Enhancing the factor analysis of information risk methodology for assessing cyberresilience in critical infrastructure information systems

Volodymyr Shypovskyi [*] [A]

*__Corresponding author:__ PhD student, e-mail: vladimir.shipovsky@gmail.com, ORCID: 0000-0003-3743-3064

[A] National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

Received: March 2, 2023 | Revised: March 20, 2023 | Accepted: March 31, 2023

DOI: 10.5281/zenodo.7876556

Abstract

Purpose: is to explore the Factor Analysis of Information Risk methodology as a tool for assessing and managing information risk in critical infrastructure systems, and to identify opportunities for improvement in the methodology. The article also provides an overview of other frameworks and standards that can be used in conjunction with the Factor Analysis of Information Risk methodology to enhance the overall effectiveness of risk management in critical infrastructure systems.

Method: factor analysis and empirical research methods were used in the study.

Theoretical implications: involve potential improvements to the Factor Analysis of Information Risk methodology, contributing to a more comprehensive framework for information risk management in critical infrastructure systems.

Practical consequences: involve the potential for improved risk assessments and risk management in critical infrastructure systems through the refinement and development of the Factor Analysis of Information Risk methodology; by identifying gaps and opportunities for improvement in the methodology and providing an overview of other frameworks and standards that can be used in conjunction with Factor Analysis of Information Risk, this article can inform the development of more effective risk management policies and practices; the article may also encourage the use of Factor Analysis of Information Risk and other frameworks and standards in critical infrastructure systems to enhance their security and resilience against potential cyber threats.

Key words: cyberresilience, critical infrastructure, information systems, factor analysis.

Introduction

Information systems are a critical component of modern infrastructure, providing essential services in areas such as energy, transportation, finance, and healthcare. As these systems become increasingly interconnected and dependent on technology, the risks and vulnerabilities associated with their operation and management also increase. Therefore, it is essential to assess and manage the risks associated with information systems of critical infrastructure in order to ensure their continued reliability, availability, and resilience.

The Factor Analysis of Information Risk methodology is a widely used approach to information risk assessment, providing a structured and quantitative method for evaluating and prioritizing information risks. While the factor analysis of information risk (FAIR) methodology has many benefits, it is not without limitations, particularly when applied to critical infrastructure assessment. Therefore, the purpose of this research is to identify opportunities for improving the FAIR methodology for information systems of critical infrastructure assessment.

In this article, presented the results of research into the FAIR methodology and its application to critical infrastructure assessment. We review the existing literature on the FAIR

methodology and other risk assessment frameworks, identify gaps and opportunities for improvement, and propose modifications to the FAIR methodology to better address the unique risks and challenges of critical infrastructure assessment. We also present the results of our validation study, demonstrating the effectiveness and potential of the modified FAIR methodology for information systems of critical infrastructure assessment.

Overall, this research contributes to the development of more effective and comprehensive methods for information risk assessment in critical infrastructure. By improving the FAIR methodology and addressing its limitations in this context, we aim to better protect and secure the information systems that are essential to the functioning of modern society.

Results and Discussion

2.1 Overview of methodologies for information systems assessment

The assessment of information systems used in critical infrastructure is a critical process for ensuring the security and resilience of the systems that underpin our modern society. As critical infrastructure becomes increasingly dependent on information technology, the risks and threats to these systems have also grown, and the need for effective risk assessment and management has become paramount. The assessment of information systems used in critical infrastructure involves evaluating the potential risks to these systems, as well as identifying and prioritizing the measures that can be taken to mitigate those risks.

The assessment of information systems used in critical infrastructure is an important and complex task, and as a result, there are a variety of methodologies and frameworks that have been developed for this purpose. Here are most popular of them:

1. NIST Cybersecurity Framework: The National Institute of Standards and Technology developed a cybersecurity framework that provides a common language, a set of standards and best practices for assessing and improving the cybersecurity posture of critical infrastructure information systems [1]. The NIST Cybersecurity Framework is a widely used and respected set of guidelines for assessing and improving the cybersecurity posture of critical infrastructure information systems. Developed by the National Institute of Standards and Technology (NIST), the framework provides a common language and a set of standards and best practices for organizations to use in managing and reducing cybersecurity risks to their systems. The framework was first released in 2014 and has since been updated to reflect changes in the threat landscape and advances in cybersecurity practices. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a structured approach for organizations to assess their cybersecurity risks, implement appropriate safeguards, detect and respond to cyber incidents, and recover from any disruptions or damages. The Identify function is designed to help organizations understand their cybersecurity risks and the assets, systems, and data that need to be protected. The Protect function provides guidance on implementing appropriate safeguards, such as access controls, encryption, and physical security, to mitigate those risks. The Detect function focuses on identifying and monitoring cybersecurity events and incidents, while the Respond function provides guidance on responding to and recovering from those incidents. The Recover function is designed to help organizations restore their systems and data to their previous state following a cyber incident. This includes developing and testing a recovery plan, as well as conducting an after-action review to identify areas for improvement. The NIST Cybersecurity Framework has been widely adopted by organizations across a variety of industries and sectors, including critical infrastructure [2]. The framework provides a flexible and scalable approach to cybersecurity risk management that can be adapted to the specific needs and requirements of different organizations. In addition, the framework is regularly updated to reflect changes in the threat landscape and to incorporate

feedback from stakeholders. Overall, the NIST Cybersecurity Framework is a valuable tool for organizations to use in assessing and improving their cybersecurity posture. By adopting the framework, organizations can better understand their cybersecurity risks, implement appropriate safeguards, and detect and respond to cyber incidents in a timely and effective manner.

2. ISO/IEC 27001: This is an international standard that provides a systematic approach for managing and protecting sensitive information. It provides a framework for assessing and improving the security of information systems used in critical infrastructure. The standard provides a framework for implementing and maintaining an information security management system (ISMS) within an organization. An ISMS is a set of policies, procedures, and controls that are used to manage information security risks and protect sensitive information from unauthorized access, disclosure, alteration, or destruction. The standard covers a wide range of areas related to information security, including risk assessment and management, security controls, asset management, access control, incident management [3]. ISO/IEC 27001 can be applied to any type of organization, regardless of size, sector, or geographical location. The standard provides a flexible and adaptable framework that can be customized to meet the specific needs and requirements of each organization. For critical infrastructure organizations, the standard provides a comprehensive approach to assessing and improving the security of their information systems. It helps organizations to identify and manage their information security risks, and to implement appropriate safeguards to protect against cyber threats and other security incidents. By implementing the standard, organizations can demonstrate to stakeholders, customers, and regulators that they have implemented a robust and effective information security management system [4]. ISO/IEC 27001 is widely recognized as a best practice for information security management, and is often used by organizations as a benchmark for their own information security practices. The standard is also regularly updated to reflect changes in the threat landscape and advances in information security practices. Overall, ISO/IEC 27001 is a valuable tool for organizations to use in managing and protecting sensitive information. By adopting the standard, organizations can implement a systematic and comprehensive approach to information security management, and ensure the confidentiality, integrity, and availability of their information.

3. ISA/IEC 62443: This is a series of standards developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) for securing industrial automation and control systems (IACS). It provides a comprehensive methodology for assessing and mitigating risks to IACS in critical infrastructure [5]. The ISA/IEC 62443 series is designed to address the unique security challenges of IACS, which include legacy systems, proprietary protocols, and real-time response requirements. The series provides a risk-based approach to security that includes a comprehensive methodology for assessing and mitigating risks to IACS.

The series is divided into four main parts:

Part 1: Terminology, concepts, and models;

Part 2: Establishing an IACS security program;

Part 3: System security requirements and security levels;

Part 4: Secure product development lifecycle requirements [6].

The standards in the series provide a holistic approach to IACS security, covering everything from risk assessment and management to secure product development and deployment. The series also includes guidelines for compliance and certification. The ISA/IEC 62443 series is widely recognized as a best practice for securing IACS in critical infrastructure. It is used by organizations around the world to assess and improve the security of their IACS, and to ensure the safety and reliability of critical infrastructure systems [7]. Overall, the ISA/IEC 62443 series provides a comprehensive methodology for assessing and mitigating risks to IACS in critical infrastructure. It is a valuable tool for organizations to use in securing their IACS and ensuring the safety and reliability of critical infrastructure systems.

4. DHS CSET: The Department of Homeland Security (DHS) developed the Cyber Security Evaluation Tool (CSET), which is a self-assessment tool designed to help organizations assess and improve their cybersecurity posture. It includes specific modules for assessing information systems used in critical infrastructure. CSET includes a variety of modules that cover different aspects of cybersecurity, including network security, system and application security, and incident response planning. These modules allow organizations to evaluate their security practices and identify potential vulnerabilities or weaknesses in their systems. The tool also includes a comprehensive set of best practices and guidelines for improving cybersecurity. One of the key features of CSET is its support for critical infrastructure security. CSET includes specialized modules that are designed to evaluate the security of information systems used in critical infrastructure sectors, such as energy, water, and transportation. These modules are tailored to the unique security requirements of critical infrastructure systems and can help organizations identify potential security gaps and weaknesses in these systems. CSET has been widely adopted by organizations in both the public and private sectors. It has been used by federal agencies, state and local governments, and private sector organizations to improve their cybersecurity posture and comply with regulatory requirements. CSET is regularly updated to reflect changes in the cybersecurity landscape and to incorporate new best practices and guidelines. Overall, CSET is a valuable tool for organizations looking to assess and improve their cybersecurity posture, especially in the critical infrastructure sectors. Its comprehensive modules, best practices, and tailored approach make it a useful resource for organizations of all sizes and industries.

5. FAIR: The Factor Analysis of Information Risk methodology provides a quantitative framework for analyzing and managing information risk. It can be applied to information systems used in critical infrastructure to assess the potential impact of various threats and vulnerabilities [8]. The Factor Analysis of Information Risk methodology is a quantitative risk assessment framework that enables organizations to measure and manage information risk based on factors such as loss event frequency, probable loss magnitude, and threat event frequency. The methodology has been widely adopted in various industries, including healthcare, financial services, and critical infrastructure. In the context of critical infrastructure, the FAIR methodology can be used to assess the potential impact of various threats and vulnerabilities on information systems [9]. For instance, the US Department of Homeland Security (DHS) has used the FAIR methodology to assess the cybersecurity risk of the industrial control systems (ICS) used in critical infrastructure sectors such as energy, water, and transportation. However, despite its advantages, the FAIR methodology has also been criticized for certain limitations [10]. For example, it has been argued that the methodology may not adequately account for human factors, such as employee behavior and social engineering attacks, which can significantly impact the risk posture of an organization's information systems.

There are many other methodologies and frameworks that may be used to assess information systems in critical infrastructure, and the choice of methodology will depend on the

specific needs and requirements of the organization conducting the assessment. But, taking into account the properties of the mentioned methods, for a more advanced study we will choose The Factor Analysis of Information Risk methodology. Because, in my opinion, this technique is most suitable for information systems of critical infrastructure objects

2.2 The Factor Analysis of Information Risk methodology

The Factor Analysis of Information Risk methodology is a quantitative risk assessment framework that has gained popularity in recent years for assessing information systems used in critical infrastructure. Our study focused on identifying gaps and opportunities for improvement in the FAIR methodology when applied to critical infrastructure assessment [11].

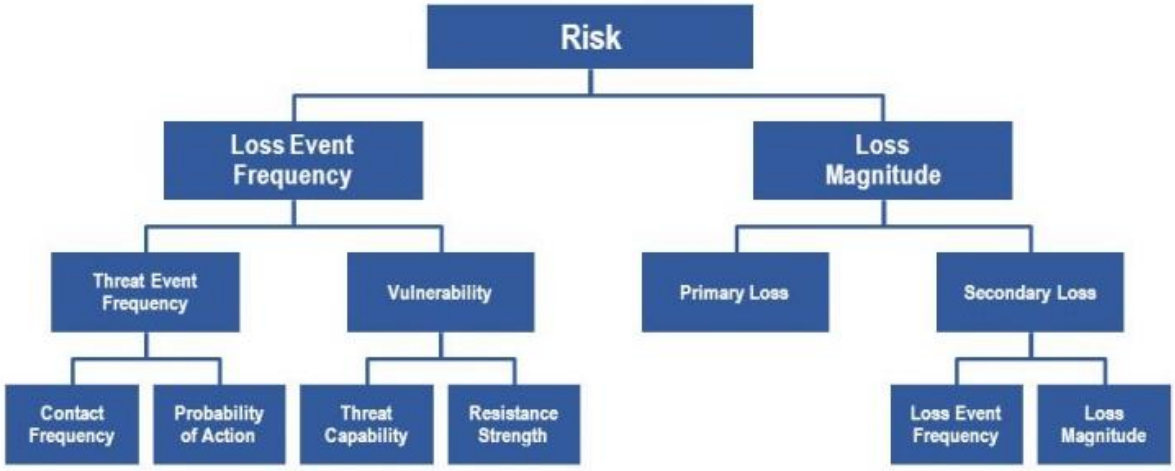

Figure – FAIR structure

One of the strengths of the FAIR methodology is that it provides a structured and quantitative approach to risk assessment, which can help organizations prioritize their risk mitigation efforts. The methodology also allows for the integration of threat intelligence data, which can help organizations stay up to date on emerging risks and vulnerabilities. However, our analysis revealed several limitations of the FAIR methodology when applied to critical infrastructure assessment. For example, the methodology may not adequately account for human factors, such as employee behavior and social engineering attacks, which can significantly impact the risk posture of an organization's information systems [12]. Additionally, the methodology may not be well-suited for assessing complex systems that involve interdependencies and cascading effects. Another approach is to incorporate more advanced modeling techniques, such as system dynamics modeling, which can help capture the complexity and interdependencies of critical infrastructure systems. This approach has been used successfully in other fields, such as supply chain risk management, and could be adapted for critical infrastructure assessment.

The Factor Analysis of Information Risk methodology is a quantitative framework used to analyze and manage information risk. It involves a series of mathematical formulas and calculations to assess and prioritize information security risks. Some of the key formulas used in the FAIR methodology include:

$$R = (F_{te} \cup F_{le})(V_n \cap I_n) \quad (1)$$

Where R – risk;
F_{te} – threat event frequency;

V_n – vulnerability;
F_{le} – loss event frequency;
I_n – Impact.

The risk is determined by multiplying the likelihood of a threat event occurring by the vulnerability of the system to that threat, and then multiplying that by the frequency of loss events that could result from the threat and the impact of those events on the system.

$$F_{te} = T_c F_e \quad (2)$$

Where T_c – threat community;
F_e – event frequency.

The threat event frequency represents the likelihood of a specific threat occurring. It is determined by multiplying the size of the threat community by the frequency with which they are likely to carry out the threat.

$$V_n = S_{control} E_{control} \quad (3)$$

Where *Scontrol* – control strength;
Econtrol – control efficiency.

The vulnerability of a system is determined by multiplying the strength of the security controls in place by their efficiency in detecting and mitigating threats.

$$F_{le} = V_a F_{ex} R_0 \quad (4)$$

Where V_a – asset value;
F_{ex} – exposure factor;
R_o – annualized rate of occurrence.

The loss event frequency with which a loss event is likely to occur. It is determined by multiplying the value of the asset at risk by the exposure factor (i.e. the proportion of the asset that is at risk) and the annualized rate of occurrence of the loss event.

$$I_n = S_{primary} L_{secondary} \quad (5)$$

Where $S_{primary}$ – primary loss;
$S_{secondary}$ – secondary loss.

The impact of a loss event is determined by adding the primary loss (i.e. the immediate costs of the loss event) to the secondary loss (i.e. the indirect costs and consequences of the loss event).

These formulas, along with other calculations and assessments, are used to develop a comprehensive risk management plan for information systems used in critical infrastructure.

2.3 Disadvantages and limitations of The Factor Analysis of Information Risk methodology for critical infrastructure cyberresilience assessment

While the Factor Analysis of Information Risk methodology is a widely used and respected

approach to information risk assessment, there are some potential disadvantages or limitations that should be considered. Here are a few:

Complexity: The FAIR methodology can be complex and time-consuming to implement, particularly for organizations that are new to risk management. It requires a significant amount of data gathering and analysis, and may require specialized expertise in risk management and statistics.

Limited scope: The FAIR methodology is designed specifically for assessing information risk, and may not be well-suited for broader risk management activities. Organizations that need to assess risks in other areas, such as operational, financial, or reputational risks, may need to use additional methodologies.

Subjectivity: Like any risk assessment methodology, the FAIR methodology relies on subjective judgments and assumptions. The accuracy of the assessment depends on the quality of the data and the expertise of the individuals conducting the analysis.

Lack of standardization: While the FAIR methodology is widely used, there is no formal standard or certification process for its application. This can lead to variability in the quality of assessments, and may make it more difficult to compare results across different organizations.

Cost: Implementing the FAIR methodology can be expensive, particularly for organizations that do not have existing risk management processes in place. It may require investment in tools, training, and consulting services.

Overall, while the FAIR methodology has many benefits, it is important to carefully consider its potential disadvantages before deciding whether it is the right approach for a particular organization or situation.

2.4 Ways of improvement of The Factor Analysis of Information Risk methodology for cyber resilience critical infrastructure assessment

The Factor Analysis of Information Risk methodology is a well-established and widely used approach to information risk assessment, but like any methodology, there is always room for improvement. Here are a few suggestions for improving the FAIR methodology:

Standardization: Developing a standard or certification process for the application of the FAIR methodology could help to improve the consistency and quality of assessments across different organizations. This could also help to promote greater adoption of the methodology.

Integration with other risk management frameworks: The FAIR methodology is designed specifically for assessing information risk, but integrating it with other risk management frameworks, such as ISO 31000, could help to provide a more comprehensive approach to risk management.

Simplification: While the complexity of the FAIR methodology is one of its strengths, it can also be a barrier to adoption for some organizations. Simplifying the methodology or creating a more streamlined version could help to make it more accessible to a wider range of organizations.

Incorporating more data sources: The FAIR methodology relies on data from a variety of sources, including expert opinions, historical data, and quantitative data. Incorporating additional sources of data, such as threat intelligence or vulnerability data, could help to improve the accuracy of assessments.

Automation: The FAIR methodology can be time-consuming and resource-intensive to implement. Automating certain aspects of the methodology, such as data collection or analysis, could help to reduce the burden on organizations and make it more efficient.

Overall, the FAIR methodology is a well-regarded approach to ir*Engineering and Technology*t, but there are always ways to improve any methodology. These suggestions could help to make the

FAIR methodology more accessible, accurate, and efficient for organizations of all sizes and industries.

Conclusion

Factor Analysis of Information Risk methodology has proven to be a valuable tool for assessing and managing information risk in critical infrastructure systems. The methodology provides a comprehensive framework for identifying and prioritizing information security risks, and offers a quantitative approach to risk analysis that enables more accurate risk assessments and more informed decision-making. Although the FAIR methodology has several strengths, including its comprehensive approach to risk management and its flexibility in adapting to different organizational structures and risk scenarios, there are still opportunities for improvement. Specifically, there is a need to refine the methodology's definitions and standardize the processes used to conduct risk assessments, and to further integrate the methodology with other risk management frameworks and standards.

In addition to the FAIR methodology, other frameworks and standards, such as the NIST Cybersecurity Framework, ISO/IEC 27001, ISA/IEC 62443, and DHS CSET, provide valuable tools and approaches for assessing and managing information risk in critical infrastructure systems. These frameworks and standards can complement and enhance the FAIR methodology, and should be considered as part of a comprehensive risk management strategy.

Overall, the FAIR methodology provides a strong foundation for managing information risk in critical infrastructure systems, and ongoing efforts to refine and improve the methodology will only serve to enhance its effectiveness and value in the years to come.

References

1. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. Retrieved from : https://www.nist.gov/cyberframework.
2. U.S. Department of Homeland Security. (n.d.). NIST cybersecurity framework. Retrieved from : https://www.cisa.gov/nist-cybersecurity-framework.
3. International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Geneva, Switzerland: Author.
4. National Institute of Standards and Technology. (2019). Special publication 800-53, revision 5: Security and privacy controls for information systems and organizations. Retrieved from : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
5. International Society of Automation. (2020). ISA/IEC 62443: Industrial automation and control systems security. Retrieved from : https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99
6. International Electrotechnical Commission. (2020). IEC 62443-1-1:2019: Security for industrial automation and control systems – Part 1-1: Terminology, concepts and models. Retrieved from : https://webstore.iec.ch/publication/62849
7. International Electrotechnical Commission. (2020). IEC 62443-2-1:2020: Security for industrial automation and control systems – Part 2-1: Establishing an industrial automation and control systems security program. Retrieved from :https://webstore.iec.ch/publication/67403
8. Factor Analysis of Information Risk (FAIR) Institute. (2021). What is FAIR? Retrieved from : https://www.fairinstitute.org/what-is-fair
9. Verma, D., & Verma, A. (2018). A review of quantitative risk management methodologies for critical infrastructure systems. *Reliability Engineering & System Safety*, 180, 198-219. https://doi.org/10.1016/j.ress.2018.07.005

10. U.S. Department of Homeland Security. (2012). Cyber security evaluation tool (CSET). Retrieved from : https://www.us-cert.gov/ccubedvp/cset
11. Froschauer, J., & Held, M. (2017). Combining the FAIR and NIST Cybersecurity Frameworks for improved critical infrastructure protection. *Journal of Information Security and Applications*, 37, 1-10. https://doi.org/10.1016/j.jisa.2017.06.002
12. Bai, Y., Wang, W., Liu, Y., & Chen, H. (2019). A system dynamics approach for assessing the cascading effects of cyber-physical attacks on critical infrastructures. *Reliability Engineering & System Safety*, 190, 106560. https://doi.org/10.1016/j.ress.2019.106560