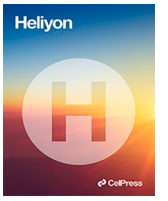
Heliyon 10 (2024) e26439

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

Risk analysis of critical infrastructure with the MOSAR method

Ajda Fošner *, Brane Bertoncelj, Tomaž Poznič, Laura Fink

GEA College, Slovenia

ARTICLE INFO

Keywords:
Risk analysis
MOSAR method
Critical infrastructure
Distribution transformer stations

ABSTRACT

The smooth running of the electric energy system is crucial, especially given the current geopolitical environment. To achieve this goal, it is essential to establish a solid infrastructure that is both accessible and safe. We protect consumer reputation and trust, reduce financial losses, and lessen unfavourable effects on employees and business owners by maintaining continuous functioning. This study has discovered several important concerns using the Method Organised Systematic Analysis of Risk (MOSAR). These include the possibility of cyberattacks, the availability of information and technology systems, the loss of critical individuals, and network problems. To address these risks, it is necessary to deliver electrical energy on time and at a high standard, to be responsive to client requests, and to follow best practices, technical standards, and personal and environmental protection measures. The findings of this study make valuable contributions to risk assessment efforts, allowing us to identify potential threats to the security and reliability of national power systems. Overall, it is essential to maintain a robust and resilient energy infrastructure to ensure uninterrupted operation and mitigate risks effectively.

1. Introduction

The term “critical infrastructure” refers to the important infrastructure – including the power grids, transportation networks, and communication systems – that is necessary for society to function. Critical infrastructure’s resilience is its capacity to foresee, tolerate, and quickly recover from disturbances while maintaining continuous operation [1]. To prevent serious consequences, such as financial losses, societal disruptions, and potential threats to public safety, it is essential to maintain the continuous operation of vital infrastructure firms. To reduce the effects of disruptions and ensure that they can continue to offer key services without interruption, these businesses must strengthen their resilience [2].

First and foremost, one of the most important steps in strengthening the resilience of critical infrastructure organizations is to undertake thorough risk assessments to pinpoint vulnerabilities, potential threats, and crucial dependencies. In order to minimise potential interruptions, effective risk management methods are essential [2]. These tactics include establishing strong cybersecurity protections and creating business continuity plans. Additionally, adding redundant power sources and data storage facilities can greatly improve the resilience of critical infrastructure organizations [3]. These steps ensure there are backup plans and resources to keep things running smoothly even in the event of breakdowns or disruptions. Additionally, encouraging cooperation among important stakeholders, government organizations, and vital infrastructure providers is crucial for boosting resilience. The development of efficient tactics, the improvement of reaction capacities, and the overall improvement of system resilience can all be facilitated

* Corresponding author.
E-mail addresses: ajda.fosner@gea-college.si (A. Fošner), bertoncelj.b@siol.net (B. Bertoncelj), tomaz.poznic1@gmail.com (T. Poznič), Laura.Fink@gea-college.si (L. Fink).

https://doi.org/10.1016/j.heliyon.2024.e26439
Received 16 August 2023; Received in revised form 9 February 2024; Accepted 13 February 2024
Available online 15 February 2024

by the sharing of knowledge, best practices, and lessons learnt [1]. Also, leveraging technological advancements, such as advanced monitoring systems, predictive analytics, and automation, can significantly contribute to enhancing the resilience of critical infrastructure companies [1]. These technologies enable early detection of potential disruptions, proactive response measures, and efficient resource allocation during crisis situations [4].

The year 2023 is marked by energy anxiety and rapidly changing global geopolitical conditions, reflected in the failure of global governance [5]. This paper discusses the challenges of critical infrastructure resilience for uninterrupted operations in today's complex and interdependent world. The COVID-19 pandemic and the war in Ukraine have exposed weaknesses and highlighted the importance of organizational and leadership resilience [5]. This paper stresses the need for continuous planning for the protection of critical infrastructure in the energy sector, to ensure an uninterrupted energy supply. Key indicators of energy security include energy dependence, energy sources, energy imports and exports, stocks, prices, and energy consumption [1]. In Slovenia, energy dependence is at 47.3% in 2021, compared to 57.5% for the EU in 2020 [6].

Business resilience, as the ability of a company to survive and thrive in difficult or unfavourable circumstances such as emergencies, changes in the environment, inappropriate human activity or other challenges, is a fundamental competency and business imperative that should be built into all key business areas [2]. To achieve organizational resilience, it is necessary to identify not only significant vulnerabilities and risks but also the risks that may appear to be just "business as usual." Business continuity, risk management, and crisis management are essential components of successful corporate governance [4].

Furthermore, the company's main task is survival. Profit maximization and loss avoidance are guiding principles in business economics. In electro distribution "business continuity" refers to processes or systems that must operate without interruption [2]. This study defines managing business continuity as a holistic approach that identifies potential risks and threats to the company. The goal is to protect business functions and critical support functions. The response to an extraordinary event usually depends on past preparations and experiences. The ISO 22301:2019 standard [7] for business continuity management systems provides requirements for planning, establishing, implementing, monitoring and improving management.

To maintain continuous operation, it is essential to comprehend the required preventive measures for detecting different risk events in the production, transmission, and distribution of electrical energy. The effective management of risk in distribution transformer substations plays a pivotal role in safeguarding the vulnerability, security, and overall resilience of the electrical network's production, transmission, and distribution processes.

Reviewing case studies and best practices from a variety of key infrastructure sectors, including energy, transportation, and telecommunications, offers insightful information on effective resilience enhancement techniques. Finding common problems, workable solutions and lessons gained that may be applied in other circumstances are made possible by analysing these examples.

Numerous case studies in the energy sector have emphasized the importance of setting up reliable backup systems and diversifying energy sources. For instance, Jasinas et al. [8] concentrate on two different threats: cyberattacks, which are now a minor but growing risk, and extreme weather, which is the primary cause of interruptions in the energy supply. They show different perspectives on hazards to the energy system by emphasizing interactions between the parts of the energy system and their environment. In addition, numerous case studies in the transportation industry have shown how important proactive maintenance and asset management are. Serdar et al. [9] present resilience evaluation methods for transportation networks, indicators, and disturbance types. Nipa et al. [10] developed a comprehensive list of dimensions that can be used to measure the resilience of transportation systems. Moreover, the telecommunications industry has also seen considerable advancements in strategies for strengthening resilience (see, for instance Refs. [11,12]).

The examination of these case studies and best practices identifies common problems and efficient fixes that can be used in numerous critical infrastructure sectors. The relevance of:

- Diversifying energy sources and investing in renewable energy for a more reliable power supply is one of the key results.
- Asset management and proactive maintenance to increase the reliability of transport networks.
- Implementing network segmentation and real-time threat monitoring systems to reduce cyber threats in the telecommunications industry.

Policymakers, infrastructure managers, and stakeholders can learn a lot about effective resilience augmentation methods by examining these examples. The resilience of critical infrastructure organizations can be increased overall by adapting and using the lessons learnt from these case studies in different circumstances.

Despite significant progress in enhancing the resilience of critical infrastructure companies, several research gaps remain. Further investigation is needed to address emerging threats, explore the impact of emerging technologies, and develop comprehensive frameworks for assessing and enhancing resilience. The aim of this paper is to significantly contribute to addressing these persistent research gaps and advancing the understanding of critical infrastructure resilience. Our innovative approach centres around the application of the MOSAR (Method Organised Systematic Analysis of Risk) method. This method offers a meticulously structured and all-encompassing framework for assessing and mitigating risk factors, particularly in the context of power supply management. Our research question: How does the application of the Method Organized Systematic Analysis of Risk (MOSAR) identify and evaluate critical risk factors affecting power supply management?

2. Methodology

The effective management of risks is crucial for the continuous and resilient operation of the power system. To understand the risk

profile, the analysis of risk evaluates the origin of risk, assets or processes that pose a risk, vulnerabilities, effectiveness of internal controls and potential impact. This analysis focuses on risks associated with the management of the power supply, particularly the efficiency of risk management related to distribution transformer stations.

Methods for managing risks are based on conceivable incident scenarios, their effects, and the possibility that a threat or risk would materialize. Risk evaluations are made sure to be documented, reproducible, and preventive using fundamental analytical methods. Risk evaluations must be open and include unambiguous weighting factors, clear assumptions, and subjective judgements. To evaluate advances in safety and resilience, effectiveness measurements must be used in the risk management process.

In the sections that follow, we go over how crucial risk analysis and business continuity are at distribution transformer stations, or DTS for short, which are essential to distributing power to lots of users. The DTSs, which are a component of the transmission network, make it possible to safely convert electrical energy from high to low voltage and vice versa. Additionally, they control voltage, enhance the quality of the electricity, and aid in the integration and management of distributed and renewable energy sources.

2.1. MOSAR method

Within the study, we use MOSAR methodology that systematically evaluates risks. It is a holistic approach that allows for progressive risk analysis and is particularly useful for studying the effects of concurrent accidents or "domino" effects. MOSAR analyzes risks in the environment and provides a systematic approach to risk assessment, prioritization, risk management and risk treatment [2, 3]. The method is characterized by a preventive approach that assesses the adequacy of preventing exceptional events and risks and introduces interdependence elements in risk management processes. The method uses logical evaluations to analyze various processes, procedures and protocols to identify potential errors, malfunctions and deficiencies. It introduces severity and probability elements in the exceptional event, error, malfunction or other harmfulness assessments. It identifies the frequency and severity levels of different identified risks and introduces scenario development of risk mitigation for exceptional events. Additionally, it links highly evaluated risks to protective measures in risk management which considers technological barriers in terms of obsolescence, poor maintenance of processes and equipment, organizational deficiency, or external threads [2].

Risk analysis occurs in several steps [13].

- Identifying system failures - identifying all risk factors involved and identifying scenarios that could lead to technical accidents.
- Risk assessment - including assessment of technical consequences of accidents and their likelihood of occurrence. Risks are classified into several categories: negligible, acceptable, and unacceptable.
- Elimination of unacceptable risks - involves establishing methods, means, and procedures aimed at preventing damage from significant risks and/or neutralizing their effects.
- Managing remaining risks and defining measures, plans, and crisis strategies.

The following figure presents a systematic approach of the MOSAR method, which provides a sequence of phases for assessing the risk of technological processes in an industrial environment and explains the content of each step, thus unambiguously contributing to the risk assessment process (Fig. 1). The methodology developed is in line with the applicable legal regulations in the field of industrial accident prevention and is harmonized with the procedures used for practical risk assessment.

The methodology encompasses an initial system description with its subsystems, defining specific and measurable performance objectives to gauge success. This is then followed by the identification of potential threats to the system's operations [4]. By leveraging a combination of experience, forecasts, system expertise, and available resources, the scope of threats and hazards that primarily impact the social community, critical infrastructure, and its users, or exhibit any influence over them, is determined [1].

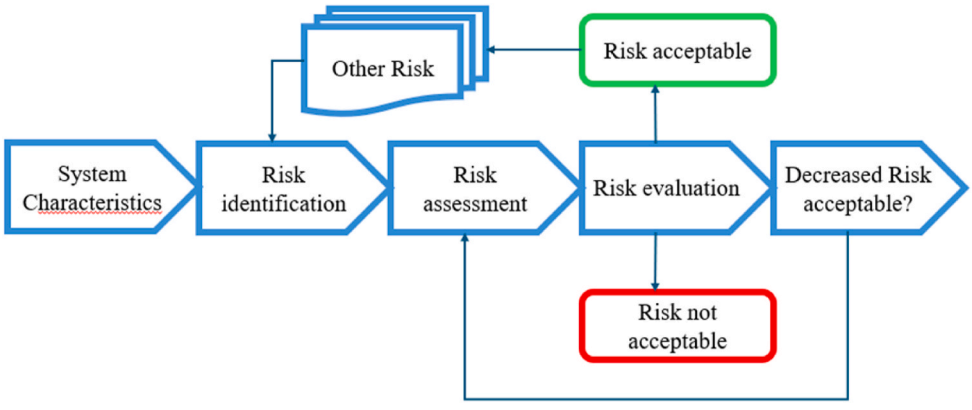


Fig. 1. MOSAR method
Note. Adapted from *Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture,* by Čaleta et al., 2019 (https://www.gov.si/assets/ministrstva/MO/Dokumenti/Studija-SPOTKI.pdf). In the public domain.

Risk analysis and assessment are used to evaluate each identified threat and hazard within the context of establishing precise capability objectives for each significant component [2]. The assessment also considers the potential for security measures to be bypassed or thwarted. It factors in any element that might facilitate security measure avoidance, such as measures that disrupt the system's operation or hinder other activities, are cumbersome to employ, involve subcontractors beyond the system operator, or are not recognized or deemed suitable for the function by the system operator.

Acceptable risks may create new risks upon re-evaluation. In the case of unacceptable risks, it becomes imperative to assess the preventive measures, procedures, and resources required to attain performance objectives for each critical capacity [4]. This may involve developing a risk reduction system, adhering to the business process control hierarchy, eliminating or replacing hazards, implementing management controls, and more. Risk reduction strategies might include hazard removal or simultaneous reduction of the two components that determine associated risks: the severity of the damage linked to a particular hazard and the likelihood of such damage occurring [1,2].

Let us also point out that we focused on Module A of the MOSAR method which is suitable for a macroscopic risk analysis that may have human consequences: industrial sites, buildings, factories, laboratories, health, planes with pilot and passengers etc. On the other hand, Module B of the MOSAR method is used for technical risk analysis for the safety and the security of systems (physical and operating risks): valve, plane without pilot, instruments, chemical or biological reactions, procedure etc.

Both modules have almost the same structure [14].

3. Risk assessment for distribution transformer stations by MOSAR method

3.1. Recognition of risk sourcesqqqq

The MOSAR methodology for risk management begins with identifying potential sources of risk in relation to the critical infrastructure of the power grid [2]. Seven key groups of risks threaten the power grid, including the supply of electricity in general and specifically the DTS. These groups were identified based on previously defined sources of risks. Risks related to corporate security and strategy are not directly related to DTS and are therefore not addressed in the study (see also [2–4]).

Technological risks: The transmission system operator's vital energy infrastructure is subject to technological hazards such as technological mishaps, transformer and component failures, maintenance errors, and electrical network flaws. It's crucial to correctly design, maintain, and test the operation of transmission stations' components to reduce technological hazards. It is important to avoid conditions that could lead to explosions or failures, such as overheating, overloading, gas buildup, and others.

War and terrorism: Here we focus on the risk of physical attacks by external groups such as terrorists or saboteurs, which can cause damage or destruction to DTS. Small DTSs are more vulnerable to physical attacks, but since they serve a relatively small number of users, they do not usually affect the overall system's reliability.

Natural disasters and environmental risks: DTS may sustain damage or be destroyed by environmental hazards and natural calamities such as earthquakes, floods, ice storms, precipitation, lightning, or wind. Potential leaks of dangerous liquids are another source of environmental risks.

Cyber security: Cyberattacks may be directed upon DTS stations because they are frequently connected to the internet. Cyber intrusions have the potential to result in a cascade of distribution system and DTS station failures. To prevent cyber-attacks, it is advisable to take a series of preventive measures, including preparing appropriate scenarios, following access protocols, regularly maintaining and testing equipment, controlling and installing appropriate equipment, training employees, and using intrusion detection systems, intrusion prevention systems and incident response systems.

Epidemics: In the face of epidemics (such as COVID-19), it is necessary to ensure the uninterrupted operation of critical infrastructure.

The human factor: The operation and management of the electric power system require a lot of knowledge and concentrated work from employees. DTS shall be properly maintained, repaired, constructed and modernized. Errors or negligence in work can cause damage and power outages, as well as affect the efficiency of the system and result in losses.

3.2. Risk scenario identification

For all main risk categories scenarios of risks are identified. Scenarios of technological risks include transformer failures, failures of electronic elements, failures of the management system, connection failures, provision of system services, energy transmission, cross-border transmission capacity, strategic technical indicators, network construction, technology changes, energy transmission network, system slowdowns, and construction of a telecommunications network. The failure of any of these subcategories can lead to a decrease in the reliability of the system, loss of electrical energy in the transmission system and an imbalance between supply and demand.

3.3. Scenario risk assessment

We evaluated each scenario's risk based on its probability and impact and classified them into a risk matrix. Scenarios with high weight or critical risk assessment require special attention. Probability and impact are assessed on a scale of 1–5. The risk is calculated by multiplying those two values. The timeframe and frequency of the risk event should also be considered.

In our risk assessment process, each scenario was meticulously analyzed to determine its likelihood of occurrence (probability) and the potential severity of its consequences (impact). Both dimensions were evaluated using a quantifiable scale from 1 (very low) to 5

(very high).

3.3.1. Probability assessment

1. Very Low - The event is rare or has happened in less than 10% of similar circumstances.
2. Low - The event is uncommon but has occurred in 10–30% of similar situations.
3. Moderate - There is a 50-50 chance of the event occurring.
4. High - The event is likely and has a history of occurring in 70–90% of similar conditions.
5. Very High - The event is almost certain to occur, with a precedent in more than 90% of similar cases.

3.3.2. Impact assessment

1. Very Low - Negligible consequences that require minimal to no intervention.
2. Low - Minor consequences that may require a simple corrective action.
3. Moderate - Notable consequences that will need management involvement and potential adjustments to plans.
4. High - Major consequences that could affect the project's critical path or objectives significantly.
5. Very High - Severe consequences that could result in failure to meet primary objectives or project termination.

The risk score is calculated by using the following formula:

Risk score = probability · impact

In our study, the assignment of probability values to various risk factors was rigorously conducted by analyzing the historical frequency of their occurrence. This analysis entailed a systematic review of empirical data spanning several years, which we sourced from publications renowned in the field of risk analysis and critical infrastructure protection [1,15]. We employed a methodical approach to quantify the frequency, where each risk factor was assigned a probability score based on its rate of occurrence within the historical record. The scoring system was derived from a standardized scale commonly accepted in risk assessment literature [1,15]. Regarding the assessment of impact, we quantified the potential damage of each risk event in monetary terms (euros), drawing on a well-established methodological framework used in the field [1,15]. This framework considers both direct and indirect costs associated with each risk scenario, encompassing repair or replacement expenses, lost revenue due to service interruption, and broader economic impacts. To ensure consistency and replicability, we adhered strictly to the valuation guidelines and damage assessment procedures as detailed in the referenced studies [1,15]. The synthesis of these quantified probability and impact assessments enabled us to calculate a risk factor for each identified risk. The risks were then ranked, and those with the highest composite risk factor—representing the most significant potential for damage and the highest likelihood of occurrence—were highlighted as priority concerns. By adhering to this structured, transparent, and literature-backed approach, our methods can be replicated and validated by other researchers in the field, ensuring the robustness and reliability of our risk assessment findings.

The data in Table 1 can be represented using the following risk matrix (Fig. 2).

We have identified ten major risks (in the red zone), namely:

- Influence – very high/Probability - unlikely: DTS failure, construction of the transmission network, poor availability of IT system, loss of key personnel.
- Influence - high/Probability - likely: malware attack, hacker attack, social engineering, maintenance and repair errors in DTS, DTS management errors.

Table 1
Risks with the highest risk factor.

ID	Risk scenario	Probability	Impact	Risk score	Timeframe[a]	Frequency[b]
1	**Technologic risks**					
1.1	Transformer malfunction	3	5	15	All operations time	Rare
1.10	Technology change	3	5	15	All operations time	Rare
1.14	IT systems not available	3	5	15	All operations time	Rare
4	**Cyber security**					
4.1	Malware attack	4	4	16	All operations time	Often
4.2	Hacker attack	3	4	12	All operations time	Rare
4.5	Social engineering	4	4	16	All operations time	Rare
6	**Human factor**					
6.6	Maintenance error	4	4	16	All operations time	Often
6.7	Operations error	4	4	16	All operations time	Often
6.12	Internal fraud	3	5	15	All operations time	Rare
6.24	Key personal loss	3	5	15	All operations time	Rare

[a] Timeframe: The time period during which the risk can materialize in the operation of the DTS.
[b] Frequency: Whether the risk can materialize only once or multiple times.

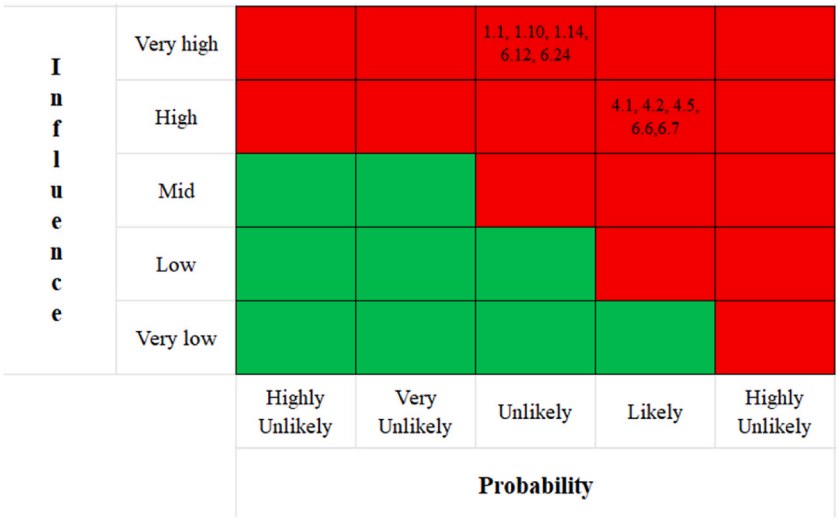


Fig. 2. Risk matrix
Note: RED – High risk, GREEN – Low risk. (For interpretation of the references to colour in this figure legend, the reader is referred to the Web version of this article.)

3.4. Analyses and risk rating

High-risk events can highly impact business objectives, operations, reputation and financial resources. Technological, cyber security and human resources risks are deemed as the most critical, with the highest probability of occurrence and potential damage to the company. Preventive measures, such as upgrading and maintaining technology systems and investing in employee education and motivation, can significantly reduce these risks. For other emerging risks such as war, terrorism and epidemics the probability of occurring is low, but the potential consequences could be severe.

3.5. Risk mitigation assessment

Due to mitigate risks we identified activities, measures and procedures, security policies, instructions and good practices. This aims to assess resources to reduce or eliminate the causes of failures and can involve processes such as changing and supplementing operation procedures and purchasing additional equipment or control systems to improve failure detection. It is important to note that mitigation actions shall be implemented until a satisfactory risk level is achieved. As long as the root cause of the failure is not reduced or eliminated the severity of the risk should not change. The root cause of the failure may or may not be reduced based on the results of the actions taken or preventive/corrective actions. If the risk score (after implementing measures) is not improved, additional measures and activities shall be defined.

By analyzing primary and secondary sources, we determined that the electro-distribution operator recognizes sources of danger, analyzes failure modes and consequences, identifies resulting risks and assesses their criticality [16]. Therefore, we confirm that effective risk management of distribution transformer stations is crucial for maintaining the vulnerability, resilience, production, transmission and distribution of the power grid.

4. Discussion

The continuous operation management system ensures the functioning of the power grid during emergencies while minimizing their impact on customers, shareholders and business operations. It ensures corporate governance, compliance, and effective security maintenance, protects reputation and builds customer trust in business stability. It is crucial to act promptly after an emergency and any operational downtime [17]. In the event of an emergency, the response must be quick, including identifying it as an emergency, notifying business process stakeholders, initiating a response, informing responsible personnel and replacing absent employees and resources (relocating to a backup location, using cloud or hybrid capacities, engaging additional service providers, etc.).

Operational resilience involves fulfilling the vision and promises to customers that the power grid will always provide contractual services regardless of circumstances. No system is entirely immune to emergencies as they occur at different time intervals [17]. It is expected that power grid administrators dynamically respond to an emergency, whether it was anticipated as high-risk or not.

Based on the reviewed literature, experiences, and previous research, we utilised the MOSAR method to evaluate risks linked to power supply management, with a specific focus on the effectiveness of risk management in distribution transformer stations. The goal of the MOSAR methodology is to detect dysfunctions (inappropriate functioning) and manage the risks of a complex system [1–4]. It uses structured elements, contains a general approach to risk analysis, and defines measures and procedures for reducing risks. It is a

tool for easier decision-making, finding the main scenarios of system failure, and determining the necessary protection and protection measures to neutralize or reduce an emergency event. The method is suitable for preparing the conceptual design of a new system or for diagnosing an existing system. MOSAR assesses the scope of interactions of subsystems in ten steps, namely: identification of sources of danger, adequacy of prevention of danger, the interdependence of the system, use of methodology FMEA (Failure Mode Effect Analysis), event tree, damage severity table, the relation of damage severity to protection objectives, consideration of technological and human barriers, utilisation of barriers (including human intervention) and acceptability of residual risk table (see also [13]).

We used the MOSAR method because of its capacity to address the detection of dysfunctions, inappropriate functioning, and risk management in complex systems. This method is particularly valuable due to its structured framework, which incorporates a comprehensive approach to risk analysis, and clearly defines measures and procedures for risk reduction [13]. It serves as a practical decision-making tool, enabling the identification of critical system failure scenarios and facilitating the determination of the necessary protective measures to neutralize or mitigate potential emergency events.

As stated in Refs. [1,2], key advantages of the MOSAR method include its systematic approach to risk analysis, ensuring a methodical assessment of hazard sources followed by a quantitative evaluation of associated risks. It additionally offers benefits associated with its hazard source identification technique. On the other hand, it is a time-consuming process, primarily due to the extensive hazard source identification procedure, followed by the subsequent risk calculations [2,18]. This may raise questions regarding the identification of potential hazards that could be missed during this extended process.

We identified several key risk categories encompassing technological risks, war and terrorism, natural disasters, environmental risks, cyber threats, epidemics, and human factors. Within each primary risk category, we delineated various risk scenarios. For each scenario, an evaluation was conducted based on probability and potential impact, and they were categorized within a risk matrix. Unacceptable risks were addressed and mitigated. The assessment has revealed ten major risks, all classified in the high-risk category:

1. Influence - Very High/Probability - Unlikely:
   - DTS failure
   - Construction of the transmission network
   - Poor availability of the IT system
   - Loss of key personnel
2. Influence - High/Probability - Likely:
   - Malware attack
   - Hacker attack
   - Social engineering
   - Maintenance and repair errors in DTS
   - DTS management errors

A comprehensive analysis of these major risks has guided the development of a robust set of strategies and measures, encompassing activities, security policies, instructions, and best practices.

Achieving true operational resilience requires a data-driven approach to understanding the risk severity. Based on this data, the power grid administrators can anticipate, prepare, respond, learn from emergencies and reduce their impact on business disruptions. Companies that turn resilience into a competitive advantage use their awareness of the situation during emergencies [19]. To gain a competitive advantage, companies should focus on the following:

Creating a business impact analysis and business continuity plans based on risk analysis: The Corporate Security Manager should collaborate with business and technology leaders to identify critical company functions, assess dependencies, evaluate risks, and calculate total economic costs and potential impacts of identified risk events. With this deep contextual knowledge and objective understanding of the most likely risks that could significantly impact operations, they can lead the development, maintenance and testing of business continuity plans.

Risk management is tailored to the set of systemic and operational risks: All companies are facing a range of systemic and operational risks, including those related to climate change, pandemics, geopolitical instability, war and global economic recession. To manage this pillar of risk, companies must regularly review their most likely and harmful systemic risks in connection with their strategic, reputational and financial risks.

Investing in reliable technology services: The reliable expectations of technology include always-on capabilities and/or services, unlimited capacity and flexible architectures. Reliable technology services are available when needed, run with a high-security posture and provide privacy for customers and employees. To master this pillar, companies shall continuously work on technology improvements.

Automate current and new processes and business services: Automating current and new processes and business services allows companies to adapt to extraordinary events, including new business opportunities. To become resilient, companies shall use automation to transform their activities. Technologies for process automation, new inventions, and innovative business and operational models bring to the organization a competitive advantage.

Exercise scenarios of exceptional events: Experienced employees are critical during times of crisis. To train the staff the key activities are explaining the components and significance of a business continuity plan, clarifying roles and expectations, providing information on the availability, activation of the plan and conducting practice drills.

Agility with the supply chain and customers: Companies with a proper supply chain risk management program balance timely efficiency with resilience. They can better anticipate risk, recover from possible crises and redirect the supply chain to leverage new

opportunities. To manage this pillar, companies must design supply networks that are efficient and flexible.

Flexible management of emergencies: The cross-functional emergency management team of a company leads and directs necessary measures, activities and procedures when an emergency occurs. The team's response must be adaptable, as emergencies can have advance warning, (a severe storm) or no warning at all (terrorist attack). Emergencies can last for a few hours or for several months. The crisis management team uses technology to gain situational awareness (outside and inside the company), to make critical decisions and take action as the emergency evolves. Companies should have prepared technologies for use in emergency situations. Technical leaders play a crucial role in ensuring that companies are prepared for the possible emergency.

5. Conclusion

Enhancing the resilience of critical infrastructure companies is crucial for ensuring continuous operation and minimizing the impact of disruptions. By implementing strategies such as effective risk assessment, redundancy and backup systems, collaboration, and leveraging technological advancements, these companies can enhance their resilience and better withstand and recover from disruptions.

The discovery of electricity is one of humanity's greatest inventions and society has become increasingly dependent on it. The current geopolitical situation presents important requirements for the continuity of the electricity supply. The uninterrupted operation of the power grid is necessary to avoid economic damage and household problems. Preparation is the key. The focus should be on procedures and instructions for the management of risks and the establishment of an organizational culture. The assessment of risks is a critical component of this process.

One of the limitations of our study undoubtedly lies in the fact that there might be a potential constraint regarding the comprehensiveness of hazard identification. Moreover, probabilities are determined based on past experiences and events, which may impact the risk analysis's thoroughness. It is important to be mindful of these limitations when applying the MOSAR methodology in both research and practical scenarios. To address this, we propose further research that entails a more in-depth analysis of specific systems. This can be complemented by the inclusion of qualitative research involving interviews with key figures in the electrical sector. Moreover, a comparative study among European countries can offer valuable insights into the applicability and effectiveness of the strategies employed.

Let us also point out that risk management is not perfect and even the best efforts cannot guarantee complete safety. The conditions and types of risks faced by organizations are constantly changing, making it impossible to eliminate all risks completely. Therefore, organizations must work to improve their resilience, making their operations more reliable and providing essential services to critical sectors.

Data availability statement

All data required to support the results and conclusions of our study are provided in the paper.

CRediT authorship contribution statement

Ajda Fošner: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Brane Bertoncelj:** Validation, Methodology, Formal analysis. **Tomaž Poznič:** Validation, Investigation, Formal analysis, Data curation, Conceptualization. **Laura Fink:** Investigation, Formal analysis, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] D. Čaleta, M. Vršec, B. Bertoncelj, M. Vršec, A. Kandžič, Ž. Podgoršek, *Strokovne podlage Za Ocenjevanje Tveganj Za Delovanje Kritične Infrastrukture*. Ministrstvo Za Obrambo Republike Slovenije, 2019. https://www.gov.si/assets/ministrstva/MO/Dokumenti/Studija-SPOTKI.pdf.

[2] F. Khan, S. Rathnayaka, S. Ahmed, Methods and models in process safety and risk management: past, present and future, Process Saf. Environ. Protect. 98 (2015) 116–147, https://doi.org/10.1016/j.psep.2015.07.005.

[3] R. Cantelmi, G. Di Gravio, R. Patriarca, Reviewing qualitative research approaches in the context of critical infrastructure resilience, Environmental Systems and Decisions 41 (2021) 341–376, https://doi.org/10.1007/s10669-020-09795-8.

[4] B. Rathnayaka, C. Siriwardana, D. Robert, D. Amaratunga, S. Setunge, Improving the resilience of critical infrastructures: evidence-based insights from a systematic literature review, Int. J. Disaster Risk Reduc. 78 (2022) 103123, https://doi.org/10.1016/j.ijdrr.2022.103123.

[5] World Economic Forum, Global Risk Report, 2023. https://www.weforum.org/publications/global-risks-report-2023/in-full/1-global-risks-2023-today-s-crisis/ .

[6] Statistični Urad Republike Slovenije, Energy in Slovenia and the EU-27, 2022. https://www.stat.si/StatWeb/en/news/Index/10321.

[7] SIST, *Standard ISO 22301: 2019. Varnost in vzdržljivost - Sistem vodenja neprekinjenosti poslovanja – Zahteve*. https://ecommerce.sist.si/, 2019.

[8] J. Jasinas, P.D. Lund, J. Mikkola, Energy system resilience – a review, Renew. Sustain. Energy Rev. 150 (2021) 111476, https://doi.org/10.1016/j.rser.2021.111476.

[9] M.Z. Serdar, M. Koç, S.G. Al-Ghamdi, Urban transportation networks resilience: indicators, disturbances, and assessment methods, Sustain. Cities Soc. 76 (2022) 103452, https://doi.org/10.1016/j.scs.2021.103452.
[10] T.J. Nipa, S. Kermanshachi, A. Pamidimukkala, Identification of resilience dimensions in critical transportation infrastructure networks, J. Leg. Aff. Dispute Resolut. Eng. Constr. 15 (2) (2022). https://ascelibrary.org/doi/10.1061/JLADAH.LADR-870.
[11] A. Cardoni, S.L. Borlera, F. Malandrino, G.P. Cimellaro, Seismic vulnerability and resilience assessment of urban telecommunication networks, Sustain. Cities Soc. 77 (2022) 103540, https://doi.org/10.1016/j.scs.2021.103540.
[12] Z. Liang, Z. Xue, Y.-F. Li, D. Miao, K. Lin, Resilience: A Pathway towards High Service Reliability in Telecommunication Networks. *Findings*, 2022, https://doi.org/10.32866/001c.37263.
[13] L. Perrin, M.G. Felipe, O. Dufaud, A. in Laurent, Normative barriers improvement through the MADS/MOSAR methodology, Saf. Sci. 50 (7) (2012) 1502–1512.
[14] D.-C. Felegeanu, V. Nedeff, M. Panainte, Analysis of technological risk assessment methods to identify definitory elements for a new combined/complete risk assessment method, Journal of Engineering Studies and Research 9 (3) (2013) 32–43.
[15] I. Prezelj, Z. Košnjek, M. Bugeza, D. Kopše, F. Križanič, V. Kolšek, Elektroenergetska Kritična Infrastruktura V Sloveniji: Scenariji Izpadov Električne Energije, FDV, 2017.
[16] ELES, Načrt Zaščite in Reševanja Ob Naravnih in Drugih Nesrečah: NZR, Issue 3 PU, vol. 3, 2021, p. 18, 2021, https://www.eles.si/Portals/0/Documents/Nacrt_zascite_in_resevanja_ELES_d-o-o.pdf?ver=2021-04-16-141354-063.
[17] W. Qiao, E. Huang, H. Guo, Y. Liu, X. Ma, Barriers involved in the safety management systems: a systematic review of literature, Int. J. Environ. Res. Publ. Health 19 (15) (2022) 9512, https://doi.org/10.3390/ijerph19159512.
[18] J. Ge, K. Xu, C. Wu, Q. Xu, X. Yao, L. Li, X. Xu, E. Sun, J. Li, X. Li, What is the object of safety science? Saf. Sci. 118 (2019) 907–914, https://doi.org/10.1016/j.ssci.2019.06.029.
[19] Y. Sheffi, The Power of Resilience: How the Best Companies Manage the Unexpected, The MIT Press, 2015.