Decision-making support of emergency risk identification in complex hierarchical control systems

Volodymyr Sabat[1,*,†], Bohdan Durnyak[1,†], Myroslava Kulynych[1,†], Yurii Lozynskyi[2,†] and Pavlo Hibey[1,†]

[1] *Ukrainian Academy of Printing, 19 Pid Holoskom Str., Lviv, 79061, Ukraine*
[2] *Lviv State University of Internal Affairs, 26 Horodotska Str., Lviv, 79007, Ukraine*

Abstract

An analysis of a complex man-made hierarchical structure with an automated control and document management system is carried out in the conditions of active information and resource attacks, using the category algebra, which allows detecting attacks on a dynamic system, determining the risk levels of emergency situations and creating appropriate countermeasures. For the first time, the methodology of constructing categorical models for the representation of a dynamic hierarchical structure in the space of states is substantiated and developed, diagrams of energy-active objects of a dynamic system are provided, taking into account the effect of resource and information attacks on it, and methods of decision-making in emergency situations using risk assessment. For the first time, a structural diagram of the balance of the game between threats and control in the system is formed, taking into account the factors of threats and their influence on the objects of the system, on the basis of which a functional diagram of the information-resource hierarchy of the aggregated system control in the mode of countering threats is proposed. For the first time, the categorical diagram of an information attack is substantiated and the systemology of the formation of the object structure and the assessment of the dynamic state under resource threats and information attacks is proposed. As a result of the research, a hierarchical structure of the control system of the technological complex is formed under the risk of emergency situations, with the selection of security features of the document flow in the formation of control decisions at the techno-aggregate, operational administrative and strategic levels, which allows the use of the proposed methodology in the conditions of decision-making support during the functioning of complex hierarchical control systems.

Keywords

Decision-making support, categorical models, man-made systems, threats, risk assessment, hierarchical systems control.

ICyberPhyS-2024: 1st International Workshop on Intelligent & CyberPhysical Systems, June 28, 2024, Khmelnytskyi, Ukraine

* Corresponding author.
† These authors contributed equally.
v_sabat@ukr.net (V. Sabat); bohdan.durnyak@gmail.com (B. Durnyak); kumyr@ukr.net (M. Kulynych)
nevdet@ukr.net (Yu. Lozynskyi); pavlo.hibey@gmail.com (P. Hibey)
0000-0001-8130-7837 (V. Sabat); 0000-0003-1526-9005 (B. Durnyak); 0000-0002-9271-7855 (M. Kulynych); 0000-0003-2908-7747 (Yu. Lozynskyi); 0009-0008-2034-1060 (P. Hibey)

© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-3736/paper17.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

1. Introduction

The structure of the hierarchical man-made control system has a complex organization, so it is not an easy task to cover all aspects of its functioning, to present and identify energy-information connections. The problem is especially complicated if the dynamic system is affected by negative factors in the form of information and resource attacks, which can lead to uncontrolled changes in the state of aggregates and objects in the technological cycle of system control. In addition, the action of information and infrastructure attacks of an aggressive type can lead to the destruction of hierarchical connections and the system structure, which, in turn, threatens the emergence of emergency situations with a high level of accident risk. These problems are not fully solved both in the classical control theory and in modern approaches based on system analysis. Only the use of the category algebra by constructing diagrams of the structure of connections and determining the cores of influence on the system space of states allows detecting attacks on a dynamic system and creating means of countering possible attacks.

To achieve the goal of scientific research, it is necessary to solve the following tasks:

- to justify the use of the category algebra methods for solving the problems of constructing the structures of hierarchical dynamic systems with complex connections and under external negative influences;
- to construct categorical structural diagrams of transformations in an energy-active system under the threats, in the space of states and dynamics in time of a complex system;
- to propose a categorical representation of the model of threats to the system and to develop a structural diagram of the game between threats and control in the system;
- to develop a functional scheme of information-resource countermeasures against threats in the hierarchy of the man-made system and the hierarchical structure of the control system of the technological complex at risk.

2. Related works

The analysis of the problem of emergency and risk situations under the influence of active threats and attacks has shown the importance of building models for detecting attacks by the way they affect system objects. The textbook of domestic scientists [1] substantiates the use of risk assessment methods in determining the reliability of technical systems and humans, reveals the basic concepts, essence, goals and methods of information protection; multi-criteria methods for assessing the correctness of decisions in crisis situations are considered in the scientific work [2], which proposes a solution to this problem, which allows us to assert that the decision was made correctly in this particular case when ensuring the information security of a particular object; article [3] provides an overview of the concept of industry 4.0 concept with equivalent terms, basic technologies and reference structures for its implementation, it is substantiated that this paradigm is a promising result of the merger and integration of both existing and revolutionary technologies; categorized models for representing the structure and dynamic state of hierarchical systems to identify attack factors and risks are given in the collective work [4]; the theory of digital control systems that

describes the functionality of the system, explains the modeling process, presents a solution to the problem, and discusses the results of hierarchical system management processes is proposed in [5]; paper [6] presents research on assessing the occurrence of risk situations for automated control systems of metallurgical enterprises under active threats and attacks. With the help of the above-mentioned works, structural representations of hierarchical dynamic systems with complex connections and under the influence of external attacks have been developed, using also international standards in the field of information security [7], methods of software and hardware protection of network technologies. based on big data [8] and preventive security measures [9].

The concept of smart manufacturing and its impact on the future automation of labor with decision-making technology is proposed in [10]. The author identifies three possible future scenarios of production automation: digital production flows, self-organized production network, and cloud-based production equipment as a service.

The scientific article [11] describes methods for building risk models in a threat system using semantic analysis of the text of documents for the presence of anomalies in their semantic parameters. Paper [12] analyzes the concepts of risk and safety of subway passengers in cases of malicious man-made incidents. As a result, using the example of the Athens subway system, the importance of passenger protection to improve safety and avoid threatening conditions is proved. These studies reveal the essence of hierarchical systems and their vulnerability to man-made disasters under the influence of external attacks and internal threats.

Modern developed methods for analyzing general industrial control systems for hierarchical technogenic structures are presented in [13, 14]. Work [15] consider applied decision support systems based on risk analysis of complex systems.

Paper [16] presents the use of an object-oriented Bayesian network for scenario risk assessment. A model of probabilistic coverage of key factors affecting accidents in fragmented structures is developed. The study in [17] proposes a model-based methodology for hybrid management of risk assessment of reliability, availability, maintainability, and safety for critical systems. The result is a method for analyzing cybersecurity risks for industrial control systems. Agrawal et al. [18] defined an ontology to represent ISO/IEC 27,005, 2018 standards to provide a step-by-step understanding of the meaning of security concepts and their interrelationships. Researchers such as Blanco et al. [19] reviewed 31 security ontologies. Both studies group security ontologies into three categories: general, specific, and theoretical.

Two popular risk assessment methods tested for the nuclear industry use probabilistic risk assessment [20, 21], while others use dynamic Bayesian networks [22, 23]. The human factor and reliability in risk assessment and management in the context of threats and attacks are considered in the scientific paper [24]. Paper [25] presents a model of a dynamic and iterative process in which experts discuss a multi-criteria decision-making problem in complex management structures. The considered methods of modeling fuzzy preferences are aimed at evaluating, comparing, selecting, prioritizing and/or organizing alternatives.

3. Materials and Methods

Let one construct the structure of the hierarchical system in a categorical form. To do this, its main elements and parameters should be defined: [4] T is the set of moments of time on the

ordered set Z of cyclic numbers; $U \subset K^m$ is the set of values of control actions on the *m-dimensional* vector space; Y is the set of values of input parameters on K^0; X is the space of states on K^0; Ω is the space of input actions for which $\omega_i: T \to U$, $\omega_i \in \Omega$; Γ is the space of output parameters $\Gamma: T \to Y$; α is the display of the transition when the system status changes $\alpha: (T \times T \times X \times \Omega) \to X$.

For the moment of each transition one has:

$$(t+1, t, x, \omega) \longmapsto \varphi(t+1, t, x, \omega) = Fx(t) + g\omega(t), \quad (1)$$

where F, g are matrices $(n \times n), (n \times m)$ over K; φ is the output representation $T \times X \to Y$for which $(t, x) \longmapsto \varphi(t, x) = H(x)$ is true.

To study the dynamics of the system for each component, it is necessary to identify the model (input-output function) as a transfer function that connects the initial state of the system $y(t)$ with the input control signal $u\big(x(t,\tau)\big)$ through the parametric-time operator $A(t,\tau): x(t,\tau) \to y(t, \tau + \Delta\tau)$.

For linear systems in the classical theory, the "input-output" representation function f is associated with the concept of the transfer function [5].

If there is some homomorphism for the transfer function f in the structure of dynamic systems $S_d$then it can be represented in the form: $f(\omega) = \sum_{i=1}^{m} \omega_i f(l_i)$, where $f(l_i)$ describes the power series. [4]

If there is a factorization for f which is described by a commutative diagram $K[2]$ is a homomorphism, then the system $S_d(f, \Omega, \Gamma)$ will have a realized structure in the space $X_f \subset X$, i.e.$f\big(\Psi_f \cdot l_K\big) = \big(H_f \cdot g_f\big)\big(\Psi_f \cdot l_K\big)$ (Fig. 1).

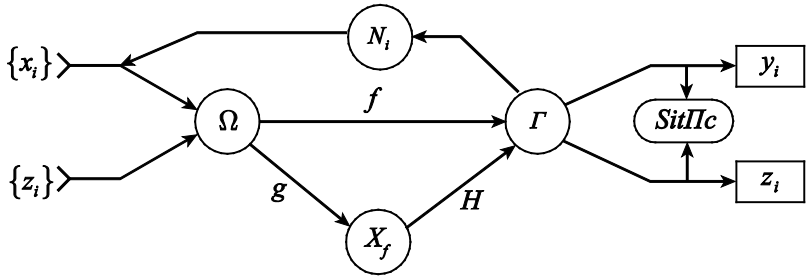

Figure 1: Realized dynamic structure in the space of states

The implementation of the matrix transfer function for an object with interconnected technological aggregates, with a common space of states $\langle C_S = \alpha C_{11}, C_{12}, \dots, C_{pm} \rangle$ in a dynamic system has the form: $Y = A_S \times \{U_i\}$, $y(t) = \phi: (T \times T \times X \times \Omega)$, $\Omega: \{\omega: T \to U\}$/

Let one construct a diagram for an energy-active object of a dynamic system, taking into account the channels of action of active threats (Fig. 2).

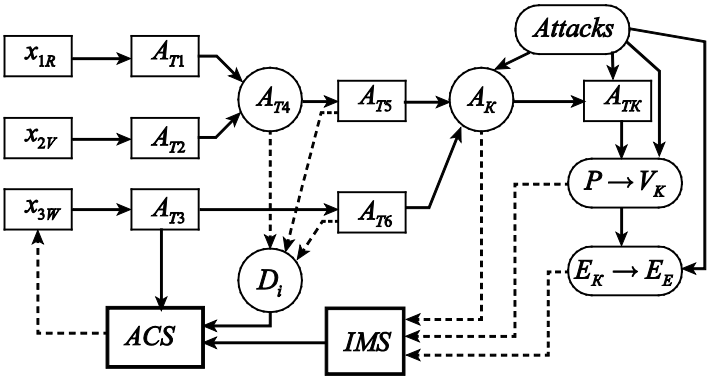

Figure 2: Diagram of transformations in the energy-active system under threats

Fig. 2 shows the following designations: $\{x_i\}$ are input flows and their parameters; $\{A_{Ti}\}$ are operators of technological transformations under the influence of input parameters; $(A_{TK}, P \to V_K)$ are functions of energy transformations; $(E_K \to E_E)$ are kinetic and, accordingly, electromagnetic operators of energy transformations; *IMS* are information and measurement systems.

The channels of resource and information attacks (A_R, A_I) have a complex structure and their representations, methods of influencing the system and the identification require a systematic and categorical approach.

The decomposition procedure will be carried out for a complex dynamic system *IIS* with a hierarchical structure into subsystems, blocks and aggregates:

$$\langle IIS \rangle \to \left\{A_{ij}|_{i=1,j=1}^{n\ m}\right\} \to \left\{B_{kb}|_{k=1,n}^{l=m1}\right\}\left\{D_{rd}|_{r=1,z}^{d=1,c}\right\} \to \{AgStruktIIS\}. \quad (2)$$

Accordingly, a scheme of internal and external connections of aggregate and hierarchical subsystems is obtained when resource and information flows are transformed (Fig. 3).

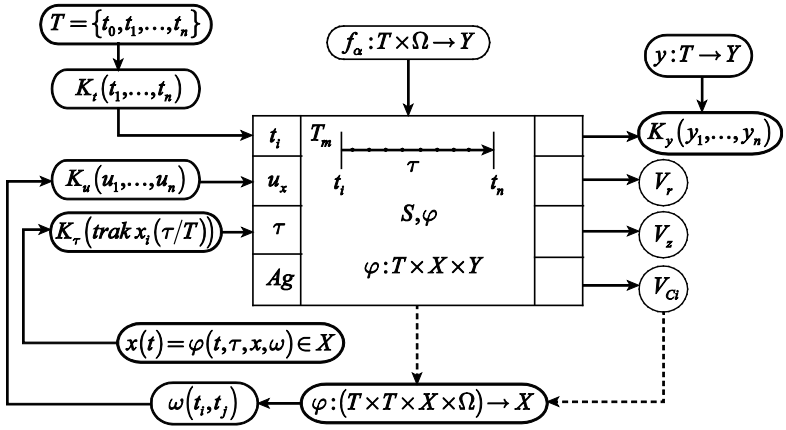

Figure 3: Categorical structure of a time-dynamic complex system

Procedures for forming the structure of the object are constructed using data and knowledge processing processes in accordance with the problem based on the concept of systemology and categories. From the structure of the man-made system, the basic structures

are singled out that describe and show the functions, targets and dynamics of the object according to the specific target task it performs $\{C_i\}$.

To achieve the target task in the system, the basic functional structure of the control object is selected, which at its level ensures the achievement of the target:

$$\{S_{i+3}\} \overset{P_d}{\to} \{S_{i+2}|C_{i+2}|\{A_{ij}|i=1,n\}\}, \tag{4}$$

due to the decomposition procedure of the system into aggregates $\{S_{i+2}\} \overset{P_d}{\to} \{A_{ij}\}$.

To get further information about the functional structure of the technological object and the control process, the aggregates are decomposed into components with selected and predefined spaces of states, targets, modes and parameters in Fig. 4.

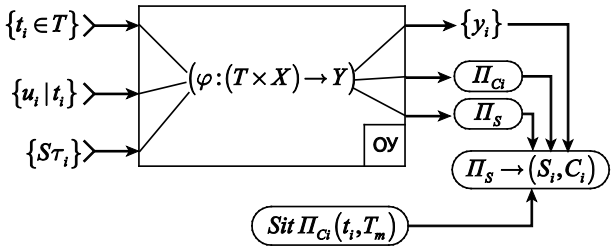

Figure 4: System structure of the dynamics of the hierarchy functioning

Designations in Fig. 3, 4: (S, φ, f_α) are dynamic characteristics of the function; (K_t, K_u, K_τ) are class models of process trajectories at the input and output of the system; (S, τ, X) is the division of the space of states into alternatives; (V_{Ci}, V_r, V_z) are areas in the space of targets, mode, state of the object and system; (Π_{Ci}, Π_Z, Π_Y) are spaces of states, targets, the initial parameter *Y*; $(Sit\Pi_{Ci}, Sit\Pi_{SZ})$ are situations in the space of targets and states according to (Z).

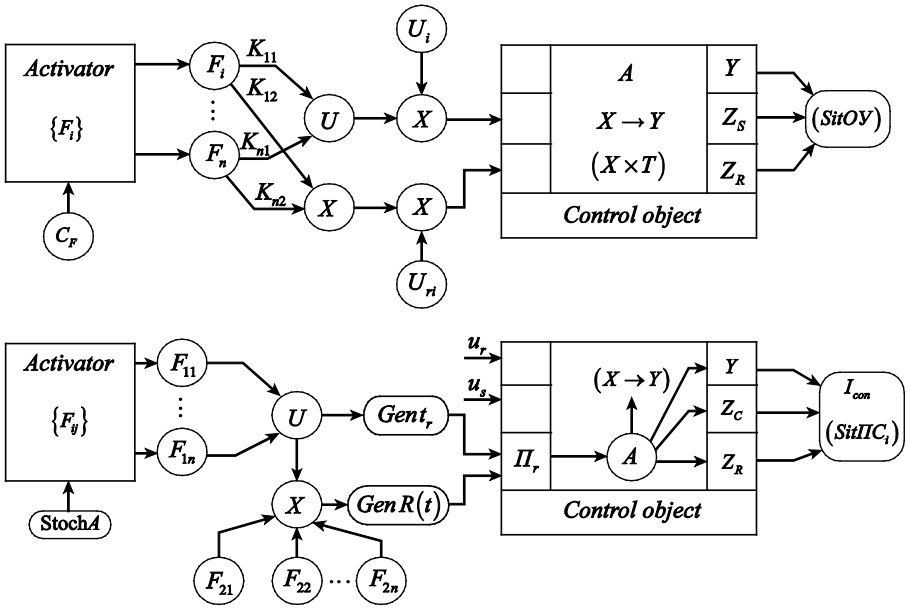

Figure 5: Categorical representation of the model of threat action on the system

On the basis of the given description of the categorical structure of the system in the terminal time base and the system structure of dynamics, a categorical representation of the action model of active threats to the system (informational and resource) is developed (Fig. 5).

Designations in Fig. 5: $Gent_r$ is a generator of the trend of changes in the constant component of the reliability of aggregates; $GenR(t)$ is a generator of impulse discrete active influence on the object of the structure of the document management system, C_F is a targets.

4. Experimental research

To assess the parameters of the system dynamics, under the control action and the influence of threats, a parametric-temporal representation of the behavior of structure objects in the spaces of input parameters, control, the mode of the object according to the load and changing its trajectory is used based on the analysis of the interaction balance <control ↔ threats> (Fig. 6), that is, the system information-resource game.

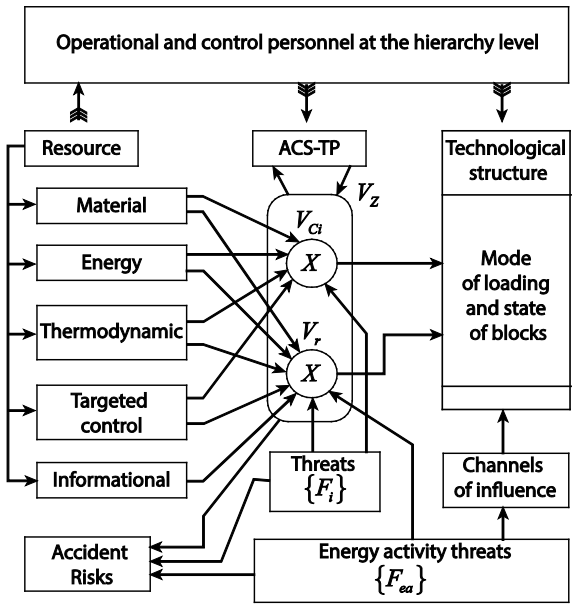

Figure 6: Structural diagram of balance of game between threats and control in the system

Accordingly, such an approach requires additional experimental research into the structure of threat factors, information attacks, and transfer channels of actions from their influence.

The function of the state, mode, and their trajectory in the state space and the target is determined based on the balance between the action of threats and control on the system, which, accordingly, leads it to deviate from the target movement in the state space (Fig. 6).

Designations in Fig. 6: *ACS-TP* is an automated control system of the technological process; $\{V_{Ci}, V_r, V_Z\}$ is an area of interaction between control and threats; $\{F_i\}$ are factors of threats and influence on the system objects.

According to the structural diagram (Fig. 6) of the balance between threats and the control process in the system, in the mode of the information-system game, a functional diagram of the information-resource hierarchy of control of the aggregated system is constructed in the mode of countering threats (Fig. 7).

The following main systems in the structure of the game are highlighted:

- a man-made aggregated system with control hierarchy;
- a system of external influence S_r with a subsystem of active attacks S_{ZA} which forms a complex of interrelated factors of influence on the aggregate sub-structure, as well as information and management, strategic one.

Based on the game concept, a functional scheme of active countermeasures against threats and attacks is developed (Fig. 7).

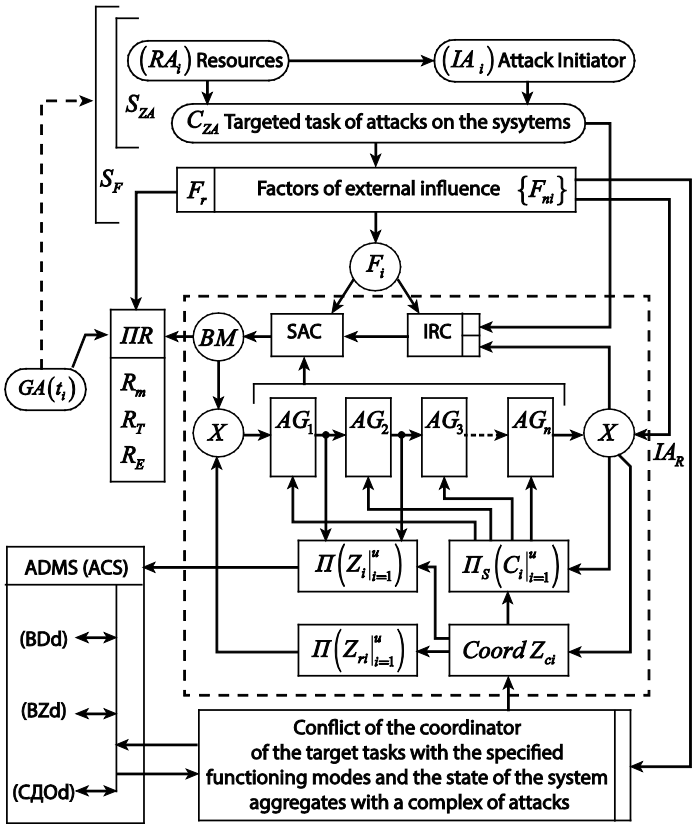

Figure 7: Functional scheme of information-resource countermeasures against threats in the hierarchy of a man-made system

The designations in Fig 7: $\{F_{ni}\}$ are factors of external influence; IA_i is an information attack; *SAC* is a system of automated control of aggregated sub-structure $\{AG_i|_{i=1}^{n}\}IMS$ is an information measuring system; $\Pi R(R_m, R_T, R_E)$ is a flow of technological and energy resources; $\big(\Pi(Z), \Pi(C)\big)$ re spaces of states and the system targets; $Coord(Z_{Ci})$ is a coordination of targets in the mode of threats; (BDd, DZd) are data and knowledge bases of automated document management system, $GA(t_i)$ is an activator of attacks.

According to the functional scheme of the information-resource hierarchy, the substructure (S_{ZA}) of the attack initiation system is considered, which includes: (RA_i) attack resources; IA_i an initiator of attacks; C_{ZA} the target task of the attack; S_F a complex formation

of threat factors, which reflect the activation process and the action of influencing factors on the system control.

In accordance with the strategy of the information-resource game, a categorical diagram of the attack on the *ACS* is constructed (Fig. 8).

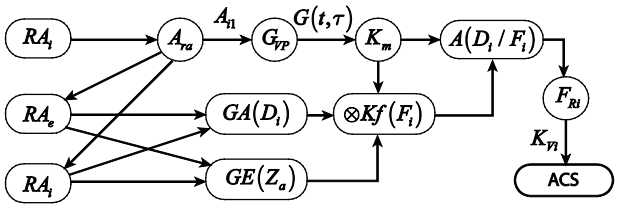

Figure 8: Categorical diagram of an information attack

Designations in Fig 8: A_{ra} is an attack activator; G_{VP} is a generator of a random process $G(t,\tau)$; RA_e is an energy attack resource; RA_i is an information attack resource; K_m is a component modulator; $GA(D_i)$ is a generator of active action; $GE(Z_a)$ is a generator of target task of an active threat, attack; $\otimes Kf(F_i)$ is a component shaper of the factor (of the information-resource class); $A(D_i/F_i)$ is an activator of the factor action on the system; K_{Vi} is a channel of influence on the *ACS* system.

To obtain the control situational information about the object state, it is necessary to decompose the object into the following components, which ensure the achievement of the local target:

$$\{S_{i+1}\} \overset{P_d}{\rightarrow} \left\{ S_{i+1} | C_{i+1} | \overset{P_d}{\rightarrow} \left\{ A_{ij} \rightarrow \{B_{ij}\} \right\} \right\}.$$

At the lower level of the object states $\langle S_{i+3}, S_{i+2}, S_{i+1}, S_i \rangle$the process of identification of elementary structures and knowledge is carried out, which reflect the peculiarities of the complex functioning $\{D_{ij}|_{i=1,n}^{j+1,k}\}$.

To analyze the general state of the system, taking into account the above, it is not possible to present the information essence of the situation that has developed in the system (Fig. 9).

In Fig. 9, the following information-resource components and procedures are denoted:

- the procedure for identifying a critical situation in the object under external influences and attacks on the control structure [4];
- the procedure for forming a target task to resolve a critical situation;
- the procedure for selecting the method of identifying the situation and state for comparison, research and formation of information about the critical state in the data and knowledge base;
- the implementation of a system model of the process of solving critical situation identification problems using an intelligent logical system processor (ILSP) according to [5];
- the procedure for assessing the dynamics of changes in the state of the object using an intelligent research agent to identify risk factors. affiliation mark: a superscript number following the author's last name.

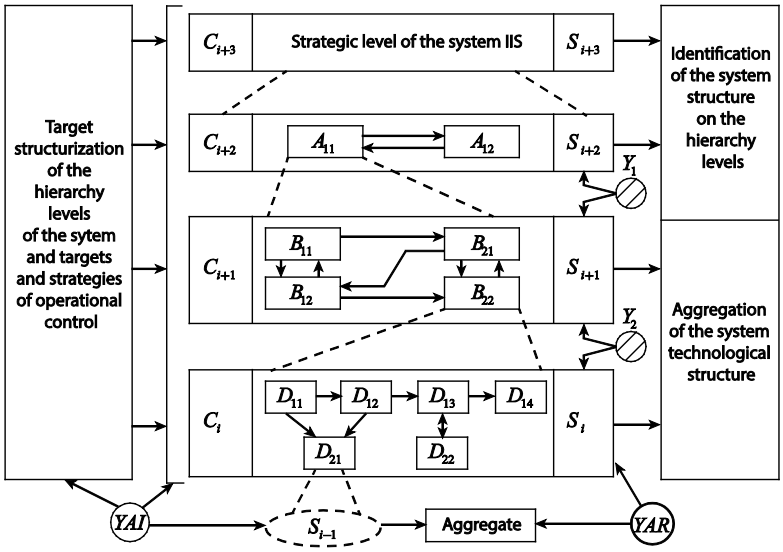

Figure 9: General diagram of a dynamic hierarchical subsystem with internal aggregate connections

4.1. Results

The evaluation of the results of the objects and aggregates state can be carried out using systemology, information technology and intelligent decision-making procedures and rules in the control process, which ensure the achievement of the target in the mode of the current situation assessment. The use of systemology methods is used to create a theoretical representation of the formation of the object structure, to determine the space of its possible states and changes in the object under the influence of threat factors in the target control process. With the help of the concepts developed in works [3-5], let us consider the component structure of a man-made system and the interaction of information, resource and energy flows that determine the general state of a dynamic system.

Common components of a dynamic system with a hierarchical structure include (Fig. 10):

- aggregates, blocks, energy-active objects that ensure the process of resource transformation into energy and are characterized by the operating mode and dynamics;
- dynamic characteristics of technological processes at all stages of functioning (power, mode: limit - standard);
- information control procedures and algorithms for describing situations, data flows in the control process.

Resource, information, control, dynamic processes, channels of flows transfer and exchange cannot be isolated using classical technologies of synthesis and analysis of systems, which in turn complicates the process of identifying crisis nodes and channels through which the redistribution of resources, energy, data flows and control teams occurs. That is, with the help of classical methods and technologies, in the structure of a man-made system it is impossible to single out agents of influence on the way the system functions, the most

vulnerable places of attacks on the control process and system goals, therefore it is impossible to describe the control process using game models. To solve the problem, the concepts of target-oriented systemology of constructing the structure of the object and assessing the dynamic state are developed as a basis for forming a strategy of active game against threats (Fig. 10).

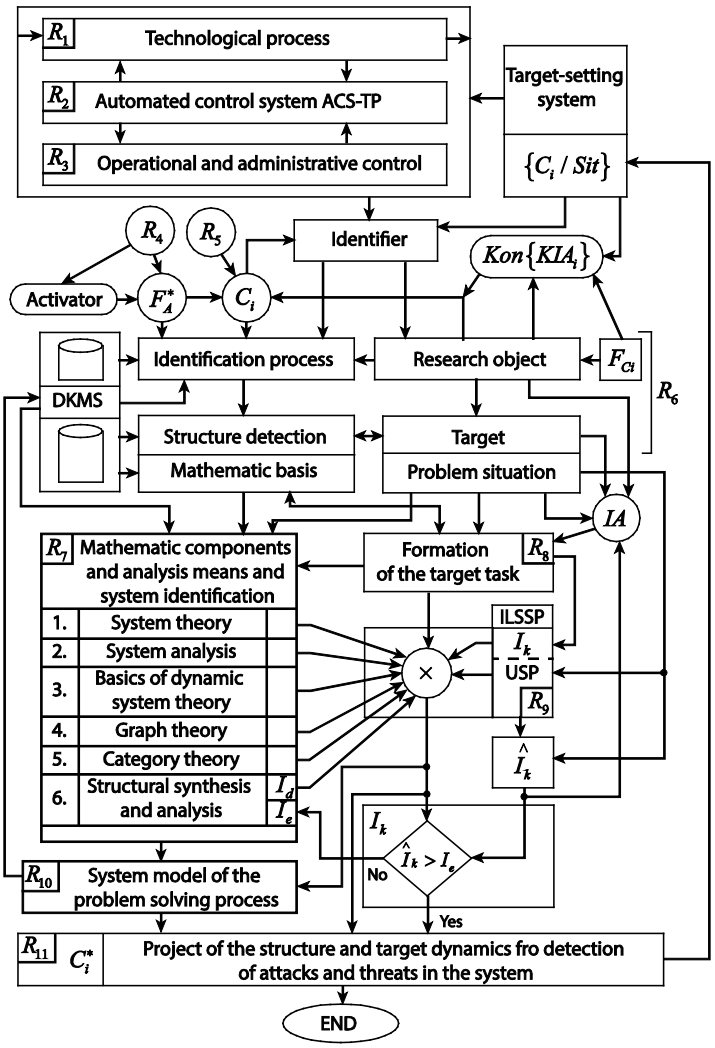

Figure 10: Systemology of object structure formation and the dynamic state assessment under resource threats and information attacks

The designations in Fig. 10: *IA* an intelligent agent; F_{ci} a target activation factor; *DKMS* a database and knowledge management system; *ILSSP* an intelligent logic synthesis system processor; $USP(Sit(CO/t)\tau)$ a unit for processing the system situation in the control object (CO) at the moment of time t in the interval τ; I_k a criterion of quality requirements; $\hat{I}_k$ current quality; I_e reference quality; H_i: $\left(\hat{I}_k \geq I_k\right) \Rightarrow [Strukt(CO) \leftrightarrow R(F_{Ci})]$ compliance of the synthesis product to the target task; I_d a quality criterion in the system dynamics process; F_A^* a factor of influence activation on the system.

Based on the systemology of the formation of the structure of the man-made system, a model of the hierarchy of the control process and the channels of transfer of threats and attacks is developed, which includes the following levels (Fig. 10): R_1 - models of the man-made process (active, thermodynamic, physical); R_2 - the level of automatic control; R_3 - the level of operational control; R_4 - the level of threats to the control; R_5 - the level of threats to the target orientation of the control system; R_6 - the level of information assessment of the dynamic situation in the system; R_7 - a mathematical apparatus for analyzing the structure and the system dynamics under threats in the target control process; R_8 - the level of formation of the target control task in the conditions of threats; R_9 - the level of processing of situational information under threats (*USP* - a unit of signals processing); R_{10} - the level of the model of the process of solving a problematic situational problem; R_{11} - the level of project formation of the defense system against attacks and threats.

Based on the system method of forming the security system structure, a hierarchical structure of the man-made complex control system under threats is constructed (Fig. 11).

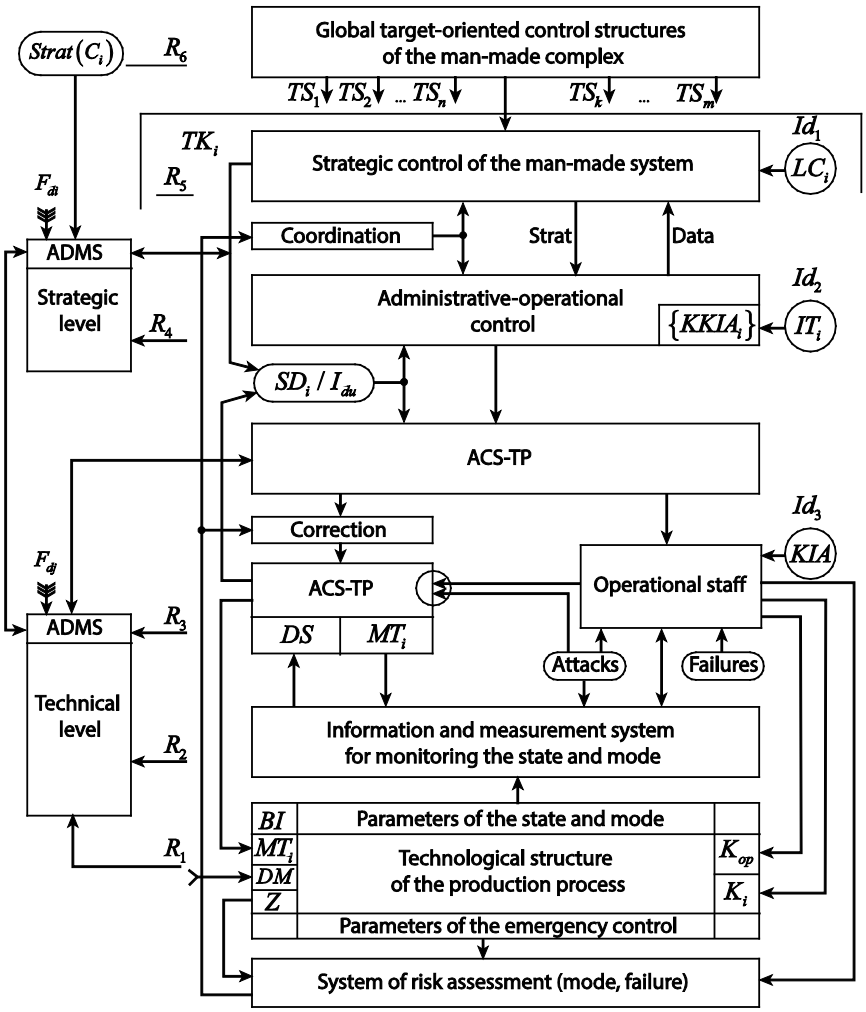

Figure 11: Hierarchical structure of the technological complex control system at risk

In the man-made hierarchy (production, transport, organizational-administrative control units, printing industry, media), the formation of the structure of the security system is based on systemology and methods of target-oriented decision-making to solve the problems of crisis situations.

Let me emphasize the security features of document circulation when formulating control decisions at the techno-aggregate, operational, administrative, and strategic levels (Fig. 11):

R_1 - a technological structure, which is provided by normative and regulatory documents;

R_2 - documents of current control and data storage from information and measurement systems;

R_3 - operational control documents and mode maps and reports for *ACS-TP*;

R_4 - documents and reports in the operational-administrative control system;

R_5 - documents that determine the strategic control of the man-made complex;

R_6 -documents of the strategic level for forecasting the situation and target orientation of the man-made complex;

S_{di}/I_{du} - the core of controlling data exchange processes; *DS* - diagnostic system for *ACS-TP*; *MT* - management team; *DM* - decision-making; IT_i - information threats.

To develop systems for the protection of the strategic structure and the design process, it is necessary to take into account the peculiarities of data accounting between all levels, which are the basis for the formation of documents (correction, management, coordination, target orientation, assessment of situations in the system), which determines the appropriate protection measures.

4.2. Discussion

A methodology for constructing categorical representations of models, structures, components, and systems, which is necessary for detecting the coordinates of intrusion attacks, is proposed, and a generalized representation of structures in a hierarchical system in the category algebra is substantiated. This makes it possible to detect vulnerabilities and threats that lead to information and resource attacks, and as a result - emergency situations in the process of functioning and control of complex hierarchical systems.

When assessing the parameters of the system dynamics, in the process of controlling hierarchical structures and the influence of active threats, a parametric-temporal representation of the behavior of the structure objects in the spaces of input parameters, control, mode of the object according to the load and change of its trajectory is used. Based on the analysis of the interaction balance <control ↔ threats> in the form of a system information-resource game and the study of the functioning of the hierarchical system on a certain terminal cycle, it is found that the game model coincides with the real processes of man-made system control under threats. Based on this, a structural diagram of the balance between threats and control in the system is developed and substantiated, an aggregate diagram of a hierarchical system with internal connections is constructed to identify the cores of attacks on it, which can be used in the context of decision-making support.

A method of structuring man-made systems is developed based on the assessment of the dynamics of changes in the state of objects to identify critical situations in the form of attacks and negative disturbances on the control process and structural organization of man-made

systems. It is shown that the risks of accidents are determined on the basis of the assessment of changes in the state of objects relative to standards, specified limits and normative modes of the system functioning in the conditions of transition of the trajectory of the state through the limit line of the functioning mode of the energy-active object.

The general concept of this approach can be applied to any company and man-made structure with a hierarchical control structure. Quantitative estimates of losses obtained according to the analysis of possible threats and vulnerabilities are submitted to the input of the model, for example, organizational assets, cognitive characteristics of factors affecting the man-made structure, taking into account risk coefficients, characteristics of various control risk components and linguistic considerations of experts in the field of security and system control and decision-making. Risks of production losses are formed in the terminal production cycle and can also be changed under the influence of active threats in the production and control process. It is necessary to take into account all the threats and vulnerabilities of such man-made hierarchical systems, and only then it is possible to determine a comprehensive indicator of the risk of system failure under the influence of active threats.

5. Conclusions

The paper solves the scientific and applied task of developing a methodology for constructing a model of the structure of hierarchical control systems of complex man-made objects under threats and attacks based on the use of the category algebra. The possibility of constructing procedures for the structuring of man-made systems (current and at the design stage) is substantiated based on the use of system analysis and the theory of categories.

The scientific novelty of the study is as follows:

1. for the first time, categorical structural diagrams of transformations in an energy-active system under threats, in the space of states and dynamics in time of a complex system are developed;
2. the categorical representation of the model of the effect of threats on the system is improved and a structural diagram of the game between threats and the control process in the hierarchical system is developed;
3. for the first time, a functional scheme of information-resource countermeasures against threats in the hierarchy of man-made systems is developed;
4. for the first time, the hierarchical structure of a technological complex control system is developed under risk conditions;
5. the proposed categorical representations for assessing the risk of failure of the control system and document flow are tested and verified as part of a hierarchical production system for the example of risk assessment of printing productions, and also a system-category diagram of interaction is proposed as a training in the information-resource game <control ↔ *threats*>.

The practical significance of the obtained results is that the proposed method of determining the coordinates of attacks based on changes in the state of objects in a dynamic hierarchical system allows determining the risk of emergency situations, which has been tested in the control and document management system as part of the hierarchical system of

printing production and can be used in various man-made hierarchical systems when solving control decision-making tasks, designing and improving protection systems.

Further research of the problem can be seen in the development of software for assessing the risk of system functioning under the influence of active threats to man-made hierarchical structures.

References

[1] Y. Ya. Bobalo, I. V. Gorbaty, A. P. Bondarev. Information security. Lviv: Lviv Polytechnic University, 2019.

[2] V. Khoroshko, M. Brailovskyi, M. Kapustian. Multi-criteria assessment of the correctness of decision-making in information security tasks. International scientific journal «Computer systems and information technologies», 4 (2023): 81-86, doi:10.31891/csit-2023-4-11

[3] F. J. Folgado, D. Calderón, I. González, A. J. Calderón. Review of Industry 4.0 from the Perspective of Automation and Supervision Systems: Definitions, Architectures and Recent Trends. Electronics 13,782 (2024): 1-33, doi:10.3390/electronics13040782

[4] V. Sabat, L. Sikora, B. Durnyak, V. Matsiuk, P. Hibey. Methods for assessing the risk of an emergency in the security system for the information complex of printing enterprises. IntelITSIS'2024: 3rd International Workshop on Intelligent Information Technologies and Systems of Information Security. Khmelnytskyi, Ukraine, V. 3675 (2024): 305-317, https://ceur-ws.org/Vol-3675/paper22.pdf

[5] A. Veloni, N. Miridakis. Digital Control Systems Theoretical Problems and Simulation Tools. CRC Press, 2021.

[6] V. Sabat, B. Durnyak, L. Sikora, V. Polishchuk. Research on the assessment of the risk situations emergence for automated control systems of the metallurgical industry companies. Acta Montanistica Slovaca. 28(1) (2023): 201-213, doi:10.46544/AMS.v28i1.16.

[7] ISO/IEC 27001:2022(en). Online Browsing Platform (OBP), https://www.iso.org/obp/ui#iso:std:iso-iec:27001:ed-3:v1:en

[8] Min Jin. Computer Network Information Security and Protection Strategy Based on Big Data Environment. International Journal of Information Technologies and Systems Approach, 16(2) (2023): 1-14, doi:10.4018/IJITSA.319722

[9] Jiaqi Sun. Computer Network Security Technology and Prevention Strategy Analysis. Procedia Computer Science, 208 (2022): 570-576, doi:10.1016/j.procs.2022.10.079

[10] Yuqian L., Xun X., Lihui W. Smart manufacturing process and system automation - A critical review of the standards and envisioned scenarios. Journal of Manufacturing Systems, 56 (2020): 312-325, doi:10.1016/j.jmsy.2020.06.010

[11] V. Sabat, B. Durnyak, M. Kulynych, O. Havrylyshyn, P. Hibey. Using semantic analysis of document text in building risk models in the threats system. IntelITSIS'2024: 3rd International Workshop on Intelligent Information Technologies and Systems of Information Security. Khmelnytskyi, Ukraine, V. 3675 (2024): 330-342, https://ceur-ws.org/Vol-3675/paper24.pdf

[12] Ch. Milioti, K. Kepaptsoglou, A. Deloukas, E. Apostolopoulou, Valuation of man-made incident risk perception in public transport: The case of the Athens metro, International Journal of Transportation Science and Technology, 11(3) (2022): 578-588, doi:10.1016/j.ijtst.2021.07.003

[13] F. Sicard, É. Zamai, J. M. Flaus. An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems. Reliab Eng Syst Saf, 188 (2019): 584-603, doi:10.1016/J.RESS.2019.03.020

[14] A. Cormier, C. Ng. Integrating cybersecurity in hazard and risk analyses. J Loss Prev Process Ind, 64 (2020), Article 104044, doi:10.1016/j.jlp.2020.104044

[15] D. H. Alahmadi, A. A. Jamjoom. Decision support system for handling control decisions and decision-maker related to supply chain. Journal of Big Data, 9:114 (2022): 1-14, doi:10.1186/s40537-022-00653-9

[16] V. Domeh, F. Obeng, F. Khan, N. Bose, E. Sanli, Risk analysis of man overboard scenario in a small fishing vessel. Ocean Engineering, 229 (2021) 108979, doi:10.1016/j.oceaneng.2021.108979

[17] J. Alanen, J. Linnosmaa, T. Malm, N. Papakonstantinou, T. Ahonen, E. Heikkilä, R. Tiusanen, Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering & System Safety, 220 (2022) 108270, doi:10.1016/j.ress.2021.108270

[18] V. Agrawal, A comparative study on information security risk analysis methods. In: International Conference on Computer Science and Information Technology (ICCSIT 2015) At: Amsterdam 12 (2017): 57-67, doi:10.17706/jcp.12.1.57-67

[19] F. De Rosa, N. Maunero, L. Nicoletti, P. Prinetto, M. Trussoni, Ontology for Cybersecurity Governance of ICT System s. ITASEC'22: Italian Conference on Cybersecurity, June 20-23, 2022, https://ceur-ws.org/Vol-3260/paper4.pdf

[20] T. Zhou, M. Modarres, E. L. Droguett, Multi-unit nuclear power plant probabilistic risk assessment: a comprehensive survey. Reliab Eng Syst Saf, 213 (2021), Article 107782, doi:10.1016/j.ress.2021.107782.

[21] M. Modarres, T. Zhou, M. Massoud, Advances in multi-unit nuclear power plant probabilistic risk assessment. Reliab Eng Syst Saf, 157 (2017): 87-100, doi:10.1016/j.ress.2016.08.005

[22] J. Kim, A.U.A. Shah, H.G. Kang, Dynamic risk assessment with bayesian network and clustering analysis. Reliab Eng Syst Saf, 201 (2020), 106959, doi:10.1016/j.ress.2020.106959

[23] J. DeJesus Segarra, M. Bensi, M. Modarres. A bayesian network approach for modeling dependent seismic failures in a nuclear power plant probabilistic risk assessment. Reliab Eng Syst Saf, 213 (2021), Article 107678, doi:10.1016/j.ress.2021.107678

[24] M. Cepin, R. Bris, Safety and Reliability. Theory and Applications. CRC Press. 2017, doi:10.1201/9781315210469

[25] M. A. Dorna, L. C. Ribeiro, H. S. Schuffner, M. P. Liborio & P. I. Ekel. Fuzzy-Set-Based Multi-Attribute Decision-Making, Its Computational Implementation, and Applications. Axioms 13(3) (2024): 142, doi:10.3390/axioms13030142