International Science Journal of Engineering & Agriculture
2024; 3(4): 78-85
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20240304.08
ISSN: 2720-6319

INTERNATIONAL
SCIENCE GROUP

Building resilience through risk management: methodology and strategy

Fedir Korobeynikov
G.E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine
ORCID 0009-0003-8127-4379

To cite this article:
Fedir Korobeynikov. Building resilience through risk management: methodology and strategy. International Science Journal of Engineering & Agriculture. Vol. 3, No. 4, 2024, pp. 78-85. doi: 10.46299/j.isjea.20240304.08.
Received: 06 13, 2024; **Accepted**: 07 22, 2024; **Published**: 08 01, 2024

Abstract: This article presents a risk management methodology designed to enhance the resilience of organisations as complex nonlinear dissipative socio-technical systems. These systems are distinguished by intricate interrelationships, information exchanges, self-organisation, and adaptability to changes in the external environment. A central tenet of this methodology is a quantitative analysis of the likelihood that specific risks could lead to the complete dysfunction of critical processes, potentially resulting in catastrophic outcomes for the organisation. Furthermore, the methodology employs a combined qualitative and quantitative approach to evaluate critical risk mitigation scenarios, acknowledging the stochastic or sporadic nature of these threats. The risk prioritisation process is driven by an assessment of the expected utility of risk mitigation, which facilitates the strategic allocation of resources in accordance with the organisation's risk appetite as defined by its budget. In alignment with the modern resilience paradigm, the proposed methodology prioritises the maintenance of critical operations continuity, rapid recovery from disruptions and the enhancement of the system’s capacity to adapt to unforeseen changes. This methodology can be integrated seamlessly into existing information security management systems, providing a robust framework for sustainable organisational resilience.

Keywords: resilience, information security, risk management, nonlinear dissipative system, risk appetite, adaptation mechanisms, stochastic risks.

1. Introduction

The continuous improvement of information security management systems is of critical importance for the strategic development of society, as it contributes to the efficiency of the functioning of organisations of all types and levels of hierarchy, from local communities to companies, organisations, national and supranational associations. In response to the intensification of globalisation processes and the growth of related destabilising factors, modern organisations must not only effectively withstand various types of threats and recover from incidents, but also demonstrate resilience, adapting to technological, environmental and sociopolitical challenges and evolving as a result. The objective of resilience engineering is to enhance an organisation's capacity to withstand disruption or stress while maintaining the functional capabilities necessary to survive and even thrive.

Effective risk management is the foundation for ensuring the resilience of organisations [2]. The methods and approaches to risk management commonly used in the field of information security are inadequate for ensuring resilience due to the significant impact of stochastic and sporadic types of risks on the effective performance of critical processes of socio-technical systems. Such types of risks

cannot be analysed within the framework of traditional risk management paradigms due to their inherent uncertainty and complexity.

In light of this, there is a pressing need to reconsider traditional risk analysis approaches and develop novel methodologies that can effectively manage all types of critical risks, including stochastic and sporadic ones, thus contributing to resilience building. Consequently, the development of novel methodologies that will guarantee the comprehensive management of critical risks is becoming a paramount scientific objective, one that is of the utmost importance for the maintenance of the resilience of socio-technical systems.

2. Object and subject of research

The objective of this study is to identify the risks that affect the resilience of complex nonlinear sociotechnical systems. The subject of the study is a methodology for managing risks critical to resilience. This methodology aggregates the stages of identifying and analysing critical processes in sociotechnical systems, identifying associated risks, and further ranking and prioritising the treatment of such risks. It also takes into account the developed mitigation scenarios and budgetary constraints. This process of critical risk management entails the analysis of the destructive potential of potential threats and the development of strategies to ensure the continuity of critical processes, with due consideration of the risk appetite of the organisation. As an integral part of resilience engineering, the proposed methodology contributes to the creation of adaptive mechanisms that preserve the functional efficiency of organisations in the face of possible crises.

3. Target of research

The target of this research is to develop a comprehensive methodology for managing all types of critical risks, including stochastic and sporadic ones. The purpose is to do this while ensuring the resilience of sociotechnical systems in conditions of high uncertainty and variability in the external and internal environment.

To achieve this purpose, the study had to address the following main tasks:

1. Identification of a set of risks that require effective management to ensure the resilience of sociotechnical systems.
2. Development of a method for identifying a set of critical risks to be treated within the framework of resilience engineering.
3. Development of a methodology for ranking critical risks based on the expected usefulness of scenarios for their processing.
4. Proposing a method for determining risk management priorities based on the organisation's available budget.

4. Research methods

The research is based on the methodological framework of the resilience paradigm and risk theory. The development of methods for identifying critical risks was informed by the application of elements of set theory and probability theory. Optimisation algorithms and elements of game theory were employed in order to develop methods for the prioritisation of the treatment of critical risks.

5. A conceptualisation of risk management in the context of resilience.

The methods of risk management in the context of ensuring resilience differ significantly from the traditional methods in the field of information security, mainly due to the different focus of their goals and objectives. The goal of resilience is to ensure the ability of a system or organisation to maintain its critical functions in the face of uncertainty and constantly changing threats [5-11]. This

approach focuses not only on preventing threats from materialising, but also on strengthening the system's ability to recover and adapt after possible incidents, thereby continuously improving its protective characteristics.

In the context of this study, it is advisable to define the term 'critical risks', the effective management of which is crucial to ensuring the resilience of systems. Critical or fatal risks of a socio-technical system (*f-risks*) are those risks which, if realised, could have catastrophic consequences, seriously disrupt the functioning of the system and cause its complete collapse. This type of risk threatens not only individual components or processes of an organisation, but also its integrity and ability to perform its core functions. Such risks may include, for example, critical failures of technological systems, disasters caused by human factors or natural phenomena, and other extreme events that could lead not only to prolonged disruption of the organisation's operations, significant financial loss or damage to its reputation, but also to its total destruction.

In contrast to traditional risk management techniques [12], which are oriented towards the prevention of predictable threats to a set of inventoried assets, the resilient approach necessitates a comprehensive approach to critical risks. This encompasses both an analysis of the potential for mitigating predictable risks within this category and an assessment of the system's recovery and adaptive capacity following the occurrence of risks whose prediction is complicated by their stochastic nature. This implies that the assessment will consider not only the previously identified threats, known vulnerabilities and available resources (budget) for counteraction, but also the inherent capabilities of the resilient system to attract and utilise external resources to cope with unforeseen threats or their consequences in the event of incidents related to them.

In the field of information security, the term "risk" is traditionally defined as the potential probability of exploitation of information asset vulnerabilities by a particular threat, which could result in damage [13]. The quantitative definition of risk is the product of the probability of an adverse event occurring and the estimated amount of damage. The probability of the event is calculated as the product of the probability of the threat and the degree of vulnerability, expressed in qualitative or quantitative terms. However, as previously stated, critical risks can be defined as those whose threats have the potential to destroy key system functions. In such cases, the cost of loss is equal to the full value of the organisation's total assets, and the maximum possible loss is considered a constant for all risks in this category.

This leads to the hypothesis that all critical risks should be analysed if there is a non-zero positive probability of their occurrence, given that the realisation of any of them could lead to catastrophic consequences for the organisation as a whole. An additional justification for this hypothesis is the potential impossibility of determining the probability of occurrence for a subset of stochastic and sporadic risks. These risks, which are characterised by a high degree of uncertainty but extremely high potential losses, are of particular relevance in the context of resilience management.

6. A methodology for the management of critical risks

Given the exorbitant cost of potential loss and the largely stochastic nature of critical risks, the methodology for managing them necessitates the utilization of more quantitative approaches than those currently employed in the security domain [14]. It must consider the characteristics of resilient strategies that enable systems to maintain the assurance of core processes and recover swiftly from failures, adapt to changes in the external environment, and evolve in response to new challenges.

A proposed approach for managing critical risks in the context of resilience encompasses a series of successive stages, each of which employs an appropriate method:

1. The initial stage is that of identifying critical processes. An analysis of the primary functions of the organisation is conducted in order to identify the processes that are critical to its functioning.

2. The identification of critical risks represents a fundamental aspect of the proposed methodology. Only those risks that have the potential to lead to the destruction of critical processes within the organisation are selected.

3. The confirmation of the criticality of the risks. The probability of catastrophic outcomes in the event of the implementation of those risks whose criticality is not immediately apparent is evaluated.

4. The selection and quantification of counteraction scenarios. A series of scenarios for the prevention or mitigation of the critical risks are developed and evaluated.

5. Ranking and prioritisation of risks. The anticipated utility of each risk is evaluated, and the risks are ordered according to their relative importance.

6. The optimal sequence of risk treatment is selected, taking into account existing budgetary constraints. The organisation's risk appetite is considered during the risk processing.

The algorithmisation of the critical risk management process in the context of resilience can be illustrated as shown in Figure 1.

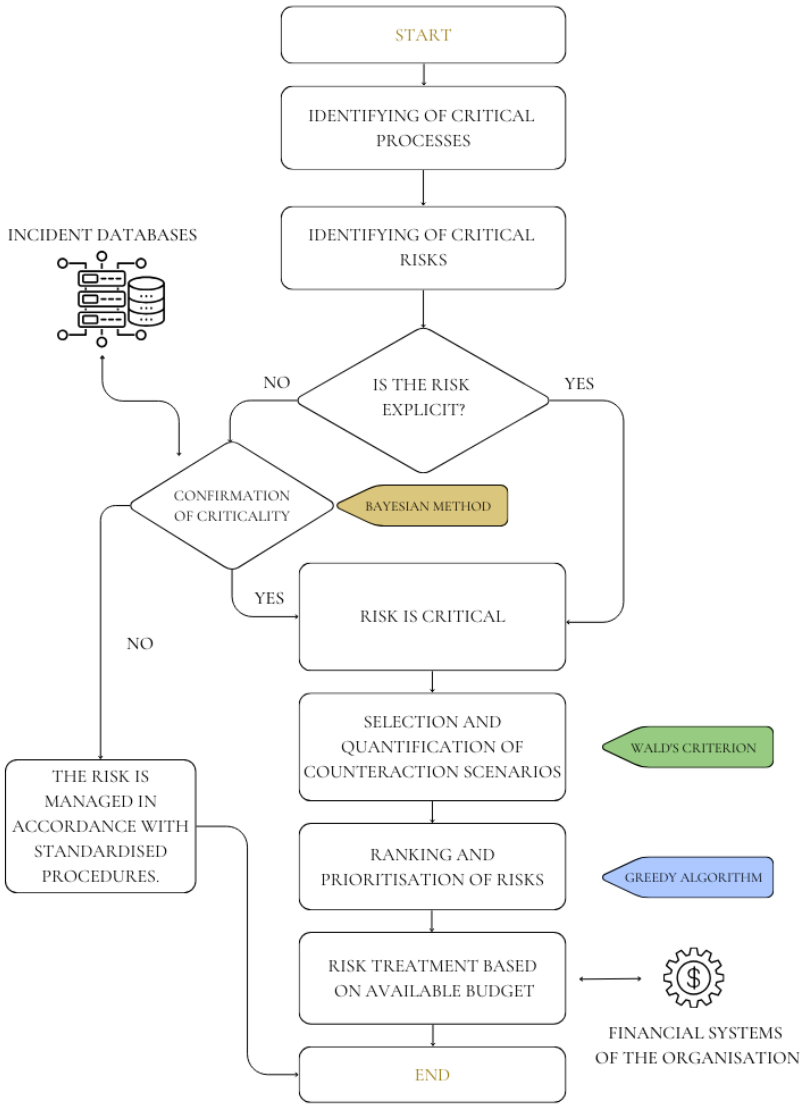

Fig. 1. The algorithmisation of the critical risk management process.

It is of the utmost importance to emphasise that the proposed methodology represents a fundamental component of an organisation's enterprise risk management strategy. In this context, the organisation's management is responsible for developing a risk mitigation budget that quantifies the organisation's risk appetite and reflects its risk tolerance.

The enterprise risk management strategy of an organisation is always subject to limitations resulting from a number of factors. These include geographical, political and religious considerations,

legal and regulatory requirements, and contractual obligations reflected in the organisation's policies and procedures. Furthermore, additional constraints may be imposed by factors that determine access to external financial resources and corporate culture. Such factors can influence the selection and adaptation of resilience engineering methods, strategies, and techniques. An illustrative example is the influence of corporate culture, which may prohibit the utilisation of "deception techniques" [15] due to their perceived ethical ambiguity.

The presence of limiting factors underscores the necessity to delineate the structural invariants of an organisation with precision, by identifying its principal functions and related processes and systems that ensure the organisation's essential operations. All efforts and resources within the framework of resilience engineering will be directed towards ensuring the guaranteed performance of these functions.

This approach to implementing the initial stage of the risk management methodology, which involves formalising the goals and objectives of the organisational and technical system and identifying its critical functions and processes as priority objects of protection, can be described as deductive. It is important to note that the audit of information assets - the initial stage of risk management in the information security paradigm, is, in contrast, inductive in nature. This highlights one of the key distinctions between "resilient" and "non-resilient" approaches to risk management. In resilience engineering, the initial step is to identify the critical functions of the system and then focus exclusively on those risks that could lead to a fatal disruption of the system's performance. In this manner, the actualisation of critical functions serves as the foundation for the identification, analysis, and prioritisation of risks directly related to resilience.

Risks that present a threat to critical processes are divided into two categories: explicit and implicit. Explicit risks are those that are immediately apparent and have a clear destructive nature. To illustrate, the nationalisation of arable land is a phenomenon that inevitably leads to the collapse of a private agribusiness company as a sociotechnical system. Implicit risks, on the other hand, are less obvious and require a different approach to substantiate their destructive potential. One such approach is to interpret the Bayesian approach in this context. The application of Bayes' theorem to the analysis of hypotheses that the realisation of implicit risks will lead to fatal consequences allows us to select only those of them that are most likely to lead to the dysfunction of critical processes. The analysis generates a set of hypotheses, each of which corresponds to a particular implicit risk whose criticality is not immediately apparent and depends on specific conditions. The hypotheses are tested using data, such as compromise indicators, incident statistics or information from threat intelligence data monitoring services. Bayes' theorem is employed to update the probability of hypotheses H_i based on the analysis of the D data, thereby elucidating the extent of their fatalisation and potential impact on the organisation. The formula for confirming the hypothesis is as follows (1):

$$P(H_i|D) = \frac{P(D|H_i)\cdot P(H_i)}{P(D)}, \quad (1)$$

where: $P(H_i \mid D)$ is the posterior probability of the hypothesis H_i, given the data D;

$P(D \mid H_i)$ is the probability of observing data D if the hypothesis H_i is true.

$P(Hi)$ is the a priori probability of the hypothesis H_i;

$P(D)$ is the total probability of observing the data, which can be calculated as the sum of the probabilities of D, for all the hypotheses under consideration.

Once the posterior probability of each H_i hypothesis has been calculated, those risks should be selected where the probability of destructiveness exceeds the "criticality threshold" approved by the organisation's management. If the calculated values of probabilities exceed the aforementioned threshold, the implicit risks are classified as critical and are processed in accordance with the procedures of resistance engineering. Otherwise, risk processing is performed in accordance with the procedures provided by the information security framework.

After the identification and verification of "f-risks" that have the potential for existential impact on the organisation (i.e. risks whose realisation is highly likely to result in the cessation of its activities), the next stage of the methodology is to develop and quantify the cost of scenarios for responding to these risks.

At this juncture, the Wald's Criterion can be employed as a tool for rational choice under uncertainty. The Wald's Criterion, also known as the maximin criterion, involves selecting response scenarios that provide the best outcome in the worst conditions [16].

This approach is predicated on the minimisation of the maximum possible damage. Consequently, the response scenarios developed should be evaluated according to their ability to cope with the worst possible consequences, with preference being given to those strategies that provide the best outcome in the worst possible set of circumstances.

In practice, a divergent approach to decision-making is employed, whereby a number of potential scenarios of risk response are considered simultaneously, with the most adverse circumstances taken into account. Each scenario is evaluated in terms of the financial and temporal costs that would be incurred in its realisation. The scenario that prevents a catastrophe in the worst-case scenario with the lowest realisation cost is selected.

Consequently, the application of the Wald criterion aligns with the principles of rational choice in conditions of uncertainty, where decisions are made on the basis of minimising the maximum possible losses. This is of particular importance when managing risks with potentially catastrophic consequences.

Once the full set of critical risks has been identified and the cost of potential scenarios to mitigate each risk has been estimated (with the most unfavourable scenario taken into account), the next step is to rank the risks based on the expected utility of their handling. This can be calculated using the formula (2):

$$u_i = l_i - c_i \,, \tag{2}$$

where: l_i – loss in case of risk realisation;

c_i – cost of the countermeasure scenario.

However, in the event of the realisation of any risk from the specified set of critical *f-risks*, the losses will always be maximum. This leads to the conclusion that the variable l is a constant ($l = const$) for all risks in this subset, and l tends to infinity ($l \to \infty$). In this context, when ranking critical risks, it is only necessary to consider the cost of processing them.

A methodology is proposed in which risks are ranked based on the expected utility of their processing. This is achieved using a greedy algorithm [17]. The proposed methodology prioritises the processing of risks with the lowest processing cost. This is because they have the highest utility in the context of resilience.

The utilisation of a greedy algorithm to optimise the selection of risks within a limited budget represents a pragmatic solution, predicated on the assumption that locally optimal decisions can result in a globally optimal outcome.

The process commences with the ranking of risks in ascending order of mitigation cost. The risk with the lowest mitigation cost is selected first, provided that its cost does not exceed the allocated budget. The budget is adjusted by subtracting the mitigation cost of the selected risk from it, and the process is repeated for the next risk in the sorted list. The process of iteration continues until either the budget is exhausted, or all risks have been covered.

In essence, the proposed method is an interpretation of the "backpack problem," a combinatorial optimisation problem where the objective is to select a subset of items with the maximum total value while ensuring that the total weight of the selected items does not exceed the specified carrying capacity of the backpack. In the context of this study, the items correspond to risks, the value corresponds to the expected utility of the mitigation, and the carrying capacity of the backpack is analogous to the organisation's budget.

The process of analysing and prioritising critical risks can be facilitated and accelerated by using a visual tool - a three-dimensional matrix that aggregates all types of risks faced by an organisation and allows them to be managed within a unified strategy [18].

It should be emphasised that in the context of a dynamically changing threat landscape and the non-linearity of processes characteristic of organisations as complex open dissipative socio-technical systems [19], regular review and updating of risk assessment is required. An iterative approach to risk management based on the proposed methodology will allow organisations to maintain a high level of preparedness for the unexpected and ensure their resilience in a constantly changing environment.

7. Prospects for further research development

Further research may be directed towards the development of methodologies for the iterative enhancement of the resilience characteristics of sociotechnical systems. This may be achieved by the stimulation of recovery and adaptation mechanisms, which will enhance their capacity to withstand stochastic and sporadic risks under conditions of uncertainty.

8. Conclusions

The paper presents a methodology for risk management in the context of resilience engineering that takes into account the specifics of sociotechnical systems. The proposed approach diverges from traditional risk management methodologies employed in the information security sector and is predicated upon the following fundamental tenets:

- The methodology places a particular emphasis on the identification and analysis of critical risks. Given the potentially catastrophic consequences of critical risks, the methodology focuses on their identification, analysis, assessment and treatment, with due consideration of the available budget.
- A quantitative approach is employed. Given the stochastic nature of critical risks, the methodology employs quantitative methods to assess the likelihood of risks being destructive.
- Risk prioritisation. The methodology entails ranking risks according to the anticipated utility of their processing, thereby facilitating the optimal allocation of resources for risk management.

The methodology is focused on the development and implementation of strategies aimed at ensuring the continuity of critical processes, rapid recovery from disruptions, as well as adaptation and evolution of the system in response to new challenges.

The proposed methodology can be employed to enhance the resilience of sociotechnical systems to a range of critical risks, including those associated with external threats, internal failures, and changes in the external environment.

9. Acknowledgements

The author extends his profound gratitude to his esteemed colleagues at SCM for their invaluable support and insightful comments, which were pivotal to the successful completion of this study. The author is particularly indebted to Corresponding Member of the National Academy of Sciences of Ukraine, Doctor of Technical Sciences, Professor Volodymyr Mokhor, whose guidance and expert opinions were crucial at all stages of this research. Additionally, the author expresses sincere appreciation to the scientists from the G.E. Pukhov Institute for Modelling in Energy Engineering (IPME), Kyiv, whose pioneering research laid the groundwork for the Ukrainian scientific school of information security and resilience and served as a significant source of inspiration for this work.

References:

1) Louisot, J. (2015). Risk and/or resilience management. Risk governance & control: Financial markets & institutions, 5(2-1), 84-91. https://doi.org/10.22495/rgcv5i2c1art2

2) NIST Special Publication 800-160, Volume 2. Developing cyber-resilient systems: A systems security engineering approach. (2021). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

3) Necci, A., Cozzani, V., Spadoni, G., & Khan, F. (2015). Assessment of domino effect: State of the art and research Needs. Reliab. Eng. Syst. Saf., 143, 3-18. https://doi.org/10.1016/j.ress.2015.05.017

4) Korobeynikov, F. (2023b). Using the Wald Maximin Criterion for Risk Analysis of Hard-To-Predict Threats in the Context of Resilience. Èlektronnoe modelirovanie, 45(6), 31–40. https://doi.org/10.15407/emodel.45.06.031

5) Bodeau D., Graubart R. Cyber Resiliency Engineering Framework. 2011. The MITRE Corporation. URL: https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf

6) Mallak, L. A. (1998). Measuring resilience in health care provider organizations. Health Manpower Management, 24(4), 148–152. https://doi.org/10.1108/09552069810215755

7) Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. Risk Analysis, 29(4), 498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

8) Hale, AR., & Heijer, H. Defining resilience. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), 2008, Resilience Engineering, P. 35-40. Ashgate. ISBN 075464641 6

9) Stephenson, A., Seville, E., Vargo, J. and Roger, D. Benchmark Resilience: A Study of the Resilience of Organisations in the Auckland Region. 2010. In: Resilient Organisations Research Report 2010/03b, Resilient Organisations Research, Auckland. URL: http://hdl. handle.net/10092/4275

10) McDonald, N. Organisational Resilience and Industrial Risk. 2017. In: Resilience Engineering by David D. Woods, Erik Hollnagel, P. 155-180, CRC Press. ISBN: 9781317065289

11) Grote, G. Rules Management as a Source of Loose Coupling in High-Risk Systems. 2008. In: Hollnagel, E., Nemeth, C.P. and Dekker, S.W.A., Eds., Resilience Engineering Perspectives Volume 1: Remaining Sensitive to the Possibility of Failure, Ashgate, Aldershot. ISBN 9780754671275

12) What is risk? (2023). У Risk Management and ISO 31000 (с. 12–20). IT Governance Publishing. https://doi.org/10.2307/jj.1094269.6

13) Mokhor, V., Bakalynskyi, O., & Tsurkan, V. (2018). Risk assessment presentation of information security by the risks map. Collection "Information technology and security", 6(2), 94–104. https://doi.org/10.20535/2411-1031.2018.6.2.153494

14) NIST Special Publication 800-37. Risk management framework for information systems and organizations. (2018). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-37r2

15) Cyber Resiliency Engineering Framework (CREF) Navigator. The MITRE Corporation. Online framework. URL: https://crefnavigator.mitre.org/navigator

16) Korobeynikov, F. (2023). Using the Wald Maximin Criterion for Risk Analysis of Hard-To-Predict Threats in the Context of Resilience. Èlektronnoe modelirovanie. https://doi.org/10.15407/emodel.45.06.031.

17) Wang, Y. (2023). Review on greedy algorithm. Theoretical and Natural Science, 14(1), 233–239. https://doi.org/10.54254/2753-8818/14/20241041

18) Korobeynikov, F. O. (2024). Resilience in Focus: Rethinking the Risk Matrix. Electronic modeling, 46(2), 35–42. https://doi.org/10.15407/emodel.46.02.035

19) Prigogine, I. (1976). L'Ordre par Fluctuations et le Système Social. In L'Ordre par Fluctuations et le Système Social / Entropie einst und jetzt (pp. 7–48). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-663-00234-5_1