Temporal conceptual models of resilience cycle for managing critical infrastructure systems*

A.V. Masloboev

Federal Research Centre "Kola Science Centre of the Russian Academy of Sciences", Apatity, Russia

Abstract. The study is mainly aimed at developing models, methods and information technologies for problem monitoring and interpretable decision-making support in the field of critical infrastructure systems management in order to ensure their resilient operation under hazardous natural and man-made impacts. For the unified formalized representation of the information structure, processes and problems of ensuring the safety and stability of the studied class of systems, conceptual models of the critical infrastructures functioning life-cycle accounting the temporal aspects of their dynamics management and based on the principals of the state-of-the-art resilience concept of complex systems, have been designed. The models provide a formal basis for the simulation, automation and coordination of the infrastructure system resilience management processes at the stages of their life-cycle in order to generate and analyze possible scenarios for the occurrence of triggering events and potential threats associated with them. In practice, the proposed models can be implemented as an applied ontology of critical infrastructure resilience, which can find applications for situational management systems and preventive safety analytics of critical entities.
Keywords: *conceptual modeling, temporal model, life-cycle analysis, management, resilience, critical infrastructure, dynamic system.*
DOI: 10.14357/20790279250408 **EDN:** MSIWLZ

Introduction

The increasing frequency and severity of various disruptions and incidents from man-made activities and casual events to transboundary cyber-attacks and natural disasters demand a dynamic, time-aware approach to critical infrastructure resilience management based on system functioning life-cycle conceptual models accounting temporal aspects of its resilience and performance. Life-cycle temporal modeling of the critical infrastructure resilience is urgently needed for enhancing the efficiency of decision-making under situational control of the system critical entities and functions. Temporal models should not be optional for resilience management processes. They are critical for preventing temporal risks and collapse in multi-hazard environments, where critical infrastructures exist and operate, as well as for optimizing limited types of resources (time, money, labor, etc.) and future-proofing policies against unknown and unforeseen disruptions. Without temporal models, we are blind to the dynamics of threats and failures. With them, we can design resilient infrastructure systems that bend, but do not fail. Besides, the application of formalized life-cycle temporal models within the resilience management is conditioned by such reasons as high demands of proactive adaptation to escalating threats; the aging rapidity of critical infrastructure systems is faster than these systems are upgraded; regulatory and insurance pressures at government level that strictly require resilience timelines for critical entities (time-to-recover/time-to-adapt metrics); cascading effects and failures that are time-dependent, but not discounted and supported in static models missing temporal phase transitions; decision support system requirements of consistent, complete and time-structured data for the resilience predictive maintenance and adaptive control; economic costs of ignoring system resilience timelines which leads to confusion of when and where to invest in upgrades and redundancy to minimize disruption costs and potential losses. Thus, resilience cycle temporal models prioritize time limits to timely operational and strategic decision-making under prognostic and health management of the critical infrastructure system. They are used to regulate scheduling terms of system resilience audits, maintenance and support within the all phases

* 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-2025-0054).

of its life-cycle, and in analysis of system performance function (resilience triangle curve) as well.

Therefore, engineering and further exploration of resilience cycle temporal models of the critical infrastructure systems is an essential research problem which is in some way complex, interdisciplinary and needs deeper studying and formal reasoning. The efficient solving of this problem is practically important, because resilience is inherently dynamic, evolving over time in response to impact of various nature destructive factors, recovery actions, and environmental shifts. By embedding temporal models into state-of-the-art resilience frameworks, it is possible to build critical infrastructure systems that not only survive disruptions, but adapt and thrive in the face of current, interconnected threats. Temporal models shift resilience control from reactive "firefighting" to proactive, data-driven risk management strategy adequate and well-suitable in atypical regimes of system operating depended on increasingly volatile ambient conditions.

In this study we make an attempt to summarize and design resilience cycle conceptual models with focus on resilience temporal aspects by formalizing backbone phases of the system adaptive cycle (a dynamic map of resilience) while accounting for systemic constraints for the purpose of critical entities and infrastructure systems efficient situational management, as well as to level existing contradictions and bridge the gaps in theory and practice in this field of research. This study is a logical continuation of the earlier research works [1-3], where a general framework for analysis of resilience capacity models and evaluation of control actions aimed at maintaining system properties (robustness, flexibility, fragility, redundancy, recoverability, resourcefulness, rapidity, etc.) in the range of its adaptative capabilities under various operating conditions and critical-case scenarios of potentially adverse events, has been developed.

At first sight, this study is primarily theoretical in nature as it may seem. Though, basically, our findings make a contribution to the development of a formal apparatus for the general theory of resilience management of complex dynamic systems, specifically by engineering conceptual models that concretize and detail the conceptualization and formalization of critical infrastructure resilience, taking into account the temporal and organizational aspects of the situational management cycle of the resilient functioning of this class of systems. This enables improved validity and efficiency of decision-making via analysis and modeling of initiating event propagation processes/scenarios, as well as the automated choice of facilities and assets relevant to the current situation for maintaining system resilience based on these models. A comparative analysis of developments proposed with existing approaches, as well as experimental validation of the theoretical assumptions and formulations in solving real-world problems (by the example of real critical entities or infrastructures operating in mining industry sector of Murmansk region, Russian Federation) are beyond the scope of this work and will be the next stage of our further research on the issues discussed here.

1. Accepted definitions and assumptions

There is no universally and commonly accepted definition of critical infrastructures. The works [4, 5] discuss and review difference in understanding of critical infrastructures and its definitions that mostly emphasize the contributing role of infrastructure to society or the potentially debilitating effect in the case of disruption. In [4] it is asserted that infrastructure systems that represent a significant public investment and where even minor disruptions can degrade the performance of global systems and cause significant societal damage can be called critical infrastructures. At once, such infrastructure systems (i.e., a set of facilities providing vital services necessary for a society to function) are considered as critical, if its malfunctioning threatens the security, economy, lifestyle or public health of a city, region or even a state. On the other hand, critical infrastructures are often interpreted as systems, whose incapacity or destruction would have a debilitation impact on the defense and economic security, or identified as those physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments, first of all, in EU-countries [4]. Meanwhile, it is difficult to define, what types of entities/infrastructure systems are critical. The critical infrastructure sectors (energy, transport, healthcare, banking, water, industry, space, food, etc.), decided by each country, government or organization, depends on their own contexts and priorities. The classification of critical infrastructure systems is not the chief aim of our study and is mentioned here without further discussion. It is an independent research problem that requires deeper focus, detached elaboration and scientific substantiation.

The complexity of modern critical infrastructures as "systems-of-systems" makes it virtual impossible to foresee and prevent all possible adverse scenarios [6]. In addition, the critical infrastructures are under dynamic stress due to operational conditions that can significantly affect the reliability, safety and resilient functioning of their components, the system configura-

tion, and consequently, the functionality/performance of components [4]. Thus, the study [7] relying on these facts postulates just critical infrastructure protection is not enough. Over time, such deliberate reasoning by reputable studies has led to a paradigm shift towards critical infrastructure resilience, i.e., from protection to genuine resilience. Subsequently, this also led to a new focus shift from resilience and protection of critical infrastructure sectors to the level of concrete critical infrastructure facilities, operators or entities, without clearly articulating this as such [8, 9].

Similarly, the term "resilience" is difficult to define, because of its very wide use. In the field of critical infrastructures, resilience still has no generally accepted definition. Etymologically, resilience comes from the Latin (resilio, resiliere), which means a return and the ability to resume [4]. Over time, a series of interpretations of resilience has been presented. The studies [5, 10, 11] considers the evolution of resilience term meaning with the last decades of development of this concept that was originally introduced as a persistent ability to absorb change and disturbance and still maintain the same state variables [12]. Later, it was refined as the ability of a system to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption. The main amendment proposed afterward was the inclusion of the ability to comprehend risks (current and emerging), leading to the definition of resilience as the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption. Then, the study [10] adopted the elaborated definition of the resilience of an infrastructure system and stated it in the following formulation: the resilience of an infrastructure is the ability to understand and anticipate the risks, including new/emerging risks, threatening the critical functionality of the infrastructure, prepare for anticipated or unexpected disruptive events (so-called "black swans" [13]), optimally absorb/withstand their impacts, respond and recover from them, and adapt/transform the infrastructure or its operation based on lessons learned, thus improving the infrastructure anti-fragility [10]. According to the latest ISO/TS 31050 "Guidance for Managing Emerging Risks to Enhance Resilience" [14], resilience is defined similar to [10] as the ability of a system to anticipate possible adverse scenarios/events representing threats and leading to possible disruptions, to prepare for these events, to withstand/absorb their impacts, to recover from disruptions caused by them and to transform/adapt to the new, changed conditions, after the event. This definition has become approximately conventional for the most foreign resilience studies. In our research works, we also abide by the given definition of infrastructure resilience and apply it to critical entities and regional infrastructures systems. Discussed definitions allow analyzing the behavior of a critical infrastructure system exposed to an adverse event over a scenario timeline and simultaneously assessing the functionality of a critical infrastructure system over the resilience cycle as notionally shown in Fig. 1. While the decomposition over the time-axis, i.e., defining the temporal phases of the resilience cycle, may be trivial, decomposition over the functionality axis is non-trivial as functionality might have different dimensions and metrics [10]. Resilience captures five phases in the resilience cycle associated with system capabilities: understand risks, anticipate/prepare, absorb/withstand, respond/recover and adapt/transform. These are the main attributes (capacities) of system resilience, reflected in [3, 15]. Even so, some relevant resilience studies (e.g., [16-18]) argue that resilience per se is very multidisciplinary and has little orthodoxy in its conceptualization, operationalization and application, and, therefore, becomes problematic when trying to measure it using heterogeneous system performance indicators within the all temporal phases of the resilience cycle.

2. Materials and methods

The background of this on-going, in some way, pilot study comprises pioneer research works and portfolio materials contributed to the development of the classical and modern theory of stability and safety of complex dynamic systems, general theory of reliability control and risk management, as well as to solving fundamental problems in the field of engineering models, methods and technologies for situational management information support of critical entities and infrastructures. First of all, there are such domestic systemic researches as: [19] in the field of situational management; [20] in the field of critical infrastructure protection; [21] in the field of risk analysis of socio-economic systems; [22, 23] in the field of modeling stability in control systems; [24, 25] in the field of adaptive control systems; [26, 27] in the field of studying the influence of human factor and its accounting in management of large-scale systems; [28, 29] in the field of system dynamics and agent-based modeling; [30] in the field of interdisciplinary research.

Conceptually, resilience can be modeled through the change in system performance or functionality over time. Therefore, based on the reputable studies of critical infrastructure resilience [31-33], the resilience cycle/scenario presents with four temporal stages [4] covering the five main phases [15] (Fig. 1) mentioned above.

The temporal model of system resilience is a framework that examines how a system's ability to withstand, adapt to, and recover from disruptions and trigger-adverse events evolves over time. It emphasizes the dynamic nature of resilience, recognizing that systems face varying multiple threats and undergo changes in their capacity to maintain functionality under influencing situational factors. Unlike static models that treat resilience as a fixed system property, the temporal models acknowledge that resilience is time-sensitive and influenced by evolving threats, system states, and recovery processes. This class of models provides both analysis of the system resilience dynamic characteristics and allows for such temporal aspects of resilience management as:

– temporal stages of resilience cycle such as pre-event/disruption (resistance, preparation, early warning), during event/disruption (absorption, adaptation), post-event/disruption (recovery, evolution), and next event/disruption preparation (learning, improvement);
– time-dependent factors such as response time (how quickly a system reacts to disruptions), recovery duration (the time needed to return to normal or a new stable state), adaptation rate (how fast the system learns and improves resilience);
– dynamic feedback loops [34], i.e., systems may enter feedback cycles where past disruptions inform future resilience strategies (e.g., learning from failures).

Pre-disruption phase is characterized as a period of time from the occurrence of a triggering event to the beginning of the system degradation (loss of functionality). At this stage the system builds robustness through redundancy, diversity, and proactive measures. During disruption phase represents the time interval from the beginning of the system degradation to the maximum loss of its functionality, i.e., when the system absorbs shocks, minimizes degradation, or adapts to continue functioning. Post-disruption phase is a part of system functioning timing loop when the system restores functionality and may improve resilience for future disruptions, i.e., a time period from the maximum degradation of the system performance to the functionality returning to the level of the pre-event stage or recovering to an ideal state, structure or property which can be worse or better than the original ones. Next disruption preparation phase is a period of time from the functionality returning to the level of the pre-event stage to the occurrence of the new triggering event/shock on the system or its components [4]. This stage in the former scenario is related to the pre-event stage in the next scenario [2]. Following [2, 4], it is worth noting that the ability of improvement may affect different subsequent cycle phases and scenarios, as well as that the system performance in each scenario should improve at least in one stage compared to previous scenarios, thanks to the ability of a system to adapt and learn from the experience.

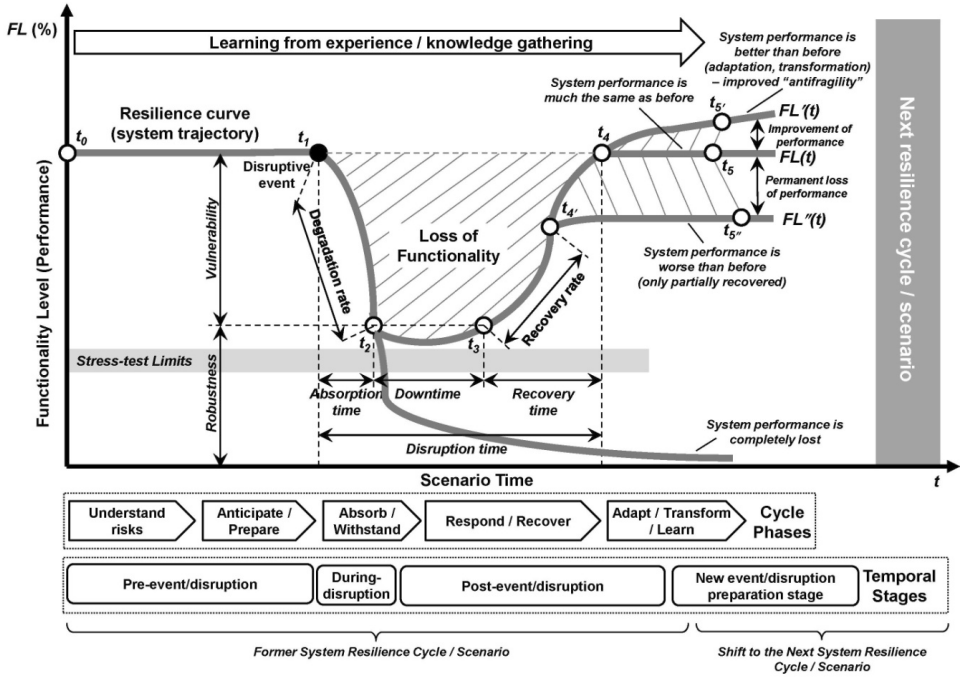

Fig. 1. Mapping the dynamics of critical infrastructure functionality level over temporal phases of the resilience cycle and possible outcomes when the system is exposed to an adverse event (adopted from [3])

Temporal modeling of system resilience cycle requires addressing both broad conceptual foundations and domain-specific technical needs. The overall requirements for system resilience temporal models engineering, derived from recent research [35-38], are shortlisted below.

General requirements such as dynamic threat handling, adaptive capacity and flexibility, standardized frameworks, systemic and contextual representation, verification and validation should apply across domains and ensure resilience models are holistic, adaptable, and actionable. Models must account for unpredictable disruptions (e.g., cyber-attacks, climate extremes, etc.) by integrating probabilistic or scenario-based approaches, and multi-hazard interactions to addressing cascading failures and compound disruptions (e.g., earthquakes triggering infrastructure collapse) through interdependency mapping. Models should reproduce graceful degradation of the system when it maintain partial functionality during disruptions and recover iteratively, and support post-disruption learning mechanisms that must be formalized to improve future system resilience and its adaptation (e.g., updating protocols, hardening infrastructure) to the recent operating conditions. Models must account unified quantifiable metrics (e.g., downtime, recovery time, performance retention, etc.) to compare resilience across systems, and align with existing safety standards like ISO 31000 [39]. Integration with complementary risk analysis/management frameworks to provide compliance and interoperability of the resilience conceptual models is quite important here. Models should examine critical infrastructures as system-of-systems and account interactions between subsystems (critical entities) to analyze and detect unintended cascading effects. As well, resilience cycle conceptual models must incorporate socio-technical factors (e.g., territory specificity, critical entities density, actor/operator behavior characteristics, etc.) that influence overall resilience, and should focus on application of the state-based formal analysis methods (e.g., probabilistic POMDPs) to verify model correctness while enabling system adaptability under disruptions or critical events.

Specific requirements address technical and operational nuances in temporal modeling of the system resilience such as temporal granularity, human-in-the-loop considerations, dynamic risk assessment, resilience quantification, domain-specific adaptations. Temporal granularity implies integration of time-varying data to capture dynamic vulnerabilities, and differentiation between immediate stabilization (minutes), short-term repairs (hours), and long-term upgrades (months), i.e., phased recovery modeling when managing the system resilience. Accounting of human factor, i.e., human response times and behavioral dynamics when modeling the resilience management cycle is needed to simulation of panic, trust, or coordination shifts during disruptions and critical events to refine joint action plans and system control programs, and quantification of manual intervention delays with uncertainty bounds. For the dynamic risk assessment and resilience quantification GIS-based spatial-temporal risk maps and fuzzy logic can be efficiently used to model risk variations of system functionality losses and cost-benefit tradeoffs. Combining of the risk continuous monitoring and system resilience cycle modeling provide a basis for the early warning and implementation of risk adaptive controls when real-time potential threat tracing. Temporal models built on resilience performance-based metrics and using stochastic dynamic programming serve for the optimization of facility and resource allocation to balance redundancy and recovery budgets under system resilience maintenance phased process. To ensure validity resilience temporal models should surely take into consideration context and domain-specific adaptations. This is especially important for critical infrastructure systems when modeling their resilience and assessing the efficacy of applying preventive measures under system performance characteristics fluctuations. Critical infrastructures are high-dimensional scalable systems that extremely required avoid bias in their resilient operating. Resilience temporal models are in some way intended to prioritization of system self-healing phases and evaluation of the relevant fail-safe modes for system functioning within these temporal phases. The discussed requirements are partially or completely allowed for some well-known formalized conceptual models of system resilience like the “SyRes Model” (Systemic Resilience Model) [40], GRAM (General Resilience Assessment Model) [41], Resilience Contracts [42] and others used widely for practical issues.

Nevertheless, there are some contradictions revealing in theory and practice of resilience cycle temporal modeling and dynamics control that in tote affect on the overall efficiency of resilience management systems engineered. In turn, the effectiveness of preventive and reactive countermeasures applied to mitigate and eliminate risks of the system functionality losses under adverse events and disruptions depend on resolving of these discordances. Generally, the contradictions between resilience conceptual frameworks and real practices arise from divergent theoretical concepts and assumptions, differing interdisciplinary interpretations and perspectives, practical constraints, evolving threat landscapes, and the inherent complexity of large-scale dynamic systems.

Traditional resilience models (e.g., engineering resilience) emphasize a system's ability to return to a pre-disruption equilibrium, often quantified by metrics like recovery time or redundancy. In terms of practical challenges, multidimensional systems, such as critical infrastructure systems, face dynamic, adaptive threats (e.g., triggering events, dependent cascading failures, cyber-attacks, etc.) that require continuous adaptation rather than static recovery. Thereat, static models fail to account for systems that must evolve into new stable states (e.g., socio-ecological resilience) or operate under persistent adversarial conditions.

Another contradiction lies in accepted terminology. Resilience is often conflated with robustness or adaptive capacity, treating them as interchangeable. Robustness focuses on resisting degradation without structural change, while resilience involves adaptation and recovery, i.e., evolving in response to disruptions. Thereat, distinct definitions for resilience (adaptation) and robustness (resistance) are critical for design of effective resilience management models and methodologies. Robustness-centric models prioritize redundancy and hardening to withstand known threats, assuming static system boundaries whereas adaptive models emphasize dynamic reconfiguration, learning, and flexibility to address unforeseen challenges. Practitioners often design systems for robustness (e.g., redundant components) but neglect adaptive mechanisms (e.g., self-healing algorithms), leading to brittle systems under novel threats. Thus, designing for robustness can reduce adaptability (e.g., over-engineered systems become brittle), while excessive adaptability may compromise stability.

At the same time, definitions of resilience oscillate between preventive measures (avoiding disruptions) and reactive recovery (post-disruption restoration). Proactive approaches (e.g., threat anticipation, redundancy, etc.) aim to eliminate exposure to risks, whereas reactive approaches focus on rapid recovery and adaptation after disruptions. Therefore, proactive strategies require significant upfront investment and may fail against "unknown unknowns", while reactive methods risk high downtime costs. Besides, investment in preventive measures often overshadows adaptive capacity, leaving systems vulnerable to "unknown unknowns". Traditional risk management theory prioritizes preventing disruptions (e.g., redundancy, hardening), while in the key practices emerging threats make prevention in a way insufficient, necessitating adaptive strategies based on real-time reconfiguration, dynamic reasoning, machine learning, etc.

Resilience is quantified using technical metrics (recovery time, MTTR, etc.), but depends on qualitative factors like trust and human behavior. Engineering models prioritize measurable parameters (redundancy levels, fault tolerance, system order, etc.). while socio-technical systems require intangible factors such as community trust, organizational culture, and cognitive flexibility, which resist quantification. At the same time, the scarcity and heterogeneity of system control and status data hinder universal metrics. Meanwhile, over-reliance on standardized metrics may overlook systemic vulnerabilities rooted in human or ecological interdependencies. Thus, the push for standardized metrics to resilience quantification clashes with context-specific resilience requirements. The way out is to develop models using flexible context-aware metrics that balance generality and specificity (e.g., hybrid flow/information-based analyses). A holistic view to system resilience modeling requires integrating cyber, physical, temporal, spatial, and human aspects into a cohesive whole. Most models are fragmentary or restricted and focus on isolated resilience domains without addressing interdependencies between critical entities. Cross-domain integration fosters interdisciplinary collaboration to address interdependencies in critical infrastructure systems.

Human behavior introduces variability (e.g., delays, errors, etc.) that is rarely quantified in resilience models. For example, manual recovery actions in industrial systems are often based on historical data, but lack real-time adaptability. Integration of human variability into resilience models via probabilistic frameworks, for example, by using Bayesian networks, to build adequate automated resilience management systems is an urgent practical issue. Human operators are often modeled as rational actors, who enhance resilience through adaptive decision-making. So, Over-reliance on automation risks ignoring human adaptability, while under-reliance introduces unpredictability.

Most resilience models often assume predictable events/disruptions, yet real-world systems face chaotic, stochastic environments and unexpected, utterly original situations. Traditional control theory relies on predefined failure modes and recovery protocols, while complex dynamic systems like critical infrastructures, socio-economic or natural-industrial ones exhibit nonlinear behaviors, hidden states, and cascading failures that defy prediction. Therefore, the implementation of automatic recovery mechanisms in such class of systems leads to ineffective responses.

The agenda involves also a problem of relevant control mechanisms implementation in designed resilience models depending on types and structural features of systems managed and maintained. This problem domain considers precisely centralized and decentralized control in the large-scale multi-level systems. Centralized systems offer streamlined resilience

control, but lack adaptability, while decentralized ones enhance flexibility at the cost of coordination. Centralized resilience control models with monolithic architectures simplify system resilience management, but at the same time are vulnerable to single points of failure. On the other hand, decentralized resilience management models improve system resilience through redundancy, but require robust coordination mechanisms to support network-centric control. For all that, achieving connectedness without centralization remains a challenge in dynamic large-scale systems.

Resilience often demands redundancy and diversity, but these introduce complexity that can undermine manageability. Redundancy-driven models enhance fault tolerance, but increase maintenance overhead. Contrariwise, simplicity-focused models prioritize modularity and loose coupling to reduce failure propagation. Thus, balancing redundancy with simplicity is critical – excessive complexity can create new failure modes (e.g., complex interdependencies in network-centric systems, critical infrastructures, etc.).

At once, traditional models of system resilience emphasize learning from failures, while emerging paradigms advocate learning from successes. So, Safety-I framework [43] focuses on the root-cause analysis of errors to prevent risk recurrence. On the other hand, Safety-II concept [43] prioritizes understanding everyday successes to build adaptive capacity as a basis of resilience engineering. As a result, overemphasis on errors may foster punitive cultures, whereas success-centric approaches risk complacency toward latent risks.

To resume, the considered fundamental discordances and nuances can be mostly handled by combining existing resilience design and management methodologies with developing innovative situational conceptual models of complex dynamic systems and, first of all, critical entities and infrastructure systems, for their resilience and safety preventive analytics. The main contradictions revealed highlight the need for resilience formal hybrid models and unified adaptive frameworks that attempt to bridge theoretical rigor and practical complexity, ensuring complex systems can withstand both predictable and emergent threats, as well as to integrate robustness with adaptability, resilience quantitative metrics with qualitative insights, and centralized oversight with decentralized autonomy while accounting for systemic constraints.

System resilience temporal modeling encompasses diverse methodologies tailored to address dynamic threats, adaptive capacity, and recovery processes. Among the variety of the state-of-the-art methodologies for conceptual and dynamic models engineering of the complex system resilience accounting the temporal aspects of the life-cycle of its resilient functioning, the following well-known frameworks are the most popular with a practical view:

– Network analysis approaches such as QtAC (Quantifying the Adaptive Cycle) method proposed by [44] and flow-based ascendency analysis method [45]. QtAC uses information transfer between system components to model resilience, overcoming data limitations in traditional flow-based analysis. It aligns with the Adaptive Cycle Model [46] (growth, conservation, release, and reorientation) to assess complex socio-economic systems. Flow-based ascendency analysis method measures material/energy flows in ecosystems or socio-economic systems, quantifying resilience via metrics like redundancy or ascendency. QtAC is ideal for socio-economic systems with incomplete data, while flow-based methods suit ecosystems with measurable resource exchanges.
– Spatial-Temporal modeling frameworks such as combined GIS-FuzzyLogic method [47], which integrates spatial data with temporal risk assessments using fuzzy logic and D-ANP (DEMATEL-based Analytic Network Process) weighting [48] for analyzing causal relationships and handling interdependencies and feedback in complex systems when managing its resilience, and transportation modeling approach, which is helpful to evaluate system resilience using metrics like redundancy, diversity, and recovery time across modes (roadways, air, rail, etc.) under natural or man-made disasters. GIS-based models are optimal for urban resilience planning, while transportation models prioritize critical infrastructure redundancy and mostly underemphasize socio-behavioral dynamics (human-centric factors). This gap is highlighted in transport systems resilience studies.
– Probabilistic and stochastic methods such as Markov process approach [49], which is very suitable to model the resilience of multi-state dynamic systems with state transitions (resistance, absorption, recovery, adaptation) using infinitesimal generator matrices, and resilience flexible contracts approach [42] for building resilience “by design” within the formal, state-based contractual frameworks, which combine POMDPs (Partially Observable Markov Decision Processes) [50] for verification and adaptability to withstand and recover from disruptions, as well as provide proactively identifying potential risks, defining clear performance expectations under disruptive conditions, and including clauses that enable flexibility and adaptation. Markov models suit energy systems (power grids, nuclear plants, etc.), while resilience contracts are ideal for safety-critical systems like autonomous vehicles. Prob-

abilistic models need empirical validation to ensure accuracy in multi-state systems.

– Data-driven an AI-based methods such as digital twins with deep learning framework [51], which combines real-time simulations with convolutional neural networks or long short-term memory neural networks for predictive fault detection and system performance optimization, and machine learning (Random Forest / Support Vector Machine), which is useful to assess building seismic resilience using factors like topography, geology, and structural integrity. Digital twins are directly aimed at optimization of industrial systems resilience, while machine learning methods aid post-disaster critical entities assessments. Digital twins and AI methods show promise, but require scalable computational resources.
– Performance-based methods such as resilience triangle and multi-component frameworks [52] measure system functionality loss over time and combine robustness, rapidity, and recovery metrics. Triangles suit infrastructure downtime analysis, while multi-component metrics are better for adaptive systems like aviation. Despite advances, metrics like the resilience triangle lack universal adoption, necessitating frameworks like axiomatic design.
– Simulation methods like system dynamics and agent-based modeling [53]. System dynamics models system resilience as a continuous feedback-driven process using stocks, flows, and feedback loops to capture system-wide behavior over time. Rooted in control theory, it emphasizes nonlinear interactions and delayed responses across system resilience cycle temporal phases. System dynamics is well-applicable in the fields of critical infrastructure degradation and long-term climate adaptation modeling, international struggle and policy trade-offs analysis, sustainable development and global security, organizational and ecological resilience management. Agent-based modeling treats resilience as an emergent property of heterogeneous agents (individuals, organizations) adapting to disruptions through local interactions. Grounded in complex adaptive systems theory, agent-based approach is suitable both to safety and resilience control problem-solving specifically when simulating crowd behavior during disasters, supply chain reconfiguration, urban and regional resilience planning, or post-disruption adaptive learning.
– Other formal methods like axiomatic design process approach [54], which decomposes resilience requirements into quantifiable parameters for critical infrastructure systems and provides clear alignment with system requirements, and hybrid information fusion framework [55], which is focused on multi-dimensional resilience and addresses physical and social factors when managing system resilience. For instance, axiomatic design standardizes power grid resilience, while hybrid fusion combines geological, architectural, and social indicators for community resilience to aid community-level planning.

The pictorial view of the system resilience temporal cycle conceptual models evolved and built on the basis of the summarized methods is represented in Fig. 2.

Thus, for domain-specific applications (e.g., nuclear safety, cyber-security, urban seismic resilience, regional security, etc.), practitioners should prioritize methods aligning with control data availability, specificity of the control object and its critical functions, and system complexity.

3. Results and Discussion

Most of the relevant frameworks and methodologies for resilience cycle analysis (e.g., [4, 7, 15, 17, 56,

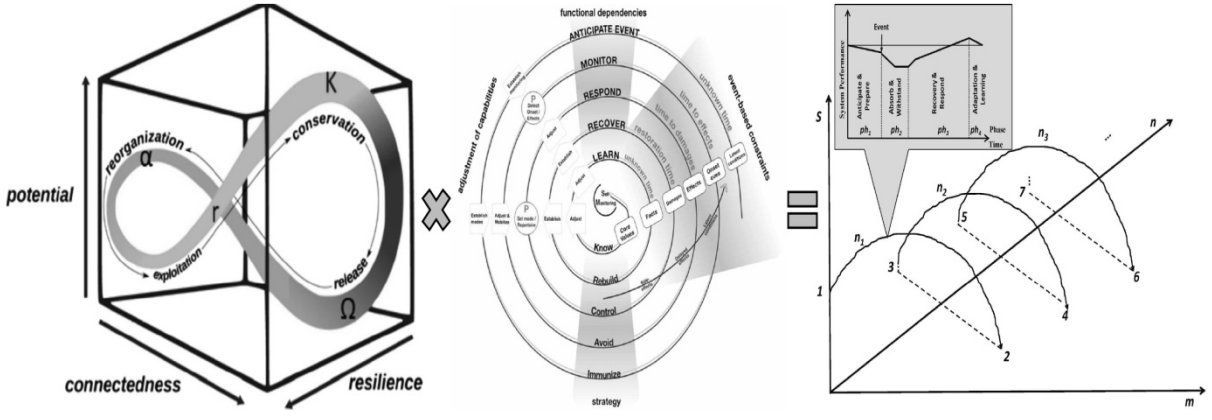

Fig. 2. The evolving of adaptive cycle, systemic resilience and resilience triangle models to resilience framework based on Ignatyev adaptation maximum phenomenon (combined from [2, 40, 46, 52])

57]) reviewed are based on indicators (quantitative, semi-quantitative or qualitative criteria), simulation and expert judgments. Four resilience capabilities, 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. In the last decade, comprehensive analysis of these resilience capabilities 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 [3].

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.

The overall resilience cycle/scenario is decomposed over five temporal phases which can be conceptualized by means of categorized performance indicators (system resilience capabilities such as sensitivity, anticipatory ability, resistivity, absorbability, responsiveness, recoverability, adaptability) that, in turn, can have values, providing the possibility to quantitatively or qualitatively describe each stage of the resilience cycle. In fact, some of these indices are poorly formalizeable, quantifiable and manageable [3, 57]. Verbal analysis of decisions [58] is an effective approach to meet the problems of resilience multicriteria assessment and optimization. As noted in [3], defining the critical functionality of an infrastructure system 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 express the physical meaning of such system properties as reliability, robustness, vulnerability, capacity, rapidity, etc., during all phases of resilience cycle schematically illustrated in Fig. 1.

The notations used in Fig. 1 are as follows [3]: $FL(t)$ is a system performance function indicating functionality level of the critical infrastructure at a particular time; 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 ($t_5 = t_{5''}$).

According to [2, 3, 57], the resilience cycle consists of interconnected time-dependent phases modeled as a continuous iterative (multi-cycle) process. The following temporal phases, each with distinct dynamic characteristics, formal representation and control actions, are commonly assigned and distinguished (see Fig. 1) [3, 57]:

Phase 1 Understand risks is applicable prior to an adverse event and emphasizes emerging risks and includes their early identification and monitoring; e.g. what could the "adverse event" be?

Phase 2 Anticipate/prepare is also applicable before the occurrence of an adverse event and includes planning and proactive adaptation strategies.

Phase 3 Absorb/withstand comes into action during the initial phase of the event and shall include the vulnerability analysis and the possible cascading/ripple effects; e.g. "how steep" is the absorption curve, and "how deep" down will it go.

Phase 4 Respond/recover is related to getting the adverse event under control as soon as possible, influencing the "how long" will it last, question. Further, it includes the post-event recovery; e.g. "how steep up" is the recovery curve for normalization of the functionality.

Phase 5 Adapt/transform/learn encompass all kinds of improvements made on the system and its environment; e.g. affecting "how well" the system is adapted after the event, and whether it is more resilient and "sustainable". The activities in this phase also lead to preparation for future events and hence, this resilience curve also exhibits a reoccurring cycle.

The resilience $CIR(t)$ of a critical infrastructure system at time t can be modeled as a function:

$$CIR(t) = f(A(t), \alpha(t), \tau(t), S(t), D(t)), \qquad (1)$$

where $A(t)$ is an absorption capacity, i.e., system ability to maintain function during disruption event; $\alpha(t)$ is an adaptation capacity, i.e., system ability to trans-

form/adjust structure and behavior over time; $\tau(t)^{-1}$ is a recovery rate, i.e., system rapidity of post-disruption restoration; $S(t)$ is a system state at time t, $S(t) \in R^n$ (an n-dimensional state vector representing key system variables, e.g., performance, capacity or functionality); $S_{crit} \in S(t)$ is a critical threshold (collapse may occur if $S(t) < S_{crit}$, i.e., system failure). $D(t)$ is a time-varying stochastic or deterministic disturbance (disruptions), i.e., external shocks or stressors; $D_{thresh} \in D(t)$ is a stress-test limit of the system.

The system performance is defined by a function:

$$\boldsymbol{E} \ : S \times T \to R^n, \qquad (2)$$

where performance function $FL(s(t),t)$ mapping system state to functionality level and represents the performance level of a critical infrastructure system at time $t \in T$.

The resilience curve is given by $FL(s(t))$ over time, with resilience metrics derived from this curve. Let $FL_0(t)$ be a nominal performance under normal operating conditions.

Thus, temporal phases of the resilience cycle can be formally written as dynamical equations:

(a) *Pre-disruption phase* ($t_0 \le t < t_1$) when the system prepares (redundancy arrangement $r(t)$, hardening investments $h(t)$, preventive-treatment, etc.) for potential adverse events, and the resilience is proactive (baseline resilience):

$$\frac{dFL(s(t))}{dt} = g(FL(s(t)), Rob_{base}) = c_r r(t) + c_h h(t) - \delta S(t), \quad (3)$$

where Rob_{base} is inherent robustness; c_r, c_h are efficacy coefficients; $r(t)$, $h(t)$ are the control variables; δ is a natural decay rate (e.g., infrastructure aging, etc.).

The chief goal of this phase is to maximize pre-event system robustness.

(b) *Disruption phase* ($t_1 \le t \le t_2$) when a disturbance $D(t)$ occurs, degrading system state $S(t)$.

During disruption system absorption and adaptation dynamics can be formulated as:

$$\frac{dFL(s(t))}{dt} = -\underbrace{\gamma_D D(t)}_{impact} + \underbrace{\gamma_\alpha \alpha(t) \cdot (FL_{\max} - FL(s(t)))}_{adaptation}, \quad (4)$$

where γ_D is vulnerability to disturbance coefficient; γ_α is absorption efficiency; FL_{max} is a maximum possible system performance.

The chief goal of this phase is to minimize performance loss of a system during disruption.

(c) *Recovery phase* ($t_3 \le t \le t_4$), including downtime period $t_2 < t < t_3$ (disrupted system state), when the system restores functionality, possibly to a new equilibrium:

$$\frac{dFL(s(t))}{dt} = \frac{1}{\tau}\left(FL_{\text{target}} - FL(s(t))\right) + \gamma_m m(t) + \eta(t), \quad (5)$$

where τ is a recovery time constant; repair rate τ^{-1} and adaptive upgrades $m(t)$ are control variables; γ_m is marginal gain from upgrades; $\eta(t)$ – noise or stochastic improvements.

The chief goal of this phase is to restore system functionality level.

(d) *Adaptation phase* ($t_4 < t \le t_5$) when the system improves its performance through transformation and post-disruption learning:

$$\frac{dFL(s(t))}{dt} = \gamma_\alpha \alpha(t) \cdot (FL_{\max} - FL(s(t))). \quad (6)$$

The chief goal of this phase is to update resilience strategies via learning. For this purpose, the knowledge integration and policy updates control variables may be used.

Total resilience over scenario time $[t_0, t_5]$ can be quantified as the integral of performance retention:

$$CIR = \frac{1}{t_5 - t_0} \int_{t_0}^{t_5} \left[\frac{FL(s(t))}{FL_{\text{nominal}}} - \lambda C(t) \right] dt, \quad (7)$$

where FL_{nominal} is the nominal (undisturbed) system performance, i.e., baseline (optimal) state $S(t)$; $C(t)$ is cost of control actions, specifically, $r(t)$ and $m(t)$; λ is cost-performance tradeoff parameter.

Time-discounted resilience management aims to find and implement optimal resilience ensuring policies (designing optimal contingency plan) $\pi^* = \{r^*(t), h^*(t), u^*(t), m^*(t)\}$ that maximize $CIR(t)$ while minimizing cost over time period $[t_0, t_5]$:

$$\max_{r,h,u,m} CIR(t) = \underbrace{\int_{t_0}^{t_5} \left[\frac{FL(s(t))}{FL_{\text{nominal}}} e^{-\beta t} \right] dt}_{\text{Performance retention}} - \underbrace{\int_{t_0}^{t_5} w \|C(t)\|^2 dt}_{\text{Control cost}} \quad (8)$$

subject to:

- state constraints: $S(t) \ge S_{crit}$;
- resilience capacity constraints: $0 \le CIR(t) \le CIR^{\max}$;
- budget constraint: $\int_{t_0}^{t_5} \left[w^T \cdot (r(t) + h(t) + u(t) + m(t)) \right] dt \le B_{\text{total}}$;
- control constraints: $r(t) \in R, h(t) \in H, u(t) \in U, m(t) \in M$;
- tochastic disruptions: $D(t) \sim$ Poison process or Markov point process,

where $u(t)$ is a control variable for resource allocation; β is a penalty for prolonged downtime; $\|C(t)\|^2$ is a cost of control actions; w^T are the weights prioritizing critical infrastructure sectors; B_{total} is a total budget (investments in preventive and reactive measures) to maintain and support the system resilience or improvement of its functionality level under disruptive conditions.

For uncertain environments, model $D(t)$ and $\alpha(t)$ as stochastic processes (e.g., Markov chains or

Wiener processes), leading to a resilience stochastic differential equation:

$$dS(t) = \mu(S,t)dt + \sigma(S,t)dW_t, \quad (9)$$

where W_t is a Wiener process, and μ, σ encode drift or diffusion terms.

System resilience can be maximized by dynamically tuning its capabilities $A(t)$, $\alpha(t)$, and $\tau(t)$.

The generic resilience cycle model emphasizes seamless transitions between phases and considers also interactions between different resilience cycles. The transition between phases is determined by specific conditions:

Preparedness to Absorption occurs when disruption happens at time t_1, $D(t) > D_{thresh}$.

Absorption to Recovery occurs when system stabilizes at $t = t_1 + (t_2 \pm t_3)$, where $\left\| \frac{dFL(s(t))}{dt} \right\| \le \varepsilon_{abs}$ or $t - t_1 \ge \tau_{abs}^{\max}$, and $D(t) = 0$ for Δt.

Recovery to Adaptation occurs when system performance reaches acceptable level: $FL(s(t),t) \ge \alpha \cdot FL_0(t)$ or $t - t_1 - \tau_{abs} \ge \tau_{rec}^{\max}$.

Adaptation to Preparedness occurs when system transformation and adaptation is complete or new cycle begins: $\left\| \frac{dFL(k(t))}{dt} \right\| \le \varepsilon_{adapt}$ or $t \ge t_0 + T$, and $CIR(t) = CIR^{\max}$ or $t \ge t_5 + \tau_{learn}$, where τ_{learn} is time period of system experience gathering from lessons learned.

For systems experiencing multiple disruptions, the formulations (1)-(8) are extended to account for learning across the cycles. Let $s^{(i)}(t)$ denote the system state during the i-th resilience cycle/scenario. The evolution of resilience capabilities across the cycles is given by:

$$s^{(i+1)}\left(t_0^{(i+1)}\right) = \phi\left(s^{(i)}\left(t_0^{(i)} + T^{(i)}\right), k^{(i)}\left(t_0^{(i)} + T^{(i)}\right)\right), \quad (10)$$

where ϕ captures how learning in one cycle influences initial conditions in the next cycle.

The learning rate across cycles can be quantified as:

$$\Lambda(i, i+1) = \frac{RL^{(i)} - RL^{(i+1)}}{RL^{(i)}}, \quad (11)$$

where $RL = \int_{t_1}^{t_1+\tau_{abs}+\tau_{rec}} [FL_0(t) - FL(s(t),t)]dt$ is the resilience loss under each cycle/scenario.

For multiple disruptions occurring over time $\{(D_1,T_1),(D_2,T_2),...,(D_n,T_n)\}$, the system performance trajectory follows:

$$FL(t) = FL_0(t) \cdot \prod_{i:t_i<t} \phi_i(t - t_i, s(t)), \quad (12)$$

where ϕ_i captures the proportional performance impact from disruption ii as a function of time since the disruption and current system state.

In this case, system adaptation capacity can be approximated as:

$$AC = \left(RL^{(i)} - RL^{(i+1)}\right) \cdot \left(\int_{t_1^{(i)}+\tau_{abs}^{(i)}+\tau_{rec}^{(i)}}^{t_{pl}^{(i+1)}} c_\alpha(\alpha(t))dt \right)^{-1},$$

where c_α is the adaptation cost function.

Proposed formalization aligns with Holling's ecological resilience and Bruneau's seismic resilience frameworks [5, 12], but to a greater extent fit to engineered and socio-technical infrastructure systems.

Principally, the formalized models of the temporal-phased resilience cycle considered can be used in two different ways as illustrated in [57], for the analysis and measuring the system resilience:

1) Treatment of the resilience cycle indirectly, as a conceptual model where indicators are used to measure the resilience in each phase indirectly, i.e. without considering the curve describing functionality of the system by means of the resilience curve.
2) Modeling the shape of the resilience curve $FL(t)$ directly and looking for "macro-indicators" (e.g. maximum loss of functionality, downtime, etc.), when the event is described as an exact scenario, and the time may be referred to as scenario time.

Moreover, the using potential of the proposed formalisms written in specific a manner can be extended with mathematical formulations given in [3] and [59]. Analyzing the formal models (1)-(12) it is worth to highlight that resilience of critical infrastructure systems must be considered as the diversity of future pathways accessible to a system rather than focusing on stability or recovery rate.

Conclusion

In fine, it should be noted that designing and implementing formal conceptual models of critical infrastructure systems resilience accounting temporal aspects of its operation is a complex, interdisciplinary problem. There are several key challenges arising in developing system resilience temporal models along with theoretic, computational, and practical issues and potential constraints. Critical infrastructures are nonlinear, interdependent, in some way inertial, and adaptive, making it difficult to model their temporal behavior, time lag and phase transitions. Triggering events (disruptions) are stochastic in timing, magnitude, and duration, while recovery efforts face unpredictable delays, increasing uncertainty in system resilience management. System resilience is not static. It is time-var-

ying and evolves due to degradation, adaptation, and learning of the system. Some of traditional metrics, e.g., time-to-recover or allowable downtime, are oversimplified. Critical infrastructure systems require real-time monitoring and tracking many state variables in the multidimensional attribute spaces, leading to the curse of dimensionality. At the same time, most critical infrastructure data is coarse-grained, while resilience models need high-resolution (more detailed) temporal disruption/recovery trajectories. System resilience management strategies must adapt on-the-fly and support real-time decision-making under uncertainty to provide predictive and adaptive control, but most control models are offline (pre-computed) without rolling time horizons. In addition, resilience maintenance standards and regulations vary by critical infrastructure sectors (energy, transport, healthcare, etc.), complicating cross-system modeling in tote. Not the least of the challenges is the traditional over-investing in redundancy and physical protection of critical entities may be economically unsustainable, while under-investing in critical infrastructure system robustness and resilience risks collapse. Without studying these issues, we risk underestimating dependent cascading failures like a cyber-attack collapsing both power and healthcare systems.

Situational conceptual models of system resilience manipulating spatial-temporal aspects provide groundbreaking advances in both theoretical foundations and practical resilience management. Conceptual models of system resilience cycle as a unified frameworks for dynamic resilience temporal modeling formalize time-varying disruptions, including cascading correlated failures (risks), and move beyond static "resilience triangles" to expanded time-explicit models integrating absorption (instantaneous robustness), adaptation (real-time adjustments), recovery (time-to-restore), and evolution (long-term learning). These models transform resilience from a reactive concept to a proactive, quantifiable science. Theoretically, they enable a rigorous math of "how systems fail and recover over time", and, practically, automate synthesis of digital shadows, models and twins of the complex dynamic systems that bend, but do not break.

The main contributions that distinguish system resilience cycle temporal models from traditional equilibrium-based deterministic resilience frameworks lie in the following scope: classical models such as static snapshots like "resilience triangles" measure only area under recovery curves, while temporal models take into consideration time-to-absorb (how fast a system degrades), recovery acceleration (how adaptation shortens downtime), and learning effects (how post-disruption upgrades improve future resilience). Generally speaking, resilience time-discounted models are the basis for combining continuous dynamics with discrete events to model complex failures that are not independent as self-exciting processes as stated stochastic resilience theory unlike general reliability theory [60].

In this study we have summarized, examined and proposed conceptual models of the critical infrastructures resilience cycle formalizing system operation temporal phases, when adverse events occurs, and written using mathematical formulations from general system and control theory subject to peculiarities of the state-of-the-art resilience concept and safety science. These models fit both to resilience management of critical entities and other types of complex dynamic systems to a wide extent. The formalized conceptual models of the resilience cycle provide a formal basis for the further simulation, automation and coordination of system performance control procedures under extreme conditions. It is necessary for the knowledge unified formal representation and structuring on the various aspects of system resilience management, as well as in order to generate and analyze scenarios for the preventive analytics of potential threatening and emergency situations. These models are distinguished by the completeness of conceptual definition of the resilience cycle phases and related temporal aspects of its management. Conceptual models are defined in the form of strict theoretical formalisms. Relations that determine the phased structure of the system resilience cycle are defined on the sets of model elements. Along the lines of the further research, the practical implementation of the designed models will be carried out in the form of applied system resilience ontology. Such ontology is intended to ensure semantic interoperability of heterogeneous elements of the situational management information structure at all stages of the system resilience maintenance life-cycle.

Resilience temporal models are not just intended for its incremental improvements. They redefine contingency plans and analyze how the system prepares (proactive hardening), responds (real-time adaptation), and evolves (post-disruption learning) under actuating multiple threats when managing its resilience. Nevertheless, most of known temporal models of system resilience have their own typical limitations such as scalability, computational complexity, human-in-the-loop factor, influencing the delay or misinterpret adaptive controls of system resilience (unpredictable human behavior), validation difficulty, and other domain-specific contingencies.

Temporal models of infrastructure system resilience can find applications for such critical domains as critical infrastructure protection (power grids,

transport networks, water systems, etc.), cybersecurity (adaptive cyber-defense, smart manufacturing, etc.), disaster response (flood resilience, wildfire management, etc.), healthcare (pandemic response, climate adaptation, etc.), logistics (resilient supply chains, inventory management, etc.), national security (international conflicts forecasting, terrorism prevention, defenses allocation to chokepoints, etc.), and other, where proactive, adaptive, and cost-effective situational management is utterly needed. Thereto, the models tailored implementation within the decision support systems provides several practical benefits such are rational choice of faster recovery schedules, evaluation of mitigation scenarios, cost savings, risk reduction, improved action planning, and enhanced control coordination for the safety and resilient operation of critical entities (systems).

References

1. *Masloboev A.V.* Formal models of the regional critical infrastructures resilience. Proceedings of the Institute for system analysis RAS. 2022;72(3):59-80. (In Russ.)
2. *Masloboev A.V.* Application of the Ignatyev adaptative maximum principle in management of critical infrastructures resilience. Reliability and quality of complex systems. 2023;4(44):165-178.
3. *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. Reliability and quality of complex systems. 2024;3(47):130-156.
4. *Yang Zh. et al.* Indicator-based resilience assessment for critical infrastructures – A review. Safety Science. 2023;160:106049.
5. *Mottahedi A. et al.* The Resilience of Critical Infrastructure Systems: A Systematic Literature Review. Energies. 2021;14(6):1571.
6. *Jovanovic A.S.* Managing emerging risks for enhanced resilience: aligning approaches internationally. Proceedings of the 29th European Safety and Reliability Conference. In *M. Beer* and *E. Zio* (Ed.), European Safety and Reliability Association. Singapore: Research Publishing. 2019. P. 2953-2960.
7. *Øien K., Bodsberg L., Jovanović A.* Resilience assessment of smart critical infrastructures based on indicators. Safety and Reliability: Safe Societies in a Changing World. In *Haugen et al.* (Ed.). London: CRC Press. 2018. P. 1269-1277.
8. *Pursiainen C., Kytömaa, E.* From European critical infrastructure protection to the resilience of European critical entities: what does it mean?. Sustainable and Resilient Infrastructure. 2022;8(sup1):85-101.
9. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. URL: https://base.garant.ru/407633886/. (In Russ.)
10. Aligning the resilience-related research efforts in the EU-DRS projects. Joint Workshop DRS7&14 projects. Brussels, September 13-14, 2017. *A. Jovanović, E. Bellini* (Eds.), Steinbeis Edition, Stuttgart, Germany. 2017. 165 p.
11. *Mentges A., Halekotte L., Schneider M., Demmer T., Lichte D.* A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. International Journal of Disaster Risk Reduction. 2023;96:103893.
12. *Holling C.S.* Resilience and stability of ecological systems. Annual review of ecology and systematic. 1973;4(1):1-23.
13. *Taleb N.N.* The Black Swan: Under the Sign of Unpredictability / Ed. M. Tyunkina. Moscow, KoLibri Publishing House. 2010. 528 p. (In Russ.)
14. ISO/TS 31050:2023 Guidance for managing emerging risks to enhance resilience. URL.: https://www.iso.org/obp/ui/en/#iso:std:iso:ts:31050:ed-1:v1:en.
15. *Jovanovic A. et al.* Smart Resilience D1.2: Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infrastructure resilience. EU project SmartResilience. Project No. 700621. Stuttgart, Germany. 2016. 174 p..
16. *Cutter S.L.* The landscape of disaster resilience indicators in the USA. Natural hazards. 2016;80(2):741-758.
17. *Rød B., Lange D., Theocharidou M., Pursiainen C.* From Risk Management to Resilience Management in Critical Infrastructure. Journal of Management in Engineering. 2020;36(4):04020039.
18. *Pesch-Cronin K.A., Marion N.E.* Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective. 2nd Edition. New York: Routledge. 2024. 278 p.
19. *Pospelov D.A.* Situational Management. Theory and Practice. 2nd ed. Moscow, URSS. 2021. 288 p. (In Russ.)
20. *Tsygichko V.N., Chereshkin D.S., Smolyan G.L.* Critical Infrastructure Safety. Moscow, URSS. 2019. 200 p. (In Russ.)
21. *Chereshkin D.S., Roizenzon G.V., Britkov V.B.* Application of Artificial Intelligence Methods for Risk Analysis in Socioeconomic Systems. Information Society. 2020;3:14-24. (In Russ.)

22. *Barkin A.I.* Absolute Stability of Control Systems. Moscow, URSS. 2020. 176 p. (In Russ.)
23. *Bogdanov A.A.* Tectology: General Organizational Science. Moscow, URSS. 2019. 680 p. (In Russ.)
24. *Trapeznikov V.A., Raibman N.S., Chadeev V.M., et al*. ASI – an Adaptive System with Identification. Moscow, Institute of Control Problems. 1980. 67 p. (In Russ.)
25. *Petrov B.N., Rutkovsky V.Yu., Zemlyakov S.D.* Adaptive Coordinate-Parametric Control of Non-Stationary Objects. Moscow: Nauka. 1980. 244 p. (In Russ.)
26. *Bashlykov A.A., Eremeev A.P.* Fundamentals of Designing Intelligent Decision Support Systems in Nuclear Energy. Moscow: INFRA-M. 2024. 351 p. (In Russ.)
27. *Tsygichko V.N., Smolyan G.L., Solntseva G.N.* The Human Factor as a Threat to the Safety of Critical Facilities. Science of Europe. 2016;2(1):60-65. (In Russ.)
28. *Popkov Yu.S.* Randomization and Entropy in Data Processing, Dynamic Systems, and Machine Learning. Moscow, URSS. 2023. 300 p. (In Russ.)
29. *Makarov V.L., Bakhtizin A.R.* Social Modeling – A New Computer Breakthrough (Agent-Based Models). Moscow: Economica. 2013. 295 p. (In Russ.)
30. *Gvishiani D.M.* Selected Works on Philosophy, Sociology, and Systems Analysis / Ed. by Yu. S. Popkov V.N. Sadovsky and A.A. Seitov. Moscow: "Canon+" ROOI "Rehabilitation". 2007. 672 p. (In Russ.)
31. Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies. Advanced Sciences and Technologies for Security Applications. In *D. Gritzalis*, *M. Theocharidou*, *G. Stergiopoulos* (Ed.), Springer Cham, Springer Nature Switzerland AG. 2019. 313 p.
32. *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.
33. *Naderpajouh N., Matinheikki J., Keeys L.A., Aldrich D.P., Linkov I.* Resilience science: Theoretical and methodological directions from the juncture of resilience and projects. International Journal of Project Management. 2023;41(8):102544.
34. *Emelyanov S.V., Korovin S.K*. New Types of Feedback: Control under Uncertainty. Moscow, Nauka. Fizmatlit. 1997. 352 p. (In Russ.)
35. *Yang Zh. et al.* A multi-criteria framework for critical infrastructure systems resilience. International Journal of Critical Infrastructure Protection. 2023;42:100616.
36. *Dan G., Shan M., Owusu E.K.* Resilience Assessment Frameworks of Critical Infrastructures: State-of-the-Art Review. Buildings. 2021;11(10):464.
37. *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.
38. *Almaleh A.* Measuring Resilience in Smart Infrastructures: A Comprehensive Review of Metrics and Methods. Applied Sciences. 2023;13(11):6452.
39. GOST R ISO 31000:2019 Risk management – Principles and Guidelines. Moscow: Standardinform. 2020. 19 p. (In Russ.)
40. *Lundberg J., Johansson B.JE.* Systemic resilience model. Reliability Engineering and System Safety. 2015;141:22-32.
41. *Sweetapple C., Fu G., Farmani R., Butler D.* General resilience: Conceptual formulation and quantitative assessment for intervention development in the urban wastewater system. Water Research. 2022;211. Article no.: 118108.
42. *Xu Zh., Ng D.J.X., Easwaran A.* Automatic Generation of Hierarchical Contracts for Resilience in Cyber-Physical Systems. Proceedings of the IEEE 25th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), August, 18-21, 2019. Hangzhou, China. 2020;1:156-166.
43. *Hollnagel E.* Safety-I and Safety-II: The Past and Future of Safety Management. 1st Edition. London: CRC Press. 2014. 200 p.
44. *Schrenk H., Garcia-Perez C., Schreiber N., zu Castell W.* QtAC: An R-package for analyzing complex systems development in the framework of the adaptive cycle metaphor. Ecological Modelling. 2022;466:109860.
45. *Christensen V.* Emergy-based ascendency. Ecological Modelling. 1994;72(1-2):129-144.
46. Panarchy: Understanding Transformations in Human and Natural Systems. *Gunderson L.H., Holling C.S.* (Eds.), Island Press, Washington D.C. 2002. 536 p.
47. *Gohil M., Mehta D., Shaikh M.* An integration of geospatial and fuzzy-logic techniques for multi-hazard mapping. Results in Engineering. 2024;21:101758.
48. *Huang J., Li L., Jiang P., Zhang S.* DEMATEL-Based ANP Model for Identifying Critical Indicators in Sustainable Emergency Material Reserve Systems. Sustainability. 2024;16(12):5263.
49. *Tan Zh., Wu B., Che A.* Resilience modeling for multi-state systems based on Markov process-

es. Reliability Engineering and System Safety. 2023;235:109207.
50. *Spaan M.T.J.* Partially Observable Markov Decision Processes. Reinforcement Learning. Adaptation, Learning, and Optimization. In: *Wiering M., van Otterlo M.* (eds), Springer, Berlin, Heidelberg. 2012;12:387-414.
51. *Ahmadilivani M.H, Raik J., Daneshtalab M., Kuusik A.* Analysis and improvement of resilience for long short-term memory neural networks. Proceedings of the 36th IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT). Juan-Les-Pins, France, October 3-5, 2023. IEEE 2023.
52. *Tang J., Han S., Wang J., He B., Peng J.* A Comparative Analysis of Performance-Based Resilience Metrics via a Quantitative-Qualitative Combined Approach: Are We Measuring the Same Thing?. International Journal of Disaster Risk Science. 2023;14:736-750.
53. *Ouyang M.* Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering and System Safety. 2014;121:43-60.
54. *Kulak O., Cebi S., Kahraman C.* Applications of axiomatic design principles: A literature review. Expert Systems with Applications. 2010;37(9):6705-6717.
55. *Chen W., Zhang L.* Resilience assessment of regional areas against earthquakes using multi-source information fusion. Reliability Engineering and System Safety. 2021;215:107833.
56. *Rehak D. et al.* Critical Entities Resilience Failure Indication. Safety Science. 2024;170:106371.
57. *Jovanović A. 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.
58. *Larichev O.I.* Verbal Analysis of Decisions. Moscow, Nauka. 2006. 181 p. (In Russ.)
59. *Jovanović A. 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.
60. *Weimar A.R.* Stochastic Models for Resilience Assessment and Improvement. USF Tampa Graduate Theses and Dissertations. University of South Florida. 2022. 73 p.

Andrey V. Masloboev. Leading Researcher, Associate Professor, Doctor of Technical Sciences, Federal Research Centre «Kola Science Centre of the Russian Academy of Sciences», Putilov Institute for Informatics and Mathematical Modeling, 14 Fersmana St., Apatity, Murmansk region, 184209, Russia. E-mail: a.masloboev@ksc.ru.

Темпоральные концептуальные модели жизненного цикла жизнеспособности динамических систем для управления критическими инфраструктурами*

А.В. Маслобоев

Федеральный исследовательский центр «Кольский научный центр Российской академии наук», г. Апатиты, Россия

Аннотация. Исследования направлены на разработку моделей, методов и информационных технологий для проблемного мониторинга и поддержки принятия интерпретируемых решений в задачах управления критически важными инфраструктурными системами с целью обеспечения их устойчивого функционирования в условиях неблагоприятных воздействий природного и искусственно инициированного характера. Для единого формализованного представления информационной структуры, процессов и задач обеспечения безопасности и устойчивости исследуемого класса систем разработаны концептуальные модели жизненного цикла функционирования критических инфраструктур, учитывающие темпоральные аспекты управления их динамикой и базирующиеся на положениях современной концепции жизнеспособности (resilience) сложных систем. Модели обеспечивают формальную основу для имитационного моделирования, автоматизации и координации процессов управления жизнеспособностью инфраструктурных систем на этапах их жизненного цикла с целью генерации и анализа возможных сценариев возникновения инициирующих событий и связанных с ними потенциальных угроз. На практике предложенные модели могут быть реализованы в виде прикладной онтологии жизнеспособности критических инфраструктур, которая сможет найти применение в системах ситуационного управления и превентивной аналитики безопасности критически важных объектов.

Ключевые слова: *концептуальное моделирование, темпоральная модель, жизненный цикл, управление, жизнеспособность, критическая инфраструктура, динамическая система*.

DOI: 10.14357/20790279250408 **EDN:** MSIWLZ

Литература

1. *Маслобоев А.В.* Формальные модели жизнеспособности региональных критических инфраструктур // Труды ИСА РАН. 2022. Т. 72. № 3. С. 59-80.
2. *Masloboev A.V.* Application of the Ignatyev adaptative maximum principle in management of critical infrastructures resilience // Reliability and quality of complex systems. 2023;4(44):165-178.
3. *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 // Reliability and quality of complex systems. 2024;3(47):130-156.
4. *Yang Zh. et al.* Indicator-based resilience assessment for critical infrastructures – A review // Safety Science. 2023;160:106049.
5. *Mottahedi A. et al.* The Resilience of Critical Infrastructure Systems: A Systematic Literature Review // Energies. 2021;14(6):1571.
6. *Jovanovic A.S.* Managing emerging risks for enhanced resilience: aligning approaches internationally // Proceedings of the 29th European Safety and Reliability Conference. In *M. Beer* and *E. Zio* (Ed.), European Safety and Reliability Association. Singapore: Research Publishing. 2019. P. 2953-2960.
7. *Øien K., Bodsberg L., Jovanović A.* Resilience assessment of smart critical infrastructures based on indicators // Safety and Reliability: Safe Societies in a Changing World. In Haugen et al. (Ed.). London: CRC Press. 2018. P. 1269-1277.
8. *Pursiainen C., Kytömaa, E.* From European critical infrastructure protection to the resilience of European critical entities: what does it mean? // Sustainable and Resilient Infrastructure. 2022;8(1);85-101.
9. Директива 2022/2557 Европейского Парламента и Совета Европейского Союза от 14 декабря 2022 года «Об устойчивости критически важных организаций». URL: https://base.garant.ru/407633886/
10. Aligning the resilience-related research efforts in the EU-DRS projects // Joint Workshop DRS7&14 projects. Brussels, September 13-14, 2017. *A. Jovanović, E. Bellini* (Eds.), Steinbeis Edition, Stuttgart, Germany. 2017. 165 p.
11. *Mentges A., Halekotte L., Schneider M., Demmer T., Lichte D.* A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures // International Journal of Disaster Risk Reduction. 2023;96. Article no.: 103893.
12. *Holling C.S.* Resilience and stability of ecological systems // Annual review of ecology and systematic. 1973;4(1):1-23.

* Работа выполнена в рамках государственного задания ИИММ КНЦ РАН (НИР № FMEZ-2025-0054).

13. *Талеб Н.Н.* Черный лебедь. Под знаком непредсказуемости / Под ред.М. Тюнькиной. М.: Издательство КоЛибри. 2010. 528 с.
14. ISO/TS 31050:2023 Guidance for managing emerging risks to enhance resilience. URL.: https://www.iso.org/obp/ui/en/#iso:std:iso:ts:31050:ed-1:v1:en.
15. *Jovanovic A. et al.* Smart Resilience D1.2: Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infrastructure resilience // EU project SmartResilience. Project No. 700621. Stuttgart: Germany. 2016. 174 p.
16. *Cutter S.L.* The landscape of disaster resilience indicators in the USA // Natural hazards. 2016;80(2):741-758.
17. *Rød B., Lange D., Theocharidou M., Pursiainen C.* From Risk Management to Resilience Management in Critical Infrastructure // Journal of Management in Engineering. 2020;36:4.
18. *Pesch-Cronin K.A., Marion N.E.* Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective. 2nd Edition. New York: Routledge. 2024. 278 p.
19. *Поспелов Д.А.* Ситуационное управление. Теория и практика. 2 изд. М.: URSS. 2021. 288 с.
20. *Цыгичко В.Н., Черешкин Д.С., Смолян Г.Л.* Безопасность критических инфраструктур. М.: URSS. 2019. 200 с.
21. *Черешкин Д.С., Ройзензон Г.В., Бритков В.Б.* Применение методов искусственного интеллекта для анализа риска в социально-экономических системах // Информационное общество. 2020. № 3. С. 14–24.
22. *Баркин А.И.* Абсолютная устойчивость систем управления. М.: URSS. 2020. 176 с.
23. *Богданов А.А.* Тектология: Всеобщая организационная наука. М.: URSS. 2019. 680 с.
24. АСИ – адаптивная система с идентификацией / В.А. Трапезников, Н.С. Райбман, В.М. Чадеев и др. М.: Ин-т проблем управления. 1980. 67 с.
25. *Петров Б.Н., Рутковский В.Ю., Земляков С.Д.* Адаптивное координатно-параметрическое управление нестационарными объектами. М.: Наука. 1980. 244 с.
26. *Башлыков А.А., Еремеев А.П.* Основы конструирования интеллектуальных систем поддержки принятия решений в атомной энергетике. М.: ИНФРА-М. 2024. 351 с.
27. *Цыгичко В.Н., Смолян Г.Л., Солнцева Г.Н.* Человеческий фактор как угроза безопасности критически важных объектов // Science of Europe. 2016. Т. 2, № 1. С. 60–65.
28. *Попков Ю.С.* Рандомизация и энтропия в обработке данных, динамических системах, машинном обучении. М.: URSS. 2023. 300 с.
29. *Макаров В.Л., Бахтизин А.Р.* Социальное моделирование – новый компьютерный прорыв (агент-ориентированные модели). М.: Экономика. 2013. 295 с.
30. *Гвишиани Д. М.* Избранные труды по философии, социологии и системному анализу / Под ред. Ю. С. Попкова, В.Н. Садовского, А.А. Сеитова. М.: «Канон+» РООИ «Реабилитация». 2007. 672 с.
31. Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies // Advanced Sciences and Technologies for Security Applications. In *D. Gritzalis*, *M. Theocharidou*, *G. Stergiopoulos* (Ed.), Springer Cham, Springer Nature Switzerland AG. 2019. 313 p.
32. *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.
33. *Naderpajouh N., Matinheikki J., Keeys L.A., Aldrich D.P., Linkov I.* Resilience science: Theoretical and methodological directions from the juncture of resilience and projects // International Journal of Project Management. 2023;41(8):102544.
34. *Емельянов С.В., Коровин С.К.* Новые типы обратной связи: Управление при неопределенности. М.: Наука. Физматлит. 1997. 352 с.
35. *Yang Zh. et al.* A multi-criteria framework for critical infrastructure systems resilience // International Journal of Critical Infrastructure Protection. 2023;42:100616.
36. *Dan G., Shan M., Owusu E.K.* Resilience Assessment Frameworks of Critical Infrastructures: State-of-the-Art Review // Buildings. 2021;11(10):464.
37. *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.
38. *Almaleh A.* Measuring Resilience in Smart Infrastructures: A Comprehensive Review of Metrics and Methods // Applied Sciences. 2023;13(11):6452.
39. ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и Руководство. М.: Стандартинформ. 2020. 19 с.
40. *Lundberg J., Johansson B.JE.* Systemic resilience model // Reliability Engineering and System Safety. 2015;141:22-32.

41. *Sweetapple C., Fu G., Farmani R., Butler D.* General resilience: Conceptual formulation and quantitative assessment for intervention development in the urban wastewater system // Water Research. 2022;211:118108.
42. *Xu Zh., Ng D.J.X., Easwaran A.* Automatic Generation of Hierarchical Contracts for Resilience in Cyber-Physical Systems // Proceedings of the IEEE 25th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), August, 18-21, 2019. Hangzhou, China. 2020;1:156-166.
43. *Hollnagel E.* Safety-I and Safety-II: The Past and Future of Safety Management. 1st Edition. London: CRC Press. 2014. 200 p.
44. *Schrenk H., Garcia-Perez C., Schreiber N., zu Castell W.* QtAC: An R-package for analyzing complex systems development in the framework of the adaptive cycle metaphor // Ecological Modelling. 2022;466:109860.
45. *Christensen V.* Emergy-based ascendency // Ecological Modelling. 1994;72(1-2):129-144.
46. Panarchy: Understanding Transformations in Human and Natural Systems. *Gunderson L.H., Holling C.S.* (Eds.), Island Press, Washington D.C. 2002. 536 p.
47. *Gohil M., Mehta D., Shaikh M.* An integration of geospatial and fuzzy-logic techniques for multi-hazard mapping // Results in Engineering. 2024;21:101758.
48. *Huang J., Li L., Jiang P., Zhang S.* DEMATEL-Based ANP Model for Identifying Critical Indicators in Sustainable Emergency Material Reserve Systems // Sustainability. 2024;16(12). Article no.: 5263.
49. *Tan Zh., Wu B., Che A.* Resilience modeling for multi-state systems based on Markov processes // Reliability Engineering and System Safety. 2023;235:109207.
50. *Spaan M.T.J.* Partially Observable Markov Decision Processes // Reinforcement Learning. Adaptation, Learning, and Optimization. In: *Wiering M., van Otterlo M.* (eds), Springer, Berlin, Heidelberg. 2012;12:387-414.
51. *Ahmadilivani M.H, Raik J., Daneshtalab M., Kuusik A.* Analysis and improvement of resilience for long short-term memory neural networks // Proceedings of the 36th IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT). Juan-Les-Pins, France, October 3-5. 2023. IEEE 2023.
52. *Tang J., Han S., Wang J., He B., Peng J.* A Comparative Analysis of Performance-Based Resilience Metrics via a Quantitative-Qualitative Combined Approach: Are We Measuring the Same Thing? // International Journal of Disaster Risk Science. 2023;14:736-750.
53. *Ouyang M.* Review on modeling and simulation of interdependent critical infrastructure systems // Reliability Engineering and System Safety. 2014;121:43-60.
54. *Kulak O., Cebi S., Kahraman C.* Applications of axiomatic design principles: A literature review // Expert Systems with Applications. 2010;37(9):6705-6717.
55. *Chen W., Zhang L.* Resilience assessment of regional areas against earthquakes using multi-source information fusion // Reliability Engineering and System Safety. 2021;215:107833.
56. *Rehak D. et al.* Critical Entities Resilience Failure Indication // Safety Science. 2024;170:106371.
57. *Jovanović A. 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.
58. *Ларичев О.И.* Вербальный анализ решений. М.: Наука. 2006. 181 с.
59. *Jovanović A. 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.
60. *Weimar A.R.* Stochastic Models for Resilience Assessment and Improvement. USF Tampa Graduate Theses and Dissertations. University of South Florida. 2022. 73 p.

Маслобоев Андрей Владимирович. Федеральный исследовательский центр «Кольский научный центр Российской академии наук», Институт информатики и математического моделирования им. В.А. Путилова, г. Апатиты, Россия. Ведущий научный сотрудник. Доктор технических наук, доцент. Область научных интересов: системный анализ, моделирование социально-экономических систем, ситуационное управление, теория безопасности систем, мультиагентные системы. E-mail: a.masloboev@ksc.ru