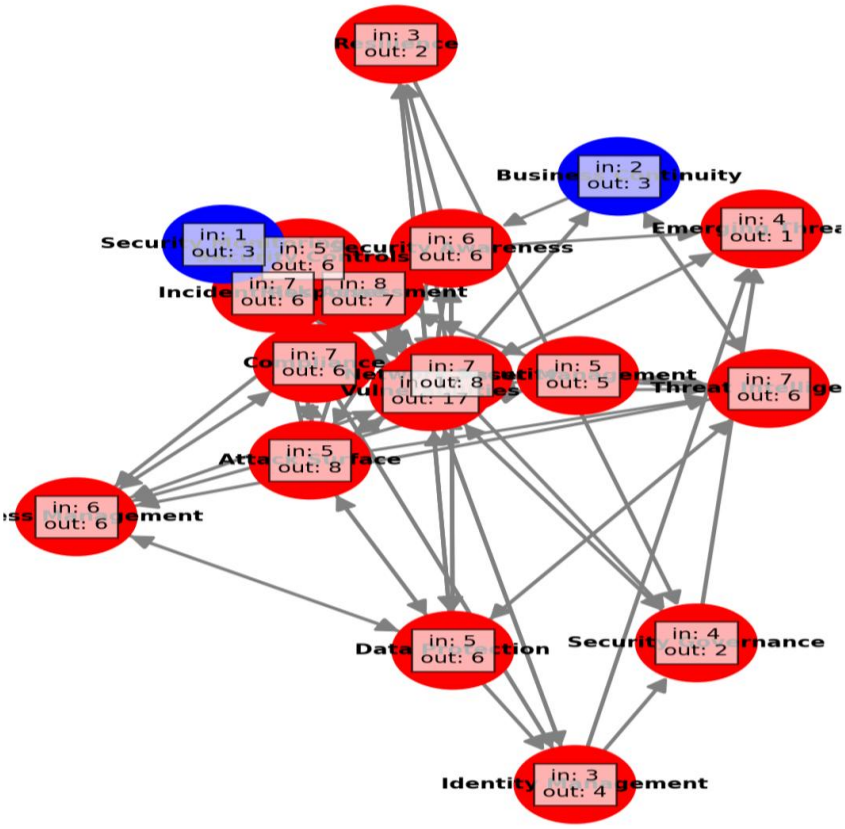



b)

Fig. 4. Results of the computational experiment




a)




b)

Fig. 5. Results of the computational experiment

The graphs a), see Fig. 3-5 show general network of influences, where concepts are connected by interactions. In our case, the nodes (concepts) represent different aspects of the influence of different indicators, e.g. "Vulnerabilities", "Incident Response", on the risks for the CCS. The numerical values above the edges show the degree of influence of one concept on the other. The blue nodes in these graphs (shown on the left side of the images) show the concepts that participate in the overall network of influences, which allows you to visually assess their interrelationships and understand how changes in one concept can affect others.

The graphs b) show histograms that visualise the degrees of influence of different concepts. The blue colour shows the concepts displaying positive influence. And in red colour, respectively, the negative influence. For example, "Threat Intelligence" may have a high blue bar indicating a strong positive influence on "Risk Assessment". And, "Attack Surface" may have a high red bar indicating a strong negative impact on Risk Assessment.

Thus, the a) graphs help experts to better understand how all concepts are related in the system and how they can influence each other. At the same time, the b) graphs with histograms help to further understand which concepts have a positive or negative impact on each specific concept. This format of presenting the results will allow for a comprehensive analysis of the cybersecurity system and allow for the identification of key risk factors and the development of effective strategies to manage them.

These results were obtained through the use of cybernetic modelling tools in Python, which provided flexibility and powerful analysis capabilities. Software libraries such as NetworkX for graph creation and visualisation, and Matplotlib for histograms, provided effective tools for modelling and analysing the relationships between concepts during cognitive risk modelling for CCS. Note that, in general, the use of Python for such tasks allows for the automation of the modelling and analysis process, which significantly improves the accuracy and efficiency of cybersecurity decisions. The research is currently ongoing.

## CONCLUSION

In this paper, we investigated various concepts that influence cybersecurity risks of automated process control systems (APCS). Using cognitive modelling techniques and cyber modelling tools in the algorithmic language Python, different variants of influence networks and histograms were constructed to visualise the mutual influence of concepts. The analysis showed that such concepts as "Vulnerabilities" and "Incident Response" play a key role in the overall risk system of the CCS. The conducted computational experiments and influence network models made it possible to identify both positive and negative links between the considered concepts, which made it

possible to better understand the dynamics of changes in the risk management system of the CCS.

The results obtained provide valuable information for the development of effective risk management strategies in the CCS. Thus, the application of cognitive and cybernetic modelling methods for the analysis of cybersecurity risks in the CCS has shown its effectiveness, allowing a comprehensive assessment and management of key risk factors.

## REFERENCES


[1] .Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946.

[2] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. computers & security, 89, 101677.

[3] Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018, 7.

[4] Djebbar, F., & Nordström, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access, 11, 85315-85332.

[5] Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219-238.

[6] Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. Journal of Information Security and Applications, 48, 102352.

[7] Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information Security Risk Management using Cognitive Modeling. In CEUR Workshop Proceedings (pp. 297-305).

[8] Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modelling. Journal of Open Innovation: Technology, Market, and Complexity, 8(2), 80.

[9] Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modelling of network attackers, defenders, and users. Frontiers in psychology, 9, 324295.

[10] Taofeek, O. T., Alawida, M., Alabdulatif, A., Omolara, A. E., & Abiodun, O. I. (2022). A cognitive deception model for generating fake documents to curb data exfiltration in networks during cyber-attacks. IEEE Access, 10, 41457-41476.

[11] Oozeer, M. I., & Haykin, S. (2019). Cognitive risk control for mitigating cyber-attacks in smart grid. IEEE Access, 7, 125806-125826.

[12] Khan, M. S., Siddiqui, S., & Ferens, K. (2018). A cognitive and concurrent cyber kill chain model. Computer and Network Security Essentials, 585-602.

[13] Aggarwal, P., Thakoor, O., Jabbari, S., Cranford, E. A., Lebiere, C., Tambe, M., & Gonzalez, C. (2022). Designing effective masking strategies for cyberdefence through human experimentation and cognitive models. Computers & Security, 117, 102671.

[14] Prébot, B., Du, Y., Xi, X., & Gonzalez, C. (2022). Cognitive models of dynamic decision making in autonomous intelligent cyber defence. In International Conference on Autonomous Intelligent Cyber-defence Agents, Bordeaux, France.

[15] Jones, R. M., O'Grady, R., Nicholson, D., Hoffman, R., Bunch, L., Bradshaw, J., & Bolton, A. (2015). Modeling and integrating cognitive agents within the emerging cyber domain. In Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) (Vol. 20). Pennsylvania State University.

[16] Oltramari, A., Ben-Asher, N., Cranor, L., Bauer, L., & Christin, N. (2014, October). General requirements of a hybrid-modelling framework for cyber security. In 2014 IEEE Military Communications Conference (pp. 129-135). IEEE.

[17] Shinde, A., & Doshi, P. (2024, May). Modelling Cognitive Biases in Decision-Theoretic Planning for Active Cyber Deception. In Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems (pp. 1718-1726).

[18] Akhmetov B., Lakhno V., Boiko Y., Mishchenko A.. Designing a decision support system for the weakly formalised problems in the provision of cybersecurity, (2017) Eastern-European Journal of Enterprise Technologies, 1 (2-85), pp. 4 - 15.