УДК 004.05, 006.015.8, 519.718, 519.876.2
doi: 10.21685/2307-4205-2024-3-15

AN INDEX-BASED METHOD FOR INTEGRAL ESTIMATION OF REGIONAL CRITICAL INFRASTRUCTURE RESILIENCE USING FUZZY CALCULATIONS (PART 2. RESILIENCE CAPACITY MODELS AND BACKBONE CAPABILITIES)

A.V. Masloboev

Putilov Institute for Informatics and Mathematical Modeling of the Federal Research Centre "Kola Science Centre of the Russian Academy of Sciences", Apatity, Russia
Institute of North Industrial Ecology Problems of the Federal Research Centre "Kola Science Centre of the Russian Academy of Sciences", Apatity, Russia
masloboev@iimm.ru

Abstract. *Background*. The study is aimed at developing well-known and designing novel models and methods for decision support in the field of security and resilient operation management of critical infrastructures and socio-economic facilities in the Arctic region of Russian Federation. This urgent problem is especially relevant at the regional level in terms of the need to protectability heightening of critical facilities/infrastructures, cascading effects restricting of the multiple threats of various nature on higher-level systems and favorable conditions providing for mitigation of the negative consequences of influencing factors on the performance of the elements of these systems. *Materials and methods*. For easy understanding, the work structurally is decomposed in two parts. In the first part, a formal problem statement is given. The substantiation of mathematical apparatus for problem-solving is carried out. The generic framework of the developed method for assessment and analysis of the regional critical infrastructures resilience based on a fuzzy-set approach and expert judgements is proposed. In the second part, the efficiency Q-function computational models of the organizational and technical systems resilience, such as anticipation ability, responsiveness, recoverability and adaptability, which are the central elements of the optimization model of critical infrastructures resilience integral index, are examined. *Results and conclusions*. An index-based method for the integral estimation and analysis of the regional critical infrastructures resilience, based on fuzzy calculations of the level and ratio of aggregated reliability, security and robustness indices, has been developed. The method allows on basis of incomplete data to quantify systemic risks affecting the critical infrastructure resilience, performances, savings and possible losses under sampling and implementing the anti-crisis measures at all stages of the resilience management lifecycle. A distinctive feature of the method is its universality, i.e., applicability to all types of critical infrastructures. The method can be practically used by operators and analysts of regional situational centers to train and generate design decisions for counteracting the actual threats and local failures in the operation of regional critical infrastructures under uncertainty.

Keywords: system analysis, resilience, security, critical infrastructure, integral performance index, expert judgement, fuzzy calculations

Financing: the work was carried out within the framework of the State Research Program of the Putilov Institute for Informatics and Mathematical Modeling KSC RAS (project No. FMEZ-2022-0023).

For citation: Masloboev A.V. An index-based method for integral estimation of regional critical infrastructure resilience using fuzzy calculations (Part 2. Resilience capacity models and backbone capabilities). *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2024;(3):130–156. (In Russ.). doi: 10.21685/2307-4205-2024-3-15

ИНДИКАТОРНЫЙ МЕТОД ИНТЕГРАЛЬНОЙ ОЦЕНКИ ЖИЗНЕСПОСОБНОСТИ РЕГИОНАЛЬНЫХ КРИТИЧЕСКИХ ИНФРАСТРУКТУР НА ОСНОВЕ НЕЧЕТКИХ ВЫЧИСЛЕНИЙ (ЧАСТЬ 2. МОДЕЛИ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ЖИЗНЕСПОСОБНОСТИ)

А. В. Маслобоев

Институт информатики и математического моделирования имени В. А. Путилова
Кольского научного центра Российской академии наук, Апатиты, Россия
Институт проблем промышленной экологии Севера
Кольского научного центра Российской академии наук, Апатиты, Россия
masloboev@iimm.ru

Аннотация. *Актуальность и цели.* Исследование направлено на развитие известных и разработку новых моделей и методов поддержки принятия решений в области управления безопасностью и устойчивым функционированием критических инфраструктур и социально-экономических объектов Арктической зоны Российской Федерации. Эта задача особенно актуальна на региональном уровне с точки зрения необходимости повышения защищенности критически важных объектов/инфраструктур, сдерживания каскадных эффектов воздействия множественных угроз различной природы на системы более высокого уровня и обеспечения благоприятных условий для смягчения негативных последствий влияющих факторов на состояние работоспособности элементов этих систем. *Материалы и методы.* Работа состоит из двух частей. В первой части дана формальная постановка задачи, приводится обоснование математического аппарата для ее решения и представлена общая структура разработанного метода оценки и анализа жизнеспособности региональных критических инфраструктур на основе нечетко-множественного подхода и экспертных оценок. Во второй части исследуются вычислительные модели целевых функций качества устойчивости организационных и технических систем таких, как упреждаемость, реактивность, восстанавливаемость и адаптируемость, являющихся центральными компонентами оптимизационной модели интегрального показателя жизнеспособности критических инфраструктур. *Результаты и выводы.* Разработан индикаторный метод интегральной оценки и анализа жизнеспособности региональных критических инфраструктур, основанный на нечетких вычислениях уровня и соотношения агрегированных показателей надежности, безопасности и устойчивости. Метод позволяет на основе неполных данных количественно оценить системные риски, влияющие на жизнеспособность критической инфраструктуры, полезные эффекты и возможные потери при выборе и реализации антикризисных мер на всех стадиях жизненного цикла управления устойчивостью. Отличительной особенностью метода является его универсальность, т.е. применимость ко всем типам критических инфраструктур. Метод может быть использован операторами и аналитиками региональных ситуационных центров для подготовки проектных решений по противодействию актуальным угрозам и локальным сбоям в работе критических инфраструктур региона в условиях неопределенности.

Ключевые слова: системный анализ, жизнеспособность, безопасность, критическая инфраструктура, интегральный показатель, экспертная оценка, нечеткие вычисления

Финансирование: работа выполнена в рамках государственного задания ИИММ КНЦ РАН (НИР № FMEZ-2022-0023).

Для цитирования: Маслобоев А. В. Индикаторный метод интегральной оценки жизнеспособности региональных критических инфраструктур на основе нечетких вычислений (Часть 2. Модели показателей качества жизнеспособности) // Надежность и качество сложных систем. 2024. № 3. С. 130–156. doi: 10.21685/2307-4205-2024-3-15

Introduction

Nowadays, risk reduction, security ensuring and the resilience improvement of the critical entities and infrastructures are still major problems in management of regional socio-economic and organizational systems. This is confirmed by a number of legislations and state protection programs adopted at the highest official level both in our country and abroad, e.g.[1], etc. In the last fifteen years, foreign security policies

[1] Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: http://static.kremlin.ru/media/acts/files/0001201707260023.pdf ; Приказ ФСТЭК России от 06.12.2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации». URL: http://publication.pravo.gov.ru/document/0001201802090010 ; Директива Совета Европейского Союза 2008/114/ЕС от 8 декабря 2008 г. «О Европейских критических инфраструктурах и мерах по их защите». URL: https://base.garant.ru/70333008/ ; Директива Европейского Парламента и Совета Европейского Союза 2022/2557 от 14 декабря 2022 г. «Об устойчивости критически важных организаций». URL: https://base.garant.ru/407633886/

have shown an onrush shift from the protection of critical infrastructures towards the resilience of critical entities. In Russia such a conversion is more regular and step-by-step in nature, and the focus shifting in the field of safety practices is still in progress, but deems very challenging. Global rethinking protection of critical infrastructures in the context of system resilience at the technological and political levels suspects concentrating the activities more on maintaining the essential functions which the critical infrastructures provide by adding improved absorptive, restorative and adaptive capacities or other control features, along with preventing and reducing threat, vulnerability and impact of numerous hazards by traditional management facilities. Thus, the resilience concept is a refocus from protection (security) to adaptation and recovery of the critical infrastructure systems. Reputable experts define the resilience concept as an extension of modern safety studies, namely the risk analysis and assessment, and position it as a new era of risk management, even though this concept contested and ambiguous in some cases is. Consequently, critical infrastructure resilience is a recent trend of the safety sciences conditioned by the current worldwide geopolitical situation, and its popularity has increasingly exploded in both academic and policy discourses.

From the system of systems approach perspective the critical infrastructures is commonly understood as distributed, multi-level, highly dynamic complex systems that are comprised of the interdependent subsystems, which themselves may be large-scale, compounding and multifaceted, and operate in an emergent or synergistic manner. This means that considered class of systems have unique properties, such as large number of interacting components, emergent properties difficult to anticipate from the knowledge of single components, adaptability to absorb random disruptions, and highly vulnerability to widespread failure under adverse conditions. Accounting of these capacities is important when examining overall resilience of critical infrastructures. In accordance with[1], a critical infrastructure is defined as an "asset, system or part thereof located Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions". Considering the complexity and interconnectivity, it is obvious that critical infrastructures are highly vulnerable systems to and may be threatened by multiple hazards and disruptions of various natures.

Resilience is characterized as an immanent and relevant, but abstract system property of its self-preservation, because of the exponential growth (in number and dependence) of the internal and external threats and hazards that directly or indirectly may affect critical infrastructure performance. In turn, the loss of essential functionality of critical infrastructures due to adverse events may hurt the well-being of the society in tote. More formally, resilience is defined as the ability of a critical infrastructure system, facility or asset to anticipate/prevent, absorb/withstand, respond to, recover from and adapt to a potentially disruptive event, shock, threat or a changing environment within acceptable losses of functionality, cost and time, which should be as minimum as possible. In other words, resilience is the ability to reduce the magnitude and/or duration of disruptive events, and to cope with future risks. Broadly speaking, a resilient critical infrastructure refers to a system capable to subsist under anticipated and unpredictable events by efficiently planning, reducing vulnerability, absorbing and minimizing the consequences of multiple threats, quickly recovering and adapting all its elementary functions and structures. However, resilience concept is used in different contexts and composed of several dimensions that are related to a specific resilience management strategy each, which addresses to areas of control and actions that can be implemented in order to increase the various aspects of critical infrastructure resilience.

Despite the resilience concept has become well studied and better understood among system engineers, risk managers and owners/operators of critical infrastructures, there is still a lack of consensus regarding its formal unambiguous definition, as well as consistency and accuracy in its measurement by "one number". The absence of a common framework and standardized metrics for measuring the critical infrastructure resilience undermines the effectiveness of decision-making in the field of resilience management and situational control in the face of potential threats and uncertainties caused and triggered by disruptive events or dynamically changing environment. For the purpose of providing adequate and efficient situational management, the critical infrastructure resilience should be assessed all-round before, during and after the occurrence of disruptive events. Implementation of the proper preventive actions and protective measures on the basis of these assessments will improve system resilience, lead to useful effects and savings, as well as optimize system performance and functionality level. Thus, considering these issues, a holistic, transparent and easy-to-use methodology for comprehensive assessment and analysis of critical infrastructures resilience – from withstanding specific threats and mitigating negative impacts to eliminating post-event consequences and returning to normal operation conditions, as well as to support decision-making for risk management, is imperatively needed.

[1] Директива Совета Европейского Союза 2008/114/ЕС от 8 декабря 2008 г. «О Европейских критических инфраструктурах и мерах по их защите». URL: https://base.garant.ru/70333008/

Therefore, the aim of this study is to develop computable methods for integral estimation of the critical infrastructure resilience and to perform an analysis of resilience backbone capabilities, as well as to select appropriate resilience capacity models relevant and suitable for combined use within the proposed assessment procedures. Background is based on a systematic literature survey of current methodologies for evaluation of resilience concept, which enable its operationalization to critical infrastructures, and summarizing benefits and drawbacks of the existing approaches for the assessment and control of critical infrastructure resilience. Most of the state-of-the-art frameworks and methodologies reviewed in the first part of this study [1] are based on indicators (quantitative, semi-quantitative or qualitative criteria), simulation, expert judgments and fuzzy calculations. Four resilience capacities, i.e. resistive, absorptive, restorative and adaptive, are the target objectives of these approaches and are closely related with the different stages of typical resilience cycle [2]. All these resilient system capabilities (resistivity, absorbability, recoverability, adaptability) are poorly formalizeable, quantifiable and manageable, and, thus, require detailed analysis and consideration.

This article being a logical continuation of the study [1], where a generic framework of the proposed index-based method for integral estimation of the critical infrastructure resilience based on fuzzy calculations has been developed, is organized as follows. Section 1 outlines briefly related work and the background of the study. In section 2 the backbone resilience capabilities and dynamic characteristics of critical infrastructures are systematized and analyzed. Section 3 encompasses the applicable computational models of the resilience capacities, which are the central components (Q-functions) of the general estimation model of critical infrastructure resilience integral index. Finally, conclusions are drawn and the future research directions are highlighted.

Background and Related work

The resilience concept in the context of critical infrastructures has evolved from existing disciplines in other fields and is related to the foundations of risk, reliability and security. For a system to be characterized as resilient, it is important to be able to bring the system back to its original state or an adjusted state, as well as to provide a minimum service level while undergoing changes or facing disturbances [3]. According to [3], resilience is defined as the overarching goal of a system to continue to function to the fullest possible extent in the face of stress to achieve its purpose, where resilience is a function of both the vulnerability of the system and its adaptive capacity. Disruptive events and crises that start in one critical infrastructure can spread through a network of critical infrastructures, affecting them also and other sectors of socio-economic systems. According to [3], two resilience types are distinguished: internal resilience (the resilience level of the critical infrastructure, where the triggering event occurs) and external resilience (the resilience level of the rest of the external involved critical entities).

The majority of the available approaches for studying resilience are only resilience analysis methodologies. The subsequent stage of resilience evaluation is often missing, and where it is present then it is only in the form of a comparison of the resilience of the organization, asset, or system in question with other comparable objects. Thus, the evaluation is reduced to a simple comparison with ones peers. The implementation of resilience concepts to critical infrastructure on this basis seems to be rather arbitrary and this points towards the need for a framework for assessing resilience which includes some sort of evaluation process based on the needs and requirements of stakeholders of the critical infrastructure, including dependent entities, governments and the society which the critical infrastructures serve. The elaboration of this framework is one of the objectives of the current study, however, the intention is that it will be able to incorporate the results from all of the analysis methodologies reviewed.

Resilience assessment is a process for knowing its value or level by applying appropriate steps [4]. To evaluate the resilience of critical infrastructures, different metrics and definitions are discussed in up-to-date academic literature. Thereto, the commonly used approaches are qualitative, quantitative, hypothetical and empirical methods based on diverse data. However, these methods are limited to the availability of information, subjectivity of the responses provided, to a specific critical infrastructure or scenario and lack in generalization [5]. While conducting academic literature review, it is found that there are several models and tools exist for evaluating and measuring resilience. However, there are a rather limited number of freely available frameworks, and only limited information about them is publicly available. Moreover, they tend to cover specific domains/dimensions of resilience, and are sectorally limited to a specific type/class of critical infrastructure or territorially limited to a region/country.

Findings reported in [2, 6] give the following definitions for various stages in a resilience assessment framework, which are based on the similar definitions for risk assessment[1]:

[1] ISO 31000:2018 Risk management – Guidelines. 2nd Edition. Switzerland, International Organization for Standardization, 2018. 24 p.

– *Resilience analysis* is the process to comprehend and to determine the level of resilience based on selected resilience indicators.

– *Resilience evaluation* is the process of comparing the results of resilience analysis with criteria or objectives to determine whether resilience level is acceptable and identify areas for improvement.

– *Resilience assessment* is the overall process of resilience analysis and evaluation.

There are many proposed methods for resilience assessment and analysis, some of which are directly targeted to critical infrastructures and few others long-listed in [1], which may apply to critical infrastructures. These estimation methods differ considerably in their background, focus and application. While a few of them are already in operational use, others exist only as theoretical and methodological models. The output of all of the methods is also expressed differently and the question remains what should be done with the calculated resilience of critical infrastructure. The following frameworks for evaluating resilience of critical infrastructures have been considered in [1]: Critical Infrastructure Resilience Indicator (CIRI), Resilience Management Index (RMI), Benchmark Resilience Tool (BRT), Guidelines for Critical Infrastructures Resilience Evaluation ("Guidelines"), Organisational Resilience Health Check (ORHC), Resilience Analysis Grid (RAG) and the "Swiss approach". A generic conceptual framework for analysis and assessment of critical infrastructure resilience is schematically represented in Fig. 1.

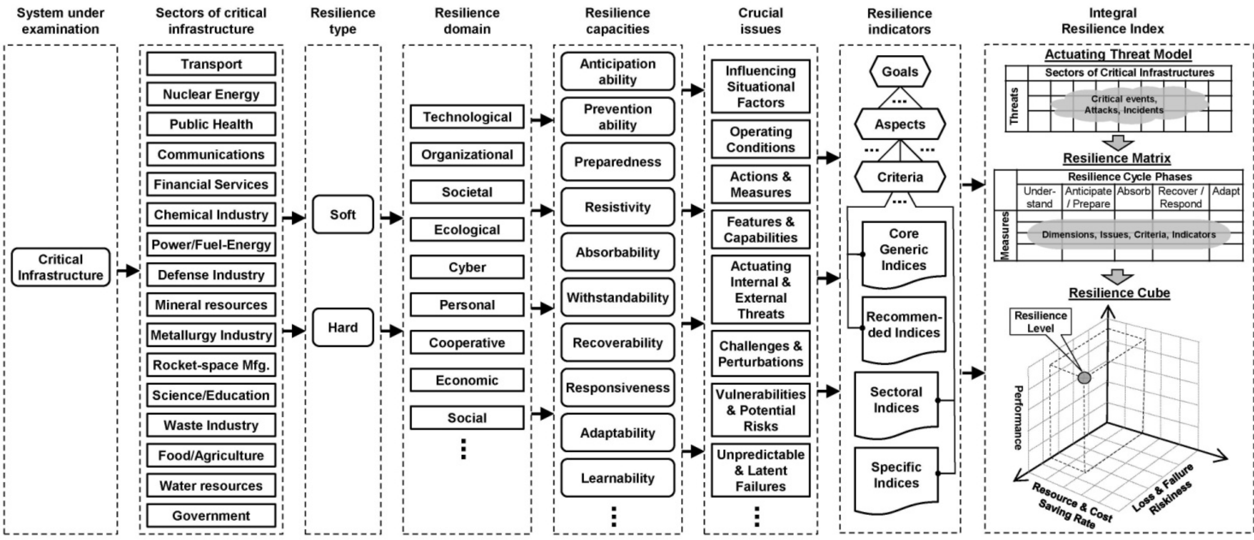

Fig. 1. The conceptual framework for analysis and assessment of critical infrastructure resilience

The broadly used and named above methods in science and practice of resilience assessment of critical infrastructures are mostly based on indicators [4]. Indicator, being a less abstract concept than resilience, can be used to show positive or negative changes in resilience. Therefore, the index-based resilience assessment could help stakeholders to analyze critical infrastructures on a practical and situational basis and to make efficient decisions. The identification of indicators is considered key before assessing resilience. These indicators exist already as safety or risk indicators, and are mainly taken from official statistics, reports and standards, current guidelines and practices, etc. They are based on historical and on-line data or expert judgements that are produced under strict quality assurance. Values of the indicators from any of the above sources can be numerical, fuzzy or non-numerical and in a general case need to be transferred into the single crisp score on a common relative or interval scale when applying resilience assessment procedure (selecting, measuring, weighting and aggregating the indicators). Therefore, the main challenge of resilience assessment is to transform expert knowledge and data into actionable measures by the means of indicators [4].

Resilience indicators are related to measurable variables that can be used, either alone or in combination, as a formal representation of resilience. Qualitative, semi-quantitative or quantitative indicators are analyzed and, when sufficient, aggregated to a measure of resilience. The resilience indicators should be clearly defined, in order to ensure objectivity and a proper balance between generality and specificity. To monitor resilience over time or comparing to similar critical infrastructures, the indicators must also provide reproducibility and repeatability. Measurement scales for the indicators and their possible weight factors should ideally be benchmarked at a sectoral level. Based on literature and defined requirements from critical infrastructure operators associated with regional situational centers, the resilience indicators to be included in the overall resilience assessment need concerted selection and optimization actions, because they relate to the different resilience domains and issues. Indicators and criteria are an important part of various analysis methodologies used for resilience assessment.

Obviously, the more indicators are chosen to measuring resilience, the better the coverage of an issue (anything important in order to be resilient against severe threats) is going to be, but it is also obvious that the larger the number of indicators, the more complex their handling is going to be [7]. The way out has two possible directions suggested in [7]:

– finding the right number of indicators relevant to the resilience problem tackled (in practice, the more critical the situation, the smaller the number of indicators recognized and managed by operators, i.e. in absolute emergency situations operators can hardly look at more than 5–7 indicators, and in preplanned situations – 120–150 indicators are usually a maximum);

– allowing to drill-down in cases when one or more indicators need further explanation.

Resilience assessment has become convenient and common tool for resilience management, as assessment results provide useful information to critical infrastructure managers for reasoned decision-making. However, resilience assessment of critical infrastructures is facing challenges of being practical to use on the operational level of risk management [8], where there is often no or minimum time to respond to the disruptions, impacts and perturbations. Most existing resilience assessment methodologies make both general and specific criteria generalization quite complicated. Although these methodologies are diverse and multidisciplinary, they have some several common limitations. Besides, these methodologies are not comprehensive enough.

As substantiated in [8], the current lack of thinking about spatial and temporal interactions across the network of critical infrastructures prevents designing beneficial actions and suppressing dangerous ones. A critical event often causes cascading effects while optimization measures could lead to side effects. In addition, the vagueness existing recently in critical infrastructure resilience definition makes it difficult to develop generalizable indicators or criteria for resilience assessment. At once, each critical infrastructure adverse event has uniqueness, but only few existing criteria are specific enough to fully correspond to concrete situations aimed by different critical infrastructure stakeholders. It results that most resilience assessments for critical infrastructures cannot make the resilience concept usefulness at the operational level of risk and emergency management.

Some review studies on critical infrastructure resilience assessment [2, 4–6, 8–13] assign the different criteria, dimensions and aspects of resilience that existing estimation methods are currently focused on. However, most of the state-of-the-art studies for resilience analysis of critical infrastructures do not discuss assessment criteria, even though they are focused on dimensions or perspectives, such as capacities, capabilities and characteristics, could be further developed and translated to criteria. Therein, as declared in [8], without assessment criteria critical infrastructure operators have practically no envisaged positive outcomes of estimation results. During assessment processes, a target criterion is the desired direction of selected objective information, i.e. an index that is used to monitor the evolution of a specific aspect of the issue dealt with. Estimates consisting of criteria and indices provide a commonly agreed framework for articulating and defining targets and expectations, developing management methodologies, best practices and performance elements, and are then used in monitoring and evaluating attainability of those expectations and targets [8].

Generally, the weighted aggregation process for resilience criteria and indicators within the adjusted assessment method [1] rely on a conceptual hierarchical structure shown in Fig. 2, which is traditionally used for analyzing and modeling of complex systems.

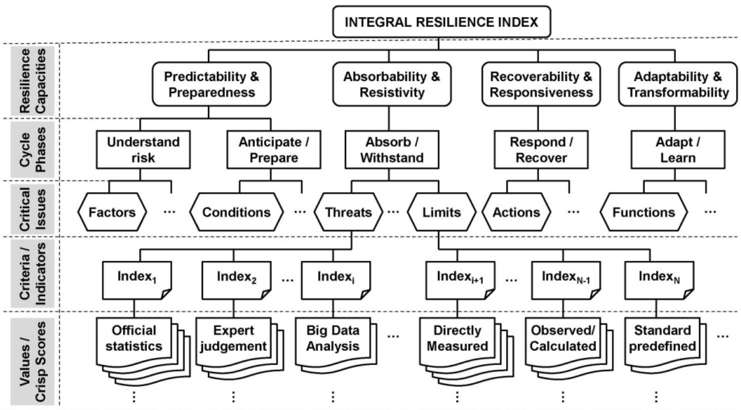

Fig. 2. The general structure of the typical index-based methodology for measuring the overall resilience of critical infrastructures based on the bottom-up weighted average aggregation

Developing generalizable criteria for resilience assessment is a current challenge to turn resilience into operational tools, i.e. resilience operationalization, because the existing formulations and theoretical models of resilience are multitude and different, but, nevertheless, are very valuable. Several studies, like [8, 14], insist that for resilience theory to become practical, it is necessary to consider not only the cost-effectiveness and negative effects of the critical infrastructure operation, but also the uniqueness of each situation. According to researches [8, 14], the operationalization of resilience concept to critical infrastructures refers to making a theory have practical and operational significance, transforming a theory into an object of practical value, regarding in the broader sense of using a theory for different purposes. Therefore, the proposed method [1] allows a wide margin of autonomy for managers and policymakers, who have the responsibility for maintaining critical infrastructure resilience and need support and guidance to operationalize the resilience-maintaining process. The adjusted method [1] is based on the multi-criteria evaluation/optimization framework similar to [7, 8, 14] and provides a regular step-by-step multidimensional aggregated assessment of positive and negative aspects, including influencing situational factors, which can better help critical infrastructure operators to make ad-hoc decisions that are better informed and profitable. It is worth noting that the usefulness and effectiveness of multi-criteria assessment approach to safety and resilience management problem-solving, as well as for the other multidisciplinary applications and issues [3, 15] have been already proofed by reputable researchers all over the world.

Thus, it is necessary to design a more complete methodology to cover the various aspects relevant to critical infrastructure resilience for the practical issues of its in-depth understanding and management. While resilience maintenance of critical infrastructures is very time and resource consuming, regular assessment and gap analysis of the functionality level of critical infrastructures exposed to disruptive events is a best practice of reacting to urgent problems as they arise, as well to planning and implementing protective measures for the future risks, and at the expense of this provide critical infrastructure system performance improvement or adaptation.

Critical infrastructure resilience backbone capabilities

In the first part of this study [1], a systematic view on resilience backbone capabilities of critical infrastructures as its target indicators used at different levels of the index-based hierarchical estimation model of the overall system resilience, has been proposed. Now, let's focus closely at the physical meaning of these key elements of the multi-level metrics system for aggregated assessment of the critical infrastructures resilience. Based on the detailed analysis of state-of-the-art literature surveys of the resilience measurement methods and frameworks [2, 3, 6, 9–11, 15, 16], the following main resilience capabilities inherent both to soft (socio-economic systems) or hard (engineering systems) resilience types and the most of resilience domains (technological, organizational, ecological, cyber, etc.) can be conditionally distinguished:

– ***Reliability*** is "the ability of the system to maintain its required capacity and performance during a given period of time (or mission time) under stated operating conditions" [17]. In other words, for critical infrastructures this means the capability to implement the needed performance under certain conditions and over some time without loss of performance. When the critical infrastructure is in a normal state (before a disruptive event), reliability provides its essential function. The aim of *absorptive*, *adaptive*, and *restorative capabilities* is to enhance the critical infrastructure reliability degradation due to disruptive events. *Reliability* focuses on avoiding disruptions, while resilience also counts the critical infrastructure recovery. Therefore, *reliability* and *recoverability* are complement and greatly related to the critical infrastructures resilience.

– ***Maintainability*** is "the ability of an item under given conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources" [18]. *Maintainability* is a measure of how easily the critical infrastructures are repaired to a specified condition. In practice, *recovery speed* or *recovery time* is mostly used to quantify critical infrastructures maintainability. Therefore, if the time required to recover the critical infrastructure is short, it indicates proper critical infrastructure maintainability. The aim of *absorptive*, *adaptive*, and *restorative capabilities* is to increase the ease of critical infrastructure recovery by reducing the critical infrastructure damages caused by disruption or adverse events.

– ***Supportability*** is the critical infrastructure "ability to be supported to sustain the required availability with a defined operational profile and given logistic and maintenance resources"[1]. This capability refers to the intrinsic features of the critical infrastructures that facilitate efficient and effective support of the

[1] ГОСТ IEC 60050-191 International Electrotechnical Vocabulary (IEV). 2017. 149 p.

critical infrastructures throughout its life cycle [19]. *Resourcefulness* and *mean time to support (service)* are often used as a measure of system supportability. *Supportability* is heavily influenced by logistics considerations, such as *spare parts*, *personnel availability*, strategic resources, test equipment and tools [20]. *Supportability* can be characterized as *planned* (preventive) or *unplanned* (corrective) *maintenance* activities. At once, according to study [21], the system ability to support the mission objectives includes passive and active supportabilities. Passive supportability refers to the *resource provision* (e.g., *spare parts*) at the system design phase. On the other hand, active supportability refers to the *resource allocation* at the system operational phase (e.g., *spare parts transportation speed*). Thus, passive and active supportabilities affect the critical infrastructure supportability in tote. Supportability is a characteristic that influences the availability.

– ***Availability*** is the critical infrastructure "ability to be in the state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided"[1]. This critical infrastructure ability depends on the combined aspects of reliability performance, maintainability performance and maintenance support performance. Operational availability of critical infrastructures is formally defined as the critical infrastructure uptime ratio to the total critical infrastructure uptime and downtime. Thus, the critical infrastructure availability refers to the portion of time that the critical infrastructure can be used. The operational availability is generally used as a performance measure for a given system.

Reliability, maintainability, supportability and availability refer to the technical aspect of critical infrastructures resilience. In addition, managers need another measure to evaluate resilience from the organizational aspect.

– ***Organizational resilience*** considers the resilience of the critical infrastructure owner. It plays an important role in the critical infrastructure resilience. Applying this measure helps organizations to be able to deal effectively with hazards, especially when the situation is very uncertain and unstable [22]. Organizational resilience includes all actors involved in resilience management of critical infrastructures, such as resilience analysts, experts, personnel, managers and operators of situational centers. The general purpose of organizational resilience is to enhance organizational management performance in the face of irregular conditions and to provide an efficient problem-solving mentality at the organizational level of resilience control hierarchy. In [22] the organizational resilience is estimated using internal processes of an organization, including risk management, innovation, learning and design processes, which provide the proper conditions for critical infrastructures to adapt to disruptions.

– ***Prevention ability (predictability)*** refers to the early warning, anticipation and detection ability of disruptions and adverse events in the critical infrastructures and directly affects the critical infrastructures *recoverability*. In [14], the Prognostic and Health Management (PHM) system is used as a useful tool for prediction multiple threats and pre-event early warning. The PHM system assesses the critical infrastructures current state by monitoring facilities, anticipates potential defects by analyzing the monitoring data and assists in the proper management of critical infrastructures throughout their life cycle [14]. Early warning and predictability provide timely information to implement efficient response measures against disruptive events. Therefore, it can positively affect the dedicated costs and time for the critical infrastructures recovery process. Resilience can be described as a function of reliability and restoration, where *restoration* is defined as "the ability of an engineered system to restore its capacity and performance by detecting, predicting, and mitigating or recovering from the system-wide effects of adverse events" [17]. *Restoration* or *recoverability* can be considered as the degree of reliability of the restoration, formulated as the joint probability of a system failure event, a correct diagnosis event, and a correct prognosis event, and a mitigation/recovery action success event [17]. Hence, by knowing the actual condition of the system (diagnosis), one can estimate the maintenance and support that is needed (prognosis), and thus, the *repair/recovery time* can be optimized.

– ***Absorbability (absorptive capacity)*** is the degree that the critical infrastructure can absorb the negative impact of the disruptive event automatically. This capability is often considered as an immanent critical infrastructure characteristic to minimize the disruptive effects of the adverse events. Absorptive capacity includes a set of proactive actions that should be implemented in the critical infrastructure preparedness phase. Robustness is commonly used to quantify the adsorptive capacity of critical infrastructures.

– ***Redundancy*** refers to the degree to which critical infrastructure or its elements exist that are interchangeable and can meet functional needs in the presence of adverse events, degradation or inoperability.

[1] ГОСТ IEC 60050-191 International Electrotechnical Vocabulary (IEV). 2017. 149 p.

Redundancy creates alternative functions for the critical infrastructure items operation under disruption and its goal is to achieve a robust critical infrastructure. *Redundancy* increases the absorptive capacity of critical infrastructures. In addition, the redundancy is also related to backup resource and asset diversity. To provide backup for the replacement of failing functionality both *internal* and *external redundancy* can be used.

Thus, discussed key system resilience capabilities influence the recoverability (restorative capacity) and responsiveness of critical infrastructures.

– ***Recoverability*** is the ability of a system or critical infrastructure to restore its capacity and performance promptly by recovering from the negative effects of adverse events during a period of time under certain conditions using the available resources required to perform the adequate recovery actions. *Recoverability* is formally defined as the probability that a failed critical infrastructure element or system as a whole recovers quickly to perform the required functions at given time.

– ***Responsiveness*** is the ability of critical infrastructure to understand and carry out its tasks in a timely manner. Responsiveness refers to the way the system reacts quickly and effectively to a wide range of disruption events within possible modes of system operation as they occur.

– ***Restorative capacity*** is the degree to which the critical infrastructure can effectively restore its damaged performance and is typically affected by available budget and resources. Therefore, this capacity is affected by the critical infrastructure supportability. Restorative capacity provides permanent solutions to damages caused by the disruptions. Rapidity is commonly used to quantify the restorative capacity of critical infrastructures. The cost of restorative capacity is much more than an adaptive capacity.

– ***Adaptability (adaptive capacity)*** is the self-organization degree to the new conditions and changes, to which the critical infrastructure can arrange itself and use temporary and often non-standard actions to prevent critical infrastructure downtime during and after the disruption events. This capacity can prevent sudden collapses in the critical infrastructure performance level, but these actions have a temporary nature and for the critical infrastructure performance recovery permanent actions should be taken as soon as possible.

– ***Learnability (learning capacity)*** is the degree to which the critical infrastructure can learn from the occurred disruptions to prevent similar future events. The obtained experience and knowledge from past events can be incorporated for future iterations.

A graphical interpretation of the physical meaning of system resilience capabilities at different phases of the critical infrastructures resilience management cycle is shown in Fig. 3.

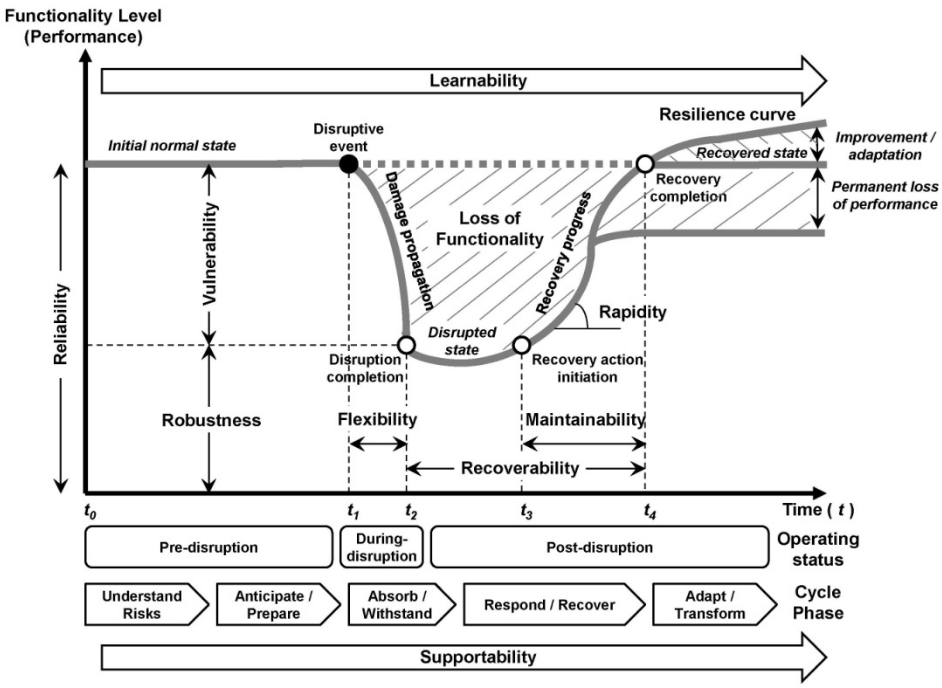

Fig. 3. The physical meaning of critical infrastructure resilience capabilities at different phases of the resilience management cycle (adapted from [9]).

Specification of the given resilience capabilities is structurally proposed in Tables 1–4. It should be noted that all the resilience capabilities are much interconnected and complementary.

Table 1

Characteristics determining the preventive capacity of critical infrastructure resilience

Resilience capacity	**Characteristics / Indicators**	**Description & Definition of capabilities**
Anticipation ability & Resistance	Preparedness degree	An extent that characterizes the available set of facilities and assets, as well as on-the-shelf strategies, response plans and actions for implementing and executing the precautionary measures relevant to the system in the face of potential disruptive events and emergency situations influencing critical infrastructure resilience. In other words, the state of critical infrastructure of being ready for the occurrence and impact of disruptive events (e.g., failure, error, critical situation, crisis, etc.). Preparedness is defined as "a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective active in an effort to ensure effective coordination during incident response" and includes a checklist of protective measures relevant to implementation in the current situation, i.e. a set of the analytical-planning documents to increase the preparedness of critical infrastructure elements for adverse events. As a measure of preparedness can be the resource intensity of forces and means to reduce the effects of disruptions
	Reliability	This capability was described above
	Detection ability	Probability and/or time of identification of the disruptive events
	Prognostic & Health Management (PHM)	This capability was described above
	Planned Maintenance	The percentage of time that the critical infrastructure was dedicated to planned maintenance activities relative to the total operating time. This general metric provides insights into the efficiency and effectiveness of critical infrastructure maintenance program in ensuring optimal performance and reliability. It refers to as scheduled maintenance and focuses on minimizing the downtime and costs associated with breakdowns, as well as fault tolerance improvement
	Joint activity cooperation plan	Refers to a degree of concordance and relevance of the planned preventive measures and actions, decentralized local decisions made and implemented to the operational context and specificity of disruptive events occurred
	Protectability	Ability of critical infrastructure to be safe and preserve its essential functions under the impact of negative situational factors of various natures. The risk impact and risk probability factors determine the system protection level. A higher protectability score indicates a lower overall risk level and better protection in the face of multiple potential threats or vulnerabilities
	Operability	Ability of critical infrastructure that has the capacity and flexibility to achieve a range of operating conditions safely, reliably, profitably and with positive dynamic performance and quality, i.e. the *operability* ensures to keep the system, its units or service in a safe and reliable functioning condition that is pre-defined operational requirements. The *operability* is a measure of the resilience support of critical infrastructure through the ability to adapt and transform to restore system critical functions at the operational level, which can be achieved before all system repairs are made. In other words, the *operability* can be described as the fitness, capacity, or system ability to use to provide critical services allowing stakeholders and management entities to receive required, or near required, essential functions from a potentially impaired critical infrastructure following a disruptive event
	Sensitivity	A degree to which a critical infrastructure is vulnerable or susceptible to disruptions and threats that could impact its operation, performance, or ability to perform essential functions. As well, it describes the extent to which the dynamics of a critical infrastructure change in response to perturbations or parameter variations. Unlike robustness and flexibility, which are measured in terms of behavioral fitness, sensitivity refers only to the responsiveness of a system to perturbations. Sensitivity to perturbations can be either beneficial, detrimental, or neutral with respect to task performance, and sensitivity refers only to the magnitude of the response to a perturbation, rather than its effect on fitness [23]
	Resistance / Resistivity	The ability of a critical infrastructure and its functional elements to prevent and withstand the occurrence of the disruptive or undesirable events

Table 2

Characteristics determining the absorptive capacity of critical infrastructure resilience

Resilience capacity	**Characteristics / Indicators**	**Description & Definition of capabilities**
1	2	3
Absorbability & Robustness	Robustness	The strength or ability of critical infrastructure to resist a certain disruption level (withstand a given level of stress or demand) and absorb its primary effects without suffering degradation or significantly reducing performance (losses of functionality). A critical infrastructure with high robustness maintains its central function in a disruptive event. *Robustness* is measured by the critical infrastructure amount of residual performance after a disruption. Furthermore, *survivability*, *resistant ability* and *stability* of critical infrastructures have a similar formal definition to its robustness
	Fragility	A hazard specific indicator of the critical infrastructure performance loss function within the absorption and response phase of the system resilience life-cycle as discussed in [15]. *Fragility* of a critical infrastructure refers to the conditional probability of failure or a given level of damage conditioned on the response parameter (intensity measure), i.e. the probability of reaching or exceeding a given damage level as a function of the hazard intensity. The greater degree of damage is associated with higher fragility, and a lower robustness or reliability. *Fragility* is often used as a specific description of vulnerability
	Vulnerability	The degree of the critical infrastructures sensitivity to disruption. There is no consensus about the relationship between vulnerability and resilience, but it seems that higher vulnerability of the critical infrastructures leads to lower resiliency and vice versa.. Vulnerability is an inherent feature of the critical infrastructures, even before any disruptive event. Analyzing the vulnerabilities can help to identify the possible weak points of the critical infrastructure operation, which cause the most damage during disruption, and generate proper control strategies to fallback. The key parameters of vulnerability are: stress to which a critical infrastructure is exposed, its sensitivity and its adaptive capacity. *Exposure* is perceived as the degree to which a critical infrastructure is exposed to a given stressor. *Sensitivity* is the degree to which a stressor impacts the critical infrastructure. *Adaptive capacity* is perceived as the potential for the critical infrastructure to adjust or cope with impact
	Stress rate	A resilience measure used to determine the stability of a given item, system, critical infrastructure or any other entity when deliberately intense or thorough testing. Stress rate measurement involves testing beyond normal operational capacity, often to a breaking point, in order to observe the outcomes and consequences for the purpose of further training and enhancing the system performance in different operational conditions. Such an examination and fitness of the system resistance provide damage level and limitation exercise, as well as identifying ultimate stress limits under disruptions, deviations or disturbances
	Independency	Refers to the ability of a critical infrastructure to function autonomously and self-sufficiently without being overly reliant on external resources, dependencies, or vulnerabilities. An independent critical infrastructure is characterized by its capacity to operate independently and sustainably, even in the face of disruptions, failures, or external threats. This characteristic describes the level of autonomy and isolation of components within the critical infrastructure from each other, i.e. the degree of interdependence among these components. *Independency* of critical infrastructures is crucial for ensuring their reliability, security and resilience in performing essential functions. By identifying potential points of failure and bottlenecks, as well as reducing risks, vulnerabilities and dependencies, an independent critical infrastructure can enhance its ability to adapt to dynamically changing environment, mitigate threats and maintain the continuity of essential functions for society and the economy

End of Table 2

1	2	3
	Resourcefulness	The ability of a system to direct resources to critical infrastructure support by using, mobilizing and supplying the required resources (spare parts, finances, information, laborers, technology, etc.) to identify and solve problems under adverse event of a disturbance or shock in a prioritized manner. It describes a level of system preparedness to effectively combat an adverse event. The main destination of resourcefulness is to enhance the critical infrastructure rapidity and increase the restorative capacity of critical infrastructure
	Facilitation ability	Refers to the capacity of a critical infrastructure to support, enable and enhance the efficient and effective performing of essential functions and operational services. A critical infrastructure system with strong *facilitation ability* can streamline control processes and provide coordination of decision-making, foster creativity and innovation of resilience management, and improve collaboration and communication among its components, operators or stakeholders to address complex challenges and to ensure the reliable and continued delivery of critical services. Critical infrastructures with high *facilitation ability* are more efficient in withstanding impacts of multiple potential threats and in achieving their goals and objectives as well. Facilitation plays a key role in optimizing the performance of critical infrastructures intended for resilient economic growth, public safety and national security support
	Internal redundancy	The *internal redundancy* is provided by a part of the critical infrastructure which is always online. With no redundancy the impact of a disruptive event on the performance of critical infrastructure results in a considerable drop. The presence of internal redundancy with additional capacity within the critical infrastructure results in the lesser or minor drop in its performance under unexpected circumstances. If the critical infrastructure has a sufficient *internal redundancy*, the system performance can be restored using alternative pathways. The effect can be indirectly measured in recovery time or backup cost. A redundant critical infrastructure is expected to have lesser recovery time, but the initial backup expenses may be considerable. *Internal redundancy* contributes to robustness (insensitivity to local failure) and could be described as the means to decrease the dependence of a critical infrastructure to its components
	Safe failure	The ability of a critical infrastructure to absorb shocks and the cumulative effects of slow-onset challenges in ways that avoid catastrophic failure or irretrievable losses
	Situational awareness	The ability of decision makers and the operators of critical infrastructures to perceive, comprehend, and project relevant information in a given context, as well as their capacity to maintain a clear understanding of the current situation and respond effectively to changing conditions or risks. It enables critical infrastructure managers to aware/anticipate the information on potential threats, perturbations and adverse events in agreed manner, analyze/interpret that information within a unified context, using it to make informed decisions and implement appropriate control actions (preventive, mitigating or pro-active measures), i.e. respond effectively to impact of the changing environment and deviating operating characteristics of critical infrastructures. As a measure of situational awareness can be put forward the completeness of understanding current situation and anticipation of risks before and after the disruptive event occurred, or the entropy of the situational control data, or the response time which refers to the time it takes for critical infrastructure operators to recognize changes in the situation (risk identification) and make appropriate corrective control actions

Table 3

Characteristics determining the restorative capacity of critical infrastructure resilience

Resilience capacity	**Characteristics/ Indicators**	**Description & Definition of capabilities**
1	2	3
Recoverability& Responsiveness	Maintainability	This capability was described above. In terms of hard resilience (engineering systems) maintainability of critical infrastructures is usually associated with technological repairability of the system
	Supportability	This capability was described above
	Restoration index	A measure of how quickly critical infrastructure system can be restored to full functionality after a failure or disruption. This index is an important metric for evaluating the resilience and reliability of a critical infrastructures
	Downtime	Refers to the period during which a critical infrastructure or its components are not operational or available for use. Consideration of downtime is urgent for assessing the reliability and performance of critical infrastructures, as well as for identifying opportunities to improve uptime and minimize disruptions
	Rapidity	The ability of a critical infrastructure to return to normal operating capacity in a timely manner. It is also a rate at which a critical infrastructure can recover a satisfactory performance level. *Rapidity* refers to the critical infrastructures performance curve slope during the recovery process and is often known as the *recovery rate* of system or its elements functionality in a timely manner. *Rapidity* reflects also how quickly the spare parts can be accessed and applied to improve critical infrastructure resilience
	Safety margin	A measure of how much extra capacity or capability a critical infrastructure has beyond its normal operating requirements to ensure safe and reliable operation. It is often expressed as a percentage to indicate the level of safety buffer built into the system (critical infrastructure)
	External redundancy	The ability of a critical infrastructure to carry on providing a service in the case of failure enabled by external means. As is known from real practice, external resources are not immediately available to reduce the impact of an adverse event and they contribute to the quicker recovery of the critical infrastructure functionality. The *external redundancy* depends on availability of external reserves (services) and can be ensured by its sufficient number and capacity subject to supply rapidity with minimal cost and delay
	Modularity	Refers to the means to modular organization of critical infrastructures based on various combinations of operational units, each contributing to system performance and performing a specific system function. This characteristic of critical infrastructures is perceived as the system capacity for proper re-engineering to accommodate increasing failure or damage under contingency situations, as well as to provide flexible pathways and options for system performance enhancement by replacing the interacting components composed each other if one, or even more, fail, and by integrating new functional elements (services) if necessary. Generally, *modularity* refers to the degree to which a system can be divided into separate, independent modules or components that can be developed, maintained, and modified independently. *Modularity* of critical infrastructure system is crucial for ensuring its flexibility, scalability, and ease of maintenance
	Segregability	Refers to the degree to which a critical infrastructure system can be segregated into separate, isolated components, parts or units that can function independently without affecting each other. Segregability is important for system security, fault tolerance and scalability

End of Table 3

1	2	3
	Decomposability	Is similar to segregability of a critical infrastructure and refers to the ease with which a critical infrastructure system can be broken down into smaller, more manageable components, items or units. Decomposability is useful for critical infrastructure effective design, analysis and maintenance
	Unplanned maintenance	Refers to the corrective maintenance activities that are carried out in response to unexpected system failures, malfunctions or other crisis events that disrupt normal operation of critical infrastructures, i.e. where there is a sudden failure which was unpredicted. Unplanned maintenance is typically reactive in nature and occurs outside of scheduled maintenance plans or preventive maintenance routines. It is often necessary to address emergency situations that require immediate attention to restore the items or assets of critical infrastructures to operational status and minimize downtime. *Mean Time Between Failures* and *Mean Time to Repair* are common measures of the unplanned maintenance, which represent the average time between two consecutive failures of a system or its elements and the average time it takes to repair a system or its elements after it has failed, respectively. Both metrics can be used to estimate the general costs associated with unplanned maintenance of the functionality and operability of critical infrastructures
	Functionality	A capacity or the state of a critical infrastructure operating properly to provide a regular reliable service at, or as close as possible to, what the critical infrastructure provided prior to an adverse event. The *functionality* is a measure of the critical infrastructure resilience and is not fully restored until all system repairs are completed and operational restrictions removed
	Feasibility	Refers to ability of a critical infrastructure to be successfully implemented, operated, and maintained within the constraints of available resources, technology and time. Feasibility assessments are conducted to determine whether a proposed critical infrastructure is viable and achievable, taking into account factors such as technical feasibility, economic feasibility, operational feasibility, legal and regulatory feasibility. Technical feasibility assesses whether the necessary technology and expertise are available to develop and implement the critical infrastructure. Economic feasibility evaluates whether the benefits of the critical infrastructure outweigh the costs and if the project is financially viable. Operational feasibility examines whether the critical infrastructure can be effectively integrated into existing systems, processes and operations. Legal and regulatory feasibility considers compliance with established laws, regulations and standards. A critical infrastructure that is deemed feasible is more likely to be successfully implemented and deliver the intended benefits. Feasibility analysis is essential for identifying potential challenges, risks and opportunities early in the planning phase to ensure the successful development and deployment of critical infrastructures
	Autonomy	Refers to the ability of a critical infrastructure to operate independently or with minimal human-aided. The measurement of critical infrastructure autonomy is based on different factors such as the degree of automation, decision-making capabilities, self-sufficiency and adaptive capacity of the system, etc
	Insurance rate	A characteristic used to assess the risk level associated with the critical infrastructure and determine the premium that needs to be paid to insure its operational units against potential losses of functionality or damages. The insurance rate is typically based on such factors as the value of a system, its susceptibility to risks and the desired level of coverage
	Restart ability	Refers to the capability of a critical infrastructure system and its components to recover and resume normal operation after a failure or disruption. The *restart ability* depends on such factors as recovery time, reliability of restart procedures and the effectiveness of fault detection mechanisms

Table 4

Characteristics determining the adaptive capacity of critical infrastructure resilience

Resilience capacity	Characteristics/ Indicators	Description & Definition of capabilities
1	2	3
Adaptability & Learnability	Flexibility	The ability of a critical infrastructure to perform essential tasks under a wide range of conditions, and to convert assets or modify structures to introduce new ways of achieving essential goals, as well as to react to disruptions and adjust its internal mechanisms with the help of adaptive capacity without the consideration of any prior responses
	Technological transformability	The capability of a critical infrastructure to effect transformational change. System transformability depends on the following attributes: getting beyond the state of denial (acknowledging the need for transformational change); creating options for transformational change; having the capacity for transformative change. Such a change suspects the transition to an entirely new stability system configuration defined by new state variables, or the old state variables supplemented by new ones. To a wide extent, transformability is the ability of a critical infrastructure to create a new stability state space (configuration) for all its functional units and the new system functioning pathways under the impact of multiple internal and external threats when the operating system being unstable. The changes introduced by the transformability cascade through and may transform the whole existing system with all its constituent adaptive cycles
	Technological upgradability	The ability of a critical infrastructure to restore system functionality quickly and to adjust it to increased demands by means of replacement some system components by new or similar ones, but with different (improved) characteristics. The upgraded critical infrastructure provides a higher system performance level leading to an improved resilience. *Upgradability* regards also to data acquisition on performance and expected changes in demands. The collected data can be effectively used for upgrading the system by removing or reducing any critical weaknesses that lead to higher demands on service and maintenance. The data can also be used to make prognoses on future maintenance and support needs, and to predict when to upgrade, modify or replace the critical infrastructure components and assets
	Integrability	The ability of a critical infrastructure system to integrate external heterogeneous elements inbye and provide their communication with existing items and each other on the basis of compatible technical, organizational and normative regulations, protocols and standards
	Interoperability	The ability of critical infrastructure elements to interact (data/control exchange) with external entities and with each other based on common conceptual models and context interpretation of information for the purpose of providing completeness of situational awareness and formation of the unified information field for decision-making under joint activities
	Composability	The ability of critical infrastructure elements to interact with any other elements in a recombinant manner to satisfy requirements based on the expectation of the behaviors of the interacting parties, as well as to form a steady composition for improving system resilience
	Reconfiguration ability	Refers to the capability of a critical infrastructure to adapt, modify or reorganize its structure, components or configuration in response to changing requirements, conditions or failures. This ability allows the system to maintain functionality, performance and reliability even in dynamic or uncertain environments. Reconfiguration involves adding, modifying and removing components, changing relationships between components, adjusting parameters or switching between different operating modes. Critical infrastructures with a high reconfiguration ability are usually more resilient, flexible, and efficient

End of Table 4

1	2	3
	Personnel availability	Refers to the degree of readiness and presence of the qualified staff, operators and other essential personnel required to operate, maintain, and manage the critical infrastructure effectively. Needs of personnel skilled and trained to respond to critical events, handle disruptions, implement preventive measures, conduct repairs and risk elimination, and ensure the continuous operation of critical infrastructure assets and components. Personnel competences directly impact the ability of a critical infrastructure to respond to and recover from disruptions or unexpected events. Adequate staffing levels, proper training, clear communication protocols, effective coordination among personnel, response time, adequacy of shift schedules and coverage and skill set diversity are essential factors in ensuring the personnel availability to support the uninterrupted operation of critical infrastructures
	Spare parts availability	Refers to the accessibility and supply of essential resources (assets, materials, components, equipment, etc.) that are necessary for the operation, maintenance and recovery of critical infrastructures when needed to quickly address failures, breakdowns, or disruptions within the system. Common measures used to assess spare parts availability are resource availability rate and the mean time to repair. Additional metrics such as stock-out rates, inventory turnover, lead times for spare parts delivery, and percentage of critical spare parts in stock can also provide the estimation of spare parts availability for critical infrastructures
	Long-term/short-term reconstruction ability	Refers to the capacity of a critical infrastructure to recover and rebuild after a disruptive event or disaster, i.e. the ability of a system to bounce back from a crisis. Short-term reconstruction refers to the immediate response and recovery efforts following a disruption. It includes activities such as restoring essential services/units, repairing damaged elements of a critical infrastructure and ensuring its safety. Short-term reconstruction focuses on rapid and effective response to minimize the impact of the event and restore basic functionality to the system. Long-term reconstruction pertains to the ability of a critical infrastructure to fully recover and rebuild over an extended period of time. It involves strategic planning, policy changes, system upgrades, and more comprehensive efforts to address the underlying vulnerabilities and improve the capacity of a critical infrastructure to withstand future disruptions. Common measure used to assess the long-term/short-term reconstruction ability of a critical infrastructure is the recovery time objective and recovery point objective. Recovery time objective refers to the targeted duration within which a critical infrastructure should be restored to full operational capacity after a disruptive event. It measures the time it takes for the system to recover and resume normal operations. Recovery point objective measures the acceptable performance loss of a critical infrastructure in the event of a disruption. It defines the maximum performance that can be lost without causing significant harm to the functional units of critical infrastructure
	Self-organization ability	Refers to the capacity of a critical infrastructure to adapt, evolve and organize itself without external actions. Self-organization ability is often influenced by such factors as system complexity, diversity, coherence and feedback mechanisms. There is still no universally accepted measure for estimating self-organization ability of complex systems
	Creativity & improvisation ability	Refers to the management system capacity of a critical infrastructure to generate novel ideas and ways to solve new and existing control problems using cumulative knowledge, and utilise innovative and creative approaches to developing solutions for the purpose of adaptation of critical infrastructure components and assets to changing circumstances. The degree of creativity and improvisation of risk analysis procedures within the resilience management of critical infrastructures directly affects the effectiveness of decision-making and situational control in times of crisis and disruptive events

Critical infrastructures resilience is currently determined by capabilities represented above and their combinations that characterize different life-cycle phases of system resilience (understand risks, anticipate/prepare, absorb/withstand, respond/recover, adapt/learn) and appropriate resilience components (capacities), specifically such as anticipation and prevention ability, absorbability and responsiveness, recoverability and adaptability. In the last decade, comprehensive analysis of these resilience components has been carried out by a great number of reputable studies, but the lion's share of them was promoted abroad. In our homeland, the resilience management support of critical infrastructures is a quite new and challenging field of research, intersecting with pioneering safety, reliability and situational control fundamentals.

Generic indicators and dimensions of system resilience listed in Tables 1–4 are commonly used within the state-of-the-art estimation models and assessment methodologies for measuring the overall resilience of critical infrastructures considered in [5–7]. The choice of the specific indicators and their measure of influence on resilience under its assessment and management depends on the types of critical infrastructures, scope, context and resilience domains, as well as the subjective preferences of experts, and remains with risk-analysts or decision makers. It is worth noting that the selection of resilience metrics is typically made in relation to the class of system under study and the nature of influencing situational factors being the sources of system disturbance or shock and clearly defined.

As is declared in [24], resilience indicators can be applied in a-priori manner when assessing resilience of critical infrastructure before a disruptive event, and post-hoc manner when giving an absolute measure of the indicator that is directly benchmarked against a predetermined baseline, and estimated following some system perturbation. According to report [24], a-priori resilience indices include failure probability, critical infrastructure quality, pre-event functionality, substitutability, interdependence, extent of mitigating features; quality of planning/response under disturbance, quality of crisis communications/information sharing, security of critical infrastructure, etc. Ad-hoc resilience indices include systems failure, severity of failure, post-event functionality, post-event damage assessment, cost of reinstating functionality post-event, recovery time post-event, recovery or loss ratio, etc. The permanent increasing of complexity and uncertainty in operation of existing critical infrastructures requires regular review, updating and improvement of resilience metrics for adequate valuation and efficient management of critical infrastructure resilience. Moreover, since acting critical infrastructures are usually connected to each other and interdependencies between them exist, the quantification of critical infrastructure resilience becomes even more complex.

Next, after discussing the conceptualization of the resilience phenomena and its capabilities, let's move to the formal representation of the main resilience capacities mathematically formalized by well-known reputable resilience researchers in specific manner.

Critical infrastructure resilience capacity models

The existing index-based methods for critical infrastructure resilience assessment found and reviewed in this study are generally intended for modeling and scenario analysis of the critical infrastructure behavior during a particular disruptive event, i.e. over scenario time. Defining the critical functionality of a critical infrastructure enables to precisely and quantitatively define and construct the system resilience curve in scenario time and analyze the main characteristic points of its performance level in discrete or continuous time. The resilience curve can be used to monitor the critical infrastructure functionality level dynamics and to define resilience dynamic characteristics (capabilities), such as reliability, robustness, vulnerability, recoverability, rapidity, maintainability, supportability, etc., mentioned in the previous section. Thus, the resilience capacity models, which correspond to the resulting macro-indicators of critical infrastructure resilience under consideration, selected and used within the framework of the designed estimation method [1] are mainly based on the mathematical formulations given in [25] and resilience curve analysis notionally illustrated in Fig. 3 and the Fig. 4. As noted in [7], these resulting macro-indicators are not the same as the input resilience and functional indices defined at the lower level of the assessment hierarchy (see Fig. 2) and then bottom-up aggregated to the macro level of the overall resilience estimates. In practice, combinations of these macro-indicators are well suitable for stress-testing of critical infrastructures by comparing their values measured or computed with the allowed critical thresholds defined for the specific operating conditions.

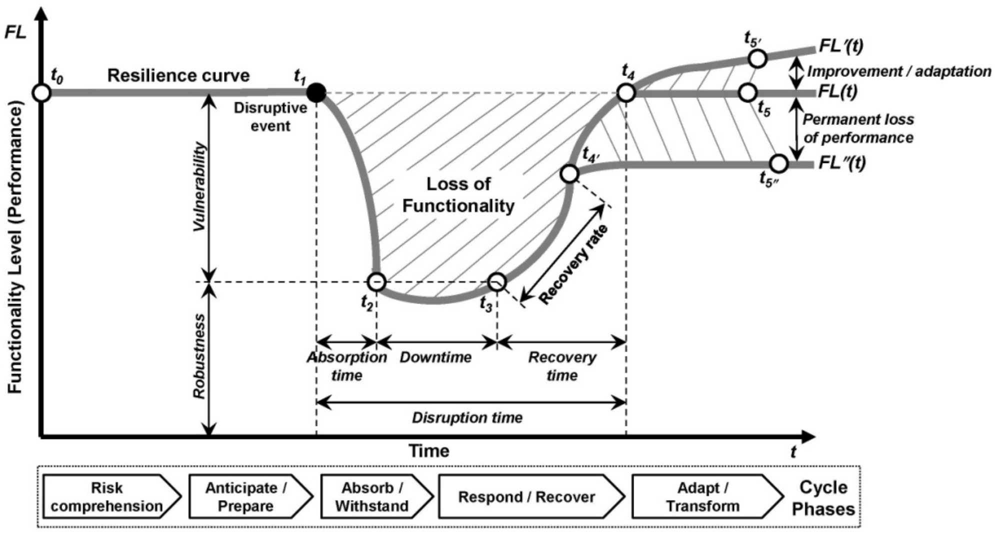

Fig. 4. Resilience curve general view: The dynamics of the resilience level of critical infrastructure over time expressed by the performance loss and recovery function (adopted from [25])

The notations used in Fig. 4 are as follows [25]: t_0 is a time before the disruptive event or a starting point of the simulating scenario; t_1 is a time at which the adverse event occurs; t_2 is a time at which the critical infrastructure reaches the minimum performance level, i.e. a starting point of its functionality loss; t_3 is a time at which the critical infrastructure starts to recover; t_4 is a time at which the critical infrastructure reaches the initial functionality level or a starting point of a new steady-state level, but with lesser performance ($t_4 = t_{4'}$); t_5 is a time at which the scenario ends or at which the critical infrastructure increases its functionality via adapting, transforming and learning ($t_5 = t_{5'}$), or, in the worst case, the system shows a permanent loss of functionality ($t_5 = t_{5''}$).

An accident or disruptive event *E* occurred at time t_1 within the critical infrastructure, which is initiated by some actuating threats as a root cause of its emergence, refers to an incident formally interpreted as a process of parametric variation (system change). Meanwhile, generally speaking, an incident is any parametric or structural change in a critical infrastructure system that is associated with various failures in operation of its components and accompanied by a loss of functionality and irreversible transition process of the system state from a normal operation to an emergency one. In this context, the process of changing the system operation conditions can be formalized as follows:

$$CI\left(\pi^{no}, \sigma^{no}\right) \to CI\left(\pi^{de}, \sigma^{de}\right) \to CI\left(\pi^{eo}, \sigma^{eo}\right), \qquad (1)$$

where $\left(\pi^{no}, \sigma^{no}\right)$, $\left(\pi^{de}, \sigma^{de}\right)$, $\left(\pi^{eo}, \sigma^{eo}\right)$ are the values of the parametric and structural state variables of the critical infrastructure system under different operating conditions: normal operation, failure-caused disruption, emergency operation.

A sudden failure of critical infrastructure system is understood as a rapid (stepwise) change in the values of system state variables that determine its quality (reliability, safety, resilience, etc.), which leads to a complete loss of its functionality at an arbitrary point of time. For the formalized representation of a sudden failure, the Heaviside unit function $1(t)$ [26] is used. The operation of the critical infrastructure system from the point of time $t = t_0$ until the loss of its functionality when $t = t_1 = (t_0 + T)$ is shown in Fig. 4. Then, in compliance with such a way of formal definition of system failure, the following mathematical formulation can be written:

$$x(t) = FL(t)\left[\ 1(t - t_0) - 1(t - t_0 - T)\ \right], \qquad (2)$$

where $FL(t)$ is a system performance function of the critical infrastructure resilience curve; $x(t) \equiv FL(t)$ is a signal actuating at the output of the system in normal operating conditions, and as a result of a failure, $x(t) = 0$; T is a critical period of time when a failure or disruptive event occurs.

In addition to sudden failures, there is also a possible case of stepless degradation of the critical infrastructure system (gradual failures), characterized by the accumulation of hazards within the system and, consequently, a slow (gradual) change in the operating characteristics of the system. Let ρ be a certain variable that expresses an internal danger to the critical infrastructure system. Let us introduce a function $J\left(x_i\left(\rho,t\right)\right)$ that reflects by x_i the damage (fatigue) accumulation within the system at time t:

$$J\left(x_i\left(\rho,t\right)\right)=\int_{t_0}^{t} x_i\left(\rho,\tau\right)d\tau . \quad (3)$$

It is obvious, when the $t_{i+1}>t_i$, an inequality meets $J\left(x_i\left(\rho,t_{i+1}\right)\right)>J\left(x_i\left(\rho,t_i\right)\right)$, and if the proposition $\left(x_i\left(t_{i+1}\right)>x_i\left(t_i\right)\right)\wedge\left(x_i\left(t_{i+1}\right)>x^{\max}\right)$ is true, then from the point of time t_{i+1} the system experiences stepless degradation due to the accumulation of structural changes in it (e.g., variation of constraints, interconnections or control coefficients), where $x^{\max}$ is a maximum permissible value (upper bound) of the system state variables in the normal operating conditions.

Next, the measures for modeling the impact on critical infrastructure system are considered.

Robustness $\left(Rob,\%\right)$ characterizes the absorption capacity of the critical infrastructure [25]. It is measured as the ratio of the percentage of the lowest post-disruption functionality level, i.e. at point of time t_2, to the pre-disruption functionality level, i.e. at point of time t_0 during normal operation. The appropriate formulation can be written as follows:

$$Rob=\frac{FL_2\left(t\right)}{FL_0\left(t\right)}\cdot 100\% . \quad (4)$$

Absorption time $\left(AT,t\right)$, measured in hours, is defined as the time during which the critical infrastructure absorbs a disruptive event while the critical infrastructure undergoes a decrease in its functionality level. It is measured as the difference between points of time t_2 and t_1. The following formulation is given:

$$AT=t_2-t_1 . \quad (5)$$

Loss of functionality $\left(LoF,\%*t\right)$ is the critical infrastructure performance lost in a given adverse situation [25]. It is measured by the area of the curve (an approximation) between the time when the critical infrastructure starts to lose its functionality (t_1) to the time when it reaches the initial state (t_4) (Fig. 4). The approximation is done for the area above the curve to a well-defined shape (e.g., a triangle) [25]. The output is measured in percentage loss of functionality over time (the time is measured in hours).

$$LoF=\int_{t_1}^{t_4}\left[\ FL_1\left(t\right)-FL\left(t\right)\ \right]dt . \quad (6)$$

The value of the functionality level $FL\left(t\right)$ of the critical infrastructure system at a particular time is calculated by aggregating the relevant indicators scores (in a particular case of $FL\left(t\right)$, the specific functionality indices) starting from t_0 and makes up $FL\left(t\right)=100\%$.

Downtime $\left(DT,t\right)$, measured in hours, is defined as the time duration for which the critical infrastructure is not functional. In respect to critical infrastructures, this could apply if the critical infrastructure stops functioning. In this case, the functionality level of the critical infrastructure remains below the threshold level of functionality [25]. It can be measured as the difference in time between points of time t_3 and t_2, as illustrated in Fig. 4 and the following formulation is assumed:

$$DT=t_3-t_2 . \quad (7)$$

This calculation is conducted when the threshold level of functionality is defined (in [25], it is assumed that the threshold level is $FL_{t_2}\left(=FL_{t_3}\right)$).

Recovery refers to the ability to not only return to acceptable operating levels, but also to recover fully from the effects of a disruptive event in the maximum allowable/acceptable recovery time [25]. Recovery time (RT, t), measured in hours, is defined as the time at which the critical infrastructure recovers from the disruptive event and gains its initial or desired functionality level [25]. It can be measured as the time taken to recover the functionality level, i.e. the time between points of time t_3 and t_4. The following formulation can be written:

$$RT = t_4 - t_3 . \quad (8)$$

Since the functionality level at the end of the scenario time may be different from at the start of the scenario, the recovery time may have to be measured at a new steady-state level [25].

Recovery rate $(RR, \% / t)$, measured in percentage, is defined as the rate at which the critical infrastructure recovers from a disruptive event and gets back to its initial functionality level [25]. It characterizes the recovery trajectories of the critical infrastructure system from the point it starts recovering from the given scenario to the final recovery. Recovery rate is measured as the ratio of change in functionality level between points of time t_3 and t_4, as shown in Fig. 4. The following formulation is given:

$$RR = \frac{FL_4(t) - FL_3(t)}{t_4 - t_3} . \quad (9)$$

Disruption time (DT, t), measured in hours, characterizes the recover capacity of the critical infrastructure to return to the desired functionality level and is defined as the total time taken by the critical infrastructure to recover [25]. In the functionality level over time FL / t curve, it is a time between points of time t_1 and t_4 when the disruptive event occurs and the critical infrastructure has fully recovered, respectively. This situation is formally represented in Fig. 4 and formulated as:

$$DT = t_4 - t_1 . \quad (10)$$

Final recovery of the functionality level of a critical infrastructure could be equal to, better than ($FL'(t)$), or worse than ($FL''(t)$) the original system performance ($FL(t)$). Hence, the model schematically illustrated in Fig. 4 allows for the calculation of the system "improvement/adaptation/transformation" capacity $(IAT, \%)$ measured in percentage [25]. This is the capacity of the critical infrastructure to learn from a disruptive event (e.g. a revision of plans, modification of procedures, introduction of new tools and technologies) [25]. It is measured as the ratio of change in functionality level during and after the disruptive event over the initial functionality level:

$$IAT = \frac{FL_5(t) - FL_0(t)}{FL_0(t)} \cdot 100\% . \quad (11)$$

According to [25], such resilience macro-indicators are ideal for comparing the functionality level responses for multiple case studies, critical infrastructures, entities, facilities and assets, etc. They allow an objective evaluation of not only how the functionality level of a system might react to a disruptive event, but also how and when it can recover. Using a theoretical acceptance level, a stress-test can also be performed.

Other important factors to take into consideration when quantifying the resilience of critical infrastructures are: reliability and recoverability of the critical infrastructure components, as well as maintainability and supportability of the disrupted system elements, the prognostics and health management efficiency of the critical infrastructure system in the case of disruption.

The reliability function of critical infrastructure R_{CI} is formally defined as the probability that the system will not fail during the specified period of time t under given conditions.

$$R^{CI}(t) = \Pr\left(the\ \ system\ \ doesn't\ \ fail\ \ during\ \ [0,t]\right) = 1 - F(t) , \quad (12)$$

where reliability $R^{CI}(t)$ is a decreasing function with time t, i.e. for $t_1 < t_2$, $R^{CI}(t_1) \geq R^{CI}(t_2)$, and it is usually assumed that $R^{CI}(0) = 1$; $F(t)$ is a failure function and is a basic (logistic) reliability measure which is defined as the probability that an element of critical infrastructure will fail before or at the moment of operating time t; t is a system operation time which is used in a generic sense and can have units such as hours, number of cycles, etc.

$$F(t) = \Pr(failure\ will\ occur\ before\ or\ at\ the\ time\ t) = \Pr(TTF \le t), \tag{13}$$

$$F(t) = \int_0^t f(u)\,du, \tag{14}$$

where $f(t)$ is the probability density function of the time-to-failure random variable (TTF) in the case of an absolutely continuous distribution function.

Recoverability can be expressed as a non-linear function of system reliability, indicating that the performance of recovery actions is affected by the health of the critical infrastructure system. Special cases of the hybrid and gamma families of recoverability functions expressed in terms of a measure of system functionality (performance) level FL are proposed in study [27]:

1) $FL(t) = 1 - \exp[-c\tilde{t}]$, when $TP_0 = 1$, $a = 1$, $b = 1$, $g(t) = \tilde{t}$; (15)

2) $FL(t) = TP_0 - (TP_0 - FL_{\min}) \cdot \exp[-c\tilde{t}]$, when $a = TP_0 - FL_{\min}$, $b = 0$, $g(t) = \tilde{t}$; (16)

3) $FL(t)_{Exp} = 1 - \alpha \cdot \exp\left[-c\dfrac{\tilde{t}}{\tilde{T}_{rec}}\right]$, when $TP_0 = 1$, $b = 0$, $g(t) = \dfrac{\tilde{t}}{\tilde{T}_{rec}}$; (17)

4) $FL(t)_{lin} = 1 - \dfrac{\tilde{T}_{rec}(TP_0 - FL_{\min})}{2TP_0\,t}$ and $FL(t)_{step} = 1 - \dfrac{\tilde{T}_{rec}(TP_0 - FL_{\min})}{TP_0\,t}$, when $TP_0 = 1$, $a = TP_0 - FL_{\min}$, $b = 0$, $c = 0$, $g(t)_{lin} = \dfrac{\tilde{T}_{rec}}{2TP_0\,t}$, $g(t)_{step} = \dfrac{\tilde{T}_{rec}}{TP_0\,t}$; (18)

5) $FL(t)_{crit\_damp} = \dfrac{d}{dt}FL(t)|_{t=0}\, t\exp[-\omega t]$, when $TP_0 = 0$, $a = \dfrac{d}{dt}FL(t)|_{t=0}$, $b = 1$, $c = \omega$; (19)

where $FL(t)$ is the measure of system functionality (performance) which is quantifiable and time-dependent and is a composite function of time; TP_0 is the target functionality level before the disruption; $[TP_0 - \eta, TP_0 + \eta]$ is the system robustness range; η is the robustness parameter which characterizes how much system performance level can deviate from the target without affecting its core functionalities; a, b, c are parameters to be estimated; $a, a \ge 0$ is a location parameter that is associated with the magnitude of the maximum incurred functionality loss, which depends upon the severity of the disruption and the extent to which the system absorbs the shock; $b, b \ge 0$ is a shape parameter that is associated with the rates of functionality loss and restoration; $c, c \ge 0$ is a scale parameter which indicates the magnitude of the functionality loss over time for fixed loss and restoration rates, has a constant effect on the recovery process during the entire period and, therefore, is associated with the degree of absorptive capability, which is intrinsic to the system, and persists over time; parameters b, c characterize the time to recovery; ω is a parameter that describes the natural frequency with which the system would oscillate if no damping occurred; $g(t)$ is a non-decreasing function such that $g(0) = 0$ and describes system performance monotonic time-domain transformations and contributes into recovery function; $\tilde{t} = t - t_{\min}$ and $\tilde{T}_{rec} = T_{rec} - t_{\min}$; T_{rec} is the time to recovery.

On the other hand, the study [28] provides a basis for estimating the recoverability of critical infrastructures using the following formulations:

$$REC^{CI} = D(t) \times RA(t) \times RC(t), \tag{20}$$

where $D(t)$ is the diagnosis capability which is the ability of a critical infrastructure system to identify true failure elements or failure modes when disruption occurs; $RA(t)$ is the resource accessibility which is the ability of a critical infrastructure system to access enough resources after correct diagnosis; $RC(t)$ is the repair capability which is the ability of a critical infrastructure system to accomplish the repair process after receiving enough resources.

Diagnosis capability of a critical infrastructure system is formulated as follows:

$$D(t) = \mu_D \cdot \frac{1}{e^{\alpha t_D}}, \tag{21}$$

where μ_D is the diagnosis accuracy; t_D is the diagnosis time; α is the coefficient of an exponential utility function used to consider the time effect.

To quantify the resource accessibility of a critical infrastructure system the following formulations are used:

$$RA(t) = \Omega(ava, req) \cdot u(t_{RA}),\ u(t_{RA}) = \frac{1}{e^{\beta t_{RA}}}, \tag{22}$$

where ava is the available amount of resources; req is the required amount of resources; t_{RA} is the time to obtain the resources which is affected by the design of critical infrastructure, resource allocation, amount of required extra resources, etc.; $u(t_{RA})$ is the time utility function; β is the coefficient of the utility function; $\Omega(ava, req)$ is the resource index function.

Quantification of the repair capability is provided by the formulae:

$$RC(t) = L \cdot u(t_W) \cdot u(t_{R\gamma}) \cdot \kappa_\gamma,\ u(t_W) = \frac{1}{e^{\omega t_W}},\ u(t_{R\gamma}) = \frac{1}{e^{\gamma t_{RC}}}, \tag{23}$$

where L is the labor availability; t_W is the required time to retrieve the labor; t_{RC} is the repair time related with available technology, structural design of the element or system, and retest process after the repair; κ_γ is the successful repair rate; $u(t_W)$ and $u(t_{R\gamma})$ are the utility functions of required time and repair time, respectively; ω and γ are the utility coefficients, respectively.

Multiplication of the expressed formulations denotes that the failed critical infrastructure elements or system as a whole can only be recovered with successful operation of all three actions.

The efficiency of the prognostic and health management (PHM) system before and after disruption can be defined as the performance of a critical infrastructure system to failure detection, diagnosis and prediction the effects of possible adverse events [29]. This index is used to maintain and increase the backbone resilience capacities described above. According to researches [29, 30], PHM efficiency is mainly determined by the probability of the correct failure diagnosis event and the probability of the correct failure prognosis event by applying Fuzzy Fault Tree Analysis. At the same time, the efficiency of system PHM depends on the accuracy of defect detection and failure prediction by the critical infrastructure operators and maintenance personnel. Thus, the probability of failure of the PHM system efficiency can be estimated using the following formulation proposed in [29]:

$$FP(\Lambda_{PHM}) = \prod_{i=1}^{m} FP(BE_i), \tag{24}$$

$$P(\Lambda_{PHM}) = 1 - FP(\Lambda_{PHM}), \tag{25}$$

where $FP(BE_i)$ is the failure possibility of i-th basic event; m is the number of basic events; $P(\Lambda_{PHM})$ is the efficiency index of the PHM system which is equal to the complement of the failure possibility of this system.

Another formal expression of the critical infrastructure system PHM efficiency also mostly applied in hard resilience studies can be given as follows:

$$PHM^{CI} = \left(1 - \frac{n}{m}\right) \cdot \left(1 - \frac{t_{dp}}{t_m}\right) \cdot \left(1 - \frac{k}{m}\right) \cdot 100\%, \tag{26}$$

where n is the number of detected defects (failures); m is the total number of supervisions (predictions); t_{dp} is the time between failure detection and its prevention or elimination; t_m is the total observation (prognosis) period; k is the number of false alarms of the PHM system.

The higher the value of this indicator, the more efficient the PHM system is in the context of the critical infrastructure resilience management.

For any critical infrastructure, the system maintainability (M^{CI}) can be calculated using the following equations:

$$M^{CI}(t) = 1 - e^{(-\mu t)}, \ \mu = \frac{1}{MTTR}, \ MTTR^{CI} = \frac{\sum_{i=1}^{n} \frac{MTTR_i}{MTBF_i}}{\sum_{i=1}^{n} \frac{1}{MTBF_i}}, \tag{27}$$

where μ is the repair rate; $MTTR_{CI}$ is a mean time to repair of the critical infrastructure and is calculated as a function in mean time to repair ($MTTR$) and mean operating time between failure ($MTBF$) of critical infrastructure element i; n is a number of critical infrastructure elements.

$MTTR$ represents the expectation of the time to system restoration. $MTBF$ is extremely difficult to predict for fairly reliable system elements. However, it can be estimated if the appropriate failure data are available. In fact, it is very rarely predicted with an acceptable accuracy.

Consequently, the value of the operational availability of critical infrastructure A^{CI} can be determined by the following formula:

$$A^{CI} = \frac{MTTF}{MTTF + MTTR + MTTS}, \tag{28}$$

where $MTTF$, $MTTR$ and $MTTS$ represent the mean time to failure, mean time to repair and mean time to support, and are measures of the system reliability, maintainability and supportability characteristics, respectively.

Mean time to failure ($MTTF$) represents the expectation of the time to failure and is used as a measure of reliability for non-repairable system elements. Mathematically, $MTTF$ can be defined as follows:

$$MTTF = \int_0^\infty rf(t)\,dt = \int_0^\infty R^{CI}(t)\,dt. \tag{29}$$

$MTTS$ can be defined as a term that represents the expectation of the time to support and is a measure of the critical infrastructure supportability characteristics. $MTTS$ is a measure of an on-product maintainability characteristic related to servicing that is calculated by dividing the total scheduled crew/operator/driver servicing time by the number of times the item was serviced.

The discussed resilience capacity models can be adapted in various ways and applied to all types of critical infrastructures and resilience domains for the overall resilience index assessment and analysis of the given class of complex dynamic systems.

Conclusion

Through the last decades, critical infrastructures have progressively begun to be the most essential complex systems influencing the socio-economic development and public welfare as well. In this connection, concerns about the protection and maintenance of critical infrastructures result into a series of state and sector-specific programs targeted to improve security and lately the resilience of this class of systems for withstanding multiple threats and hazards. The high level objective of the most of these programs is development of standards and guidelines for identifying risk factors and interdependencies, evaluating threats and impact, preparing measures to reduce vulnerabilities and to mitigate the consequences of disruptive events, as well as establishing best practices to increase resilience, validating and operationalizing methodologies and tools for system resilience management support in practice. To achieve this goal, the multidisciplinary integrated studies in the line of critical infrastructure resilience assessment and analysis should be first of all carried out.

The main difference between foreign and Russian studies and practices in the field of critical infrastructure resilience management consist in the fact that Russian approaches are mostly focused on pre-event and during disruption measures (prevention and absorption phases, respectively) for the resilience maintenance, while the foreign methodologies concentrate on the post-event measures along with that, and enclose the coping of recovery and adaptation phases as well. At the same time, both ways are complementary and accompanying within the specific case studies of infrastructure resilience issues, notably, resilience estimation and control problems of critical entities or assets.

Nevertheless, it is worth noting that some shortcomings and contradictions exist between the science and practice of resilience management that should be eliminated. In particular, the current well-developed methods of crisis and risk management require modification and adaptation in the face of new challenges brought by the real practice of situational control of critical entities, as well as approaches known from theory can be rather inefficient for protection and resilience maintenance of critical infrastructures when certain theoretical scenarios are irrelevant and mismatched to current threats which may be more complicated, compounding, diverse or unexpected in reality. Moreover, theoretical models for resilience management seems to be ideal and verified, but in real applications can meet complications due to the uncertainties, restrictions, resource limits, changing operation conditions or other influencing factors that are not fully accounted within these models. In addition, theoretical and empirical methods cannot cope all of interdependencies between situational factors, resilience aspects and dynamic characteristics of critical infrastructures when assessing the overall system resilience in real practice. The manner of system behavior and latent nature of dependences between the interconnected critical entities may differ also on conceptual (research) and operational (applied) level of resilience management framework operationalization to critical infrastructures.

To level these bottlenecks, the enhancing of critical infrastructure resilience requires regular evaluation and strengthening the capabilities of critical infrastructures to anticipate and prevent (preparedness, predictability), to resist and absorb (withstandability, absorbability), to react and recover (recoverability, responsiveness), to adapt and transform (adaptability, transformability) in the face of context-dependent disruptive events, adverse circumstances and perturbations. Thereto, an effort to develop a more complete assessment and analysis procedure of the critical infrastructure resilience has been made. It is index-based and applicable to all types of critical infrastructures of the regional scale. The proposed method uses selected estimation models of the resilience capacities and provides quantification of the level and ratio of aggregated reliability, robustness and security indices, as well as the calculation of performance level, savings and losses rate, and control risks for obtaining end-to-end resilience assessment within the all stages of the resilience management cycle.

Combining the developed method with other models of resilience capabilities and indicators allows for a comprehensive assessment of systemic risks that can support decision-making about protection, emergency and situational management of regional critical infrastructures, and thus, in conjugation with other resilience measurement tools and frameworks, allows critical infrastructure operating conditions to be compared in terms of performance characteristics, vulnerabilities, threat impacts, possible consequences, effectiveness of the preventive/mitigation measures and ultimately resilience control strategies.

This research outputs can be practically used as reliable guidance for operators and analysts of regional situational centers to train and generate design decisions about counteracting the current threats, actuating hazards and local failures in the operation of sector-specific critical infrastructure systems under uncertain situations. It is urgent and imperative to get a relevant, holistic comparative picture on the respective functionality level of critical entities and infrastructures based on adequate assessments to control and improve their resilience efficiently. In this case, the proposed method is supposed to be implemented and introduced within the decision support systems of regional and sector situational centers controlling critical entities, or in wider scale applications. In the reality, however, critical infrastructure managers are reluctant to become compared by the auditing services or security authorities, and, naturally, are uninterested to reveal the detailed resilience level across indicators and the current points of system vulnerability as well. Therefore, with a view to this fact, the proposed method can be positioned as a self-assessment tool rather than a regulative and control mechanism of the public authorities.

The future research will be aimed at analysis of the existing normative documents and legal acts adopted in the field of resilience management of critical infrastructures that are regulating and reasoning the assessment criteria and procedure of the critical entities resilience and protection. As a result, findings will be used as a basis for precision adjustment of the proposed estimation method and its further implementation as a software tool suitable and easily tailorable to specific managerial and information support needs of the resilience maintenance, assessment and control.

References

1. Masloboev A.V. An index-based method for integral estimation of regional critical infrastructure resilience using fuzzy calculations. Part 1. Problem statement and method generic structure. *Reliability and quality of complex systems*. 2024;(1):124–141.
2. Reitan N.K. et al. Evaluation of resilience concepts applied to critical infrastructure using existing methodologies. *IMPROVER Project Report: Deliverable 2.3*. 2016:97.
3. Melkunaite L. et al. International Survey. *IMPROVER Project Report: Deliverable 1.1*. 2016:343.
4. Yang Zh. et al. Indicator-based resilience assessment for critical infrastructures – A review. *Safety Science*. 2023;160:106049.
5. Osei-Kyei R., Almeida L.M., Ampratwum G., Tam V. Systematic review of critical infrastructure resilience indicators. *Construction Innovation*. 2023;23(5):1210–1231.
6. Dan G., Shan M., Owusu E.K. Resilience Assessment Frameworks of Critical Infrastructures: State-of-the-Art Review. *Buildings*. 2021;11(10):464.
7. Jovanović A., Klimek P., Renn O. et al. Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards. *Environment Systems and Decisions*. 2020;40(2):252–286.
8. Yang Zh. et al. A multi-criteria framework for critical infrastructure systems resilience. *International Journal of Critical Infrastructure Protection*. 2023;42:100616.
9. Mottahedi A., Sereshki F., Ataei M., Nouri Qarahasanlou A., Barabadi A. The Resilience of Critical Infrastructure Systems: A Systematic Literature Review. *Energies*. 2021;14(6):1571.
10. Almaleh A. Measuring Resilience in Smart Infrastructures: A Comprehensive Review of Metrics and Methods. *Applied Sciences*. 2023;13(11):6452.
11. Sathurshan M., Saja A., Thamboo J., Haraguchi M., Navaratnam S. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures*. 2022;7(5):67.
12. Wells E.M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*. 2022;15:100244.
13. Rehak D., Senovsky P., Hromada M., Lovecek T. Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *International Journal of Critical Infrastructure Protection*. 2019;25:125–138.
14. Rød B., Barabadi A., Gudmestad O.T. Characteristics of Arctic infrastructure resilience: Application of expert judgement. *Proceedings of the 26th International Ocean and Polar Engineering Conference (Rhodes, Greece, June 26 – July 1, 2016)*. Rhodes, Greece, 2016:1226–1233.
15. Honfi D. et al. Technological resilience concepts applied to critical infrastructure. *IMPROVER Project Report: Deliverable 3.2*. 2017:67.
16. Davis C.A. Understanding Functionality and Operability for Infrastructure System Resilience. *Natural Hazards Review*. 2021;22(1):0000431.
17. Youn B.D., Hu C., Wang P.F. Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design*. 2011;133(10):101011(15).
18. Barabadi A., Markeset T. Reliability and maintainability performance under Arctic conditions. *International Journal of System Assurance Engineering and Management*. 2011;(2):205–217.
19. Saraswat S., Yadava G. S. An overview on reliability, availability, maintainability and supportability (RAMS) engineering. *International Journal of Quality and Reliability Management*. 2008;25(3):330–344.
20. Smith, C., Knezevic, J. Achieving quality through supportability: Part 1. Concepts and Principles. *Journal of Quality in Maintenance Engineering*. 1996;2(2):21–29.
21. Tortorella M. *Reliability, Maintainability, and Supportability: Best Practices for Systems Engineers*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2015:464.
22. Rehak D. Assessing and strengthening organisational resilience in a critical infrastructure system: case study of the Slovak Republic. *Safety Science*. 2020;123:104573.
23. Lyttle D.N., Gill J.P., Shaw K.M. et al. Robustness, flexibility, and sensitivity in a multifunctional motor control model. *Biological Cybernetics*. 2017;111:25–47.
24. Prior T. *Measuring Critical Infrastructure Resilience: Possible Indicators. Risk and Resilience Report 9*. Zurich, Switzerland, Center for Security Studies, ETH Zurich. 2015:13.
25. Jovanović A. Øien K., Jelic M. et al. Modeling the impact of an adverse event on the "absorb" and "recover" capacity of a smart critical infrastructure, based on resilience indicators. *H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure. Report Deliverable No: D3.3*. Stuttgart, 2018:53.
26. Davies B. *Integral Transforms and their Applications. Third Edition. Applied Mathematics*. Springer Science & Business Media, 2012;41:370.

27. Cassottana B., Shen L., Tang L. Ch. Modeling the recovery process: A key dimension of resilience. *Reliability Engineering and System Safety*. 2019;190:106528.
28. Li J., Xi Z. Engineering Recoverability: A New Indicator of Design for Engineering Resilience. *Proceedings of the ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. 40th Design Automation Conference. August 17–20, 2014*. Buffalo, New York, USA. 2014;2A:V02AT03A044.
29. Rahimazar A., Nouri Qarahasanlou A., Khanzadeh D., Tavaghi M. Assessing resilience in mechanical systems: an industrial perspective. *International Journal of Quality & Reliability Management*. 2024.
30. Yurkov N.K., Mikhaylov V.S. *Integral'nye otsenki v teorii nadezhnosti. Vvedenie i osnovnye rezul'taty = Integral estimates in reliability theory. Introduction and main results*. Moscow: Tekhnosfera, 2020:152. (In Russ.)

Список литературы

1. Masloboev A. V. An index-based method for integral estimation of regional critical infrastructure resilience using fuzzy calculations. Part 1. Problem statement and method generic structure // Reliability and quality of complex systems. 2024. № 1. P. 124–141.
2. Reitan N. K. et al. Evaluation of resilience concepts applied to critical infrastructure using existing methodologies // IMPROVER Project Report: Deliverable 2.3. 2016. 97 p.
3. Melkunaite L. et al. International Survey // IMPROVER Project Report: Deliverable 1.1. 2016. 343 p.
4. Yang Zh. et al. Indicator-based resilience assessment for critical infrastructures – A review // Safety Science. 2023. Vol. 160. P. 106049.
5. Osei-Kyei R., Almeida L.M., Ampratwum G., Tam V. Systematic review of critical infrastructure resilience indicators // Construction Innovation. 2023. Vol. 23, № 5. P. 1210–1231.
6. Dan G., Shan M., Owusu E.K. Resilience Assessment Frameworks of Critical Infrastructures: State-of-the-Art Review // Buildings. 2021. Vol. 11, № 10. P. 464.
7. Jovanović A., Klimek P., Renn O. et al. Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards // Environment Systems and Decisions. 2020. Vol. 40, № 2. P. 252–286.
8. Yang Zh. et al. A multi-criteria framework for critical infrastructure systems resilience // International Journal of Critical Infrastructure Protection. 2023. Vol. 42. P. 100616.
9. Mottahedi A., Sereshki F., Ataei M., Nouri Qarahasanlou A., Barabadi A. The Resilience of Critical Infrastructure Systems: A Systematic Literature Review // Energies. 2021. Vol. 14, № 6. P. 1571.
10. Almaleh A. Measuring Resilience in Smart Infrastructures: A Comprehensive Review of Metrics and Methods // Applied Sciences. 2023. Vol. 13, № 11. P. 6452.
11. Sathurshan M., Saja A., Thamboo J., Haraguchi M., Navaratnam S. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks // Infrastructures. 2022. Vol. 7, № 5. P. 67.
12. Wells E. M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review // Progress in Disaster Science. 2022. Vol. 15. P. 100244.
13. Rehak D., Senovsky P., Hromada M., Lovecek T. Complex Approach to Assessing Resilience of Critical Infrastructure Elements // International Journal of Critical Infrastructure Protection. 2019. Vol. 25. P. 125–138.
14. Rød B., Barabadi A., Gudmestad O. T. Characteristics of Arctic infrastructure resilience: Application of expert judgement // Proceedings of the 26th International Ocean and Polar Engineering Conference (Rhodes, Greece, June 26 – July 1, 2016). Rhodes, Greece, 2016. P. 1226–1233.
15. Honfi D. et al. Technological resilience concepts applied to critical infrastructure // IMPROVER Project Report: Deliverable 3.2. 2017. 67 p.
16. Davis C. A. Understanding Functionality and Operability for Infrastructure System Resilience // Natural Hazards Review. 2021. Vol. 22, iss. 1. P. 0000431.
17. Youn B. D., Hu C., Wang P. F. Resilience-driven system design of complex engineered systems // Journal of Mechanical Design. 2011. Vol. 133. P. 10. P. 101011.
18. Barabadi A., Markeset T. Reliability and maintainability performance under Arctic conditions // International Journal of System Assurance Engineering and Management. 2011. № 2. P. 205–217.
19. Saraswat S., Yadava G. S. An overview on reliability, availability, maintainability and supportability (RAMS) engineering // International Journal of Quality and Reliability Management. 2008. Vol. 25, № 3. P. 330–344.
20. Smith, C., Knezevic, J. Achieving quality through supportability: Part 1. Concepts and Principles // Journal of Quality in Maintenance Engineering. 1996. Vol. 2, № 2. P. 21–29.
21. Tortorella M. Reliability, Maintainability, and Supportability: Best Practices for Systems Engineers. John Wiley & Sons, Inc., Hoboken, New Jersey, 2015. 464 p.
22. Rehak D. Assessing and strengthening organisational resilience in a critical infrastructure system: case study of the Slovak Republic // Safety Science. 2020. Vol. 123. P. 104573.
23. Lyttle D. N., Gill J. P., Shaw K. M. et al. Robustness, flexibility, and sensitivity in a multifunctional motor control model // Biological Cybernetics. 2017. Vol. 111. P. 25–47.

24. Prior T. Measuring Critical Infrastructure Resilience: Possible Indicators. Risk and Resilience Report 9. Zurich, Switzerland, Center for Security Studies, ETH Zurich. 2015. 13 p.
25. Jovanović A. Øien K., Jelic M. et al. Modeling the impact of an adverse event on the "absorb" and "recover" capacity of a smart critical infrastructure, based on resilience indicators // H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure. Report Deliverable No: D3.3. Stuttgart, 2018. 53 p.
26. Davies B. Integral Transforms and their Applications. Third Edition. Applied Mathematics. Springer Science & Business Media, 2012. Vol. 41. 370 p.
27. Cassottana B., Shen L., Tang L. Ch. Modeling the recovery process: A key dimension of resilience // Reliability Engineering and System Safety. 2019. Vol. 190. P. 106528.
28. Li J., Xi Z. Engineering Recoverability: A New Indicator of Design for Engineering Resilience // Proceedings of the ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. 40th Design Automation Conference. August 17-20, 2014, Buffalo, New York, USA. 2014. Vol. 2A. P. V02AT03A044.
29. Rahimazar A., Nouri Qarahasanlou A., Khanzadeh D., Tavaghi M. Assessing resilience in mechanical systems: an industrial perspective // International Journal of Quality & Reliability Management. 2024.
30. Юрков Н. К., Михайлов В. С. Интегральные оценки в теории надежности. Введение и основные результаты. М. : Техносфера, 2020. 152 с.

Информация об авторах / Information about the authors

Андрей Владимирович Маслобоев
доктор технических наук, доцент,
ведущий научный сотрудник лаборатории
информационных технологий управления
техногенно-природными системами,
Институт информатики и математического
моделирования имени В. А. Путилова
Кольского научного центра Российской академии наук;
главный научный сотрудник,
Институт проблем промышленной экологии Севера
Кольского научного центра Российской академии наук
(Россия, Мурманская область, г. Апатиты,
ул. Ферсмана, 14)
E-mail: masloboev@iimm.ru

Andrey V. Masloboev
Doctor of technical sciences, associate professor,
leading researcher of the laboratory of information
technologies for industrial-natural system management,
Putilov Institute for Informatics
and Mathematical Modeling of the Kola Science
Centre of the Russian Academy of Sciences;
chief researcher,
Institute of North Industrial Ecology Problems
of the Kola Science Centre
of the Russian Academy of Sciences
(14 Fersmana street, Apatity, Murmansk region, Russia)

Автор заявляет об отсутствии конфликта интересов /
The author declares no conflicts of interests.
Поступила в редакцию/Received 28.05.2024
Поступила после рецензирования/Revised 25.06.2024
Принята к публикации/Accepted 16.08.2024