ISSN 2782-2427

CONTROL SCIENCES

3/2022

[1] Russian Academy of Sciences.

CONTROL SCIENCES
Scientific Technical
Journal

6 issues per year
ISSN 2782-2427
Open access

Published since 2021

Original Russian Edition
Problemy Upravleniya
Published since 2003

FOUNDER AND PUBLISHER
V.A. Trapeznikov
Institute of Control Sciences
of Russian Academy of Sciences

Editor-in-Chief
D.A. Novikov, RAS Academician

Deputy Editor-in-Chief
F.F. Pashchenko

Executive Editor-in-Chief
N.E. Maximova

Editor
L.V. Petrakova

Editorial address
65 Profsoyuznaya st., office 410,
Moscow 117997, Russia

☎/🖷 +7(495) 198-17-20, ext. 1410

✉ pu@ipu.ru

URL: http://controlsciences.org

Published: August 5, 2022

Registration certificate of
Эл № ФС 77-80482
of 17 February 2021
issued by the Federal Service
for Supervision of Communications,
Information Technology, and Mass
Media

CONTROL SCIENCES

3.2022

CONTENTS

Analysis and Design of Control Systems

Control in Social and Economic Systems

Information Technology in Control

DOI: http://doi.org/10.25728/cs.2022.3.1

TRACKING SYSTEM DESIGN FOR A SINGLE-LINK SENSORLESS MANIPULATOR UNDER NONSMOOTH DISTURBANCES[1]

A.S. Antipov[1] and D.V. Krasnov[2]

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

[1]✉ scholess18@mail.ru, [2]✉ dim93kr@mail.ru

Abstract. The controlled plant is a single-link manipulator elastically jointed to a DC motor and operating under uncertainty and incomplete measurements. The problem is to design a discontinuous feedback control for tracking a given reference signal of the plant's angular position. The angular position and velocity of the manipulator are not available for measurements; the sensors are located only on the drive; parametric and exogenous disturbances affecting the manipulator are nonsmooth and cannot be directly suppressed by control applied to the actuator. Within the block approach, a decomposition procedure is developed to design a nonlinear local feedback control. This control ensures the controlled variable's invariance with respect to uncertainties unmatched with the control action. A state observer of reduced order is constructed to estimate the angular position and velocity of the manipulator required for feedback design. The state variables in this observer are estimated using the principle of restoring exogenous disturbances by their action on the controlled plant. With this principle, a dynamic model of exogenous disturbances is not needed. In both problems (control and observation), *S*-shaped bounded continuous local feedback laws are used (smooth (sigmoid) and nonsmooth (piecewise linear) local feedback, respectively). These local feedback laws suppress bounded disturbances acting with them through the same channel. The algorithms developed below do not require real-time identification of parametric and exogenous disturbances. However, they stabilize the observation and tracking errors with some accuracy. The effectiveness of the dynamic feedback is validated by the results of numerical simulation.

Keywords: electromechanical system, tracking, invariance, block approach, state observer of reduced order, *S*-shaped functions.

INTRODUCTION

This paper considers a simple electromechanical system: a single-link sensorless manipulator elastically jointed to a DC motor and operating under parametric and exogenous disturbances. The basic problem is to control the angular position of the manipulator: stabilize it at a given level or track an admissible reference signal. Despite the seeming simplicity, this plant has all attributes of a complex automatic control system. Namely, it is described by a fifth-order dynamic model with nonlinearity and uncertain parameters, has an incomplete set of sensors, and is affected by exogenous disturbances. At present, many efficient control algorithms have been developed for mechanical and electromechanical systems within various approaches; for example, see [1–5]. However, when solving such problems, a specific type of uncertainties (parametric uncertainties, or exogenous disturbances of a certain class, or incomplete measurements) is often considered. In many studies, the mathematical model consists of the mechanical system only (the dynamics of actuators are neglected), and the suppression of unmatched disturbances acting through different channels with control remains an open problem [6].

In the previous publication [7], we considered a single-link sensorless manipulator elastically jointed to a DC motor under the assumption that its reference

[1] This work was supported in part by the Russian Foundation for Basic Research, project no. 20-01-00363A.

signal, parametric and exogenous disturbances are smooth functions of time. As a result, the controlled plant model was written in the canonical input-output form in mixed variables (linear combinations of the state variables, exogenous actions, and their derivatives), and the observation and tracking problems were successfully solved based on the form. The unmeasured controlled variable necessary for feedback design in the mixed variables observer was estimated using an additional loop in the observation subsystem. However, different nonsmooth disturbances (shock loads and dry friction forces) [8] often act on a mechanical plant during operation. These disturbances cannot be differentiated and cannot be directly suppressed or compensated by applying control to the actuator. Below, we consider such nonsmooth and unmatched exogenous and parametric disturbances and piecewise discontinuous reference signals, which are an obstacle to applying typical control methods, particularly the feedback linearization method [9, 10]. The controlled plant and the problem statement are described in Section 1.

The block approach seems reasonable to design the tracking system under such conditions. According to this approach, the state variables are used as fictitious controls from a certain class of smooth functions [11, 12]. In this case, the disturbances are matched with the fictitious controls and can be suppressed with a given accuracy. The original system is reduced to another one with respect to the tracking error and the residuals between the real and generated fictitious controls (invariant local feedback laws), and the exogenous signals are not differentiated. The true discontinuous control applied to the actuator ensures the sequential convergence of the residuals to given neighborhoods of zero, thereby stabilizing the tracking error (achieving the goal of control). Stabilizing fictitious controls are constructed as smooth and bounded sigmoid functions to avoid, at the beginning of transients, the bursts (an overshoot of the state variables) inherent in systems with linear high-gain feedback laws [11, 13]. (They are traditionally used to suppress exogenous disturbances.) The paper [12] presented a local sigmoid feedback design procedure for a nonlinear single-channel plant under the assumption that the functions of the state variables on the right-hand sides of the differential system dynamics equations are bounded everywhere. The scientific novelty of this study consists in developing a block parametric design procedure for sigmoid fictitious controls for an almost linear fifth-order system with nonsmooth exogenous disturbances (whose derivatives have a discontinuity). The plant has the following peculiarity: from the theoretical point of view, the linear combinations of state variables in the system equations are not bounded. To achieve the goal of control, the values of internal variables in the control process must belong to given ranges. The design procedure of the basic control law considering these features of the plant is given in Section 2.

Section 3 solves the observation problem in the case where the angular position and velocity of the manipulator required for feedback design cannot be measured (e.g., due to an aggressive environment, vibration, etc. [14]) and the sensors are mounted on the actuator only. A reduced-order state observer is constructed. It estimates the state variables by restoring exogenous disturbances by their effect on the controlled plant without any dynamic model of the signals [15, 16]. According to this restoration principle, the variable is treated as an exogenous disturbance and estimated using a feedback law in the observer (a corrective action). Following this approach, we design a robust state observer without the system equations with uncertain parameters. Also, we develop a decomposition procedure for designing piecewise linear feedback laws to solve the observation problem with a given accuracy under the parametric and exogenous disturbances affecting the mechanical subsystem. Due to the *S*-shaped invariant feedback laws (smooth in tracking, and piecewise-smooth in observation), there is no need to identify the uncertain parameters and exogenous disturbances in the observation and control processes: it suffices to know their ranges. The controller's parameters require no retuning when uncertainties change arbitrarily within the admissible ranges. This conclusion is illustrated by the numerical simulation results in Section 4.

1. DESCRIPTION OF THE CONTROLLED PLANT. PROBLEM STATEMENT

Consider a single-link rigid manipulator with a rotating joint elastically connected to the shaft of a DC motor. Its mathematical model is described by the differential equations [7, 17]

$$\dot{x}_1 = x_2,\ \dot{x}_2 = -a_{21}x_1 - a_2\sin(x_1) + b_2x_3 + f(t), \qquad (1)$$

$$\begin{gathered} \dot{x}_3 = x_4,\ \dot{x}_4 = -a_{41}x_1 - a_{43}x_3 - a_{44}x_4 + b_4x_5, \\ \dot{x}_5 = -a_{54}x_4 - a_{55}x_5 + b_5u. \end{gathered} \qquad (2)$$

Equations (1) correspond to the manipulator dynamics whereas equations (2) to the dynamics of the DC motor with permanent magnets [6]. In addition, $a_{41} = -\ a_{43} < 0$, and the other design factors are positive:

$$b_2 = a_{21} = k_l / J_l,\ a_2 = \bar{m}\bar{g}h / J_l,\ \ a_{43} = k_l / J_m,$$
$$a_{44} = d / J_m,\ b_4 = k_m / J_m,$$
$$a_{54} = c / L,\ a_{55} = R / L,\ b_5 = 1 / L.$$

The variables $x = (x_1, ..., x_5)^{\mathrm{T}}$ and parameters of system (1), (2) are described in Table 1.

Table 1

The variables and parameters of the controlled plant

Notation	Description, measurement unit	Notation	Description, measurement unit
x_1	The angular position of manipulator's link, rad	$\bar{g}$	Acceleration of gravity, 9.8 m/s^2
x_2	The angular velocity of manipulator's link, rad/s	k_l	Gear rigidity, N·m/rad
x_3	The angular position of DC motor's shaft, rad	J_l	The manipulator's moment of inertia, kg·m^2
x_4	The angular velocity of DC motor's shaft, rad/s	k_m	Gain, N·m/A
x_5	The drive armature current of DC motor, A	J_m	The moment of inertia of DC motor, kg·m^2
$f(t)$	Uncontrolled disturbance, N/(kg·m)	D	Damping coefficient, kg·m^2/s
u	The drive armature voltage of DC motor, V	c	The counter emf coefficient of DC motor, V·s/rad
h	Manipulator's link length, m	L	The drive armature inductance of DC motor, H
$\bar{m}$	Manipulator's link mass, kg	R	The drive armature resistance of DC motor, Ω

In system (1), (2), the output controlled variable is the angular position $x_1(t)$ of the manipulator's link; the drive armature voltage u of the DC motor is a discontinuous control. The problem is to design a dynamic feedback control under which the output variable $x_1(t)$ will track a given admissible signal $g(t)$ under the following assumptions:

- The reference point $x_1(t) = 0$ is the low vertical position of the manipulator's link, which is stable; the maximum angular velocity of the manipulator's link is bounded:

$$|x_1(t)| \le \pi,\ \ |x_2(t)| \le X_2,\ t \ge 0,\ X_2 = \text{const} > 0. \quad (3)$$

- The initial values of the state variables belong to given ranges:

$$\left|x_i(0)\right| \le X_{i,0} = \text{const} > 0, i = \overline{1,5}. \quad (4)$$

- The sensors are located only on the actuator. The variables $x_1(t)$ and $x_2(t)$ are unmeasured, whereas the variables $x_3(t)$, $x_4(t)$, and $x_5(t)$ are measured without noise.
- The current values of the reference signal $g(t)$ are known; its derivative $\dot{g}(t)$ is assumed to be a nonsmooth unknown function of time, bounded by a given constant:

$$\begin{gathered} |g(t)| \le G_0 < \pi;\ |\dot{g}(t)| \le G_1, \\ t \ge 0;\ G_0, G_1 = \text{const} > 0. \end{gathered} \quad (5)$$

- The values of the parameters k_l , J_m, d, and k_m (hence, a_{43}, a_{44}, and b_4) are known. The parameters $\bar{m}$, h, J_l, c, R, and L (hence, $b_2 = a_{21}$, a_2, a_{54}, a_{55}, and b_5) are uncertain but belong to given ranges:

$$a_{21,\min} \le a_{21}(t) \le a_{21,\max}, a_{2,\min} \le a_2(t) \le a_{2,\max};$$

$$a_{5j,\min} \le a_{5j}(t) \le a_{5j,\max},\ j = 4,5;$$

$$b_{5,\min} \le b_5(t) \le b_{5,\max}, t \ge 0; \quad (6)$$

- The time-varying function $f(t)$ is unknown, nonsmooth, and bounded by a given constant:

$$\left|f(t)\right| \le F = \text{const} > 0,\ t \ge 0. \quad (7)$$

The feedback loop involves only an observer of the unmeasured state variables: identifiers of the unknown parameters and generators of the exogenous actions are not introduced. Under these conditions, the tracking error $e_1(t) = x_1(t) - g(t) \in R$ can be stabilized only with some accuracy. The goal of control is to ensure the condition

$$\left|e_1(t)\right| \le \Delta_1,\ t \ge t_1, \quad (8)$$

in the closed loop system, where $\Delta_1 > 0$ and $t_1 > 0$ are a given stabilization accuracy and a given time to reach it, respectively.

2. THE BASIC CONTROL LAW

First, we form a control law in system (1), (2) using a given reference signal $g(t)$ and all state variables. Then, we construct an observer to estimate the unmeasured state variables. To design the feedback, we apply the block control principle [11, 12].

System (1), (2) is a block controllability form [11]. This means that the true control appears additively with a nonzero factor only in the last equation; the right-hand side of each ith equation (block), $i = \overline{1,4}$, contains functions only of the state variables x_1,..., x_i, and the variable of the next $(i+1)$th equation appears additively with a nonzero factor. Due to such a form, the variable x_{i+1} in each ith equation can be treated as a fictitious control, and the local feedback laws can be sequentially obtained in each equation (top-to-bottom). In the last block, the local feedback laws are provided by the true control. Since the first equation is written in the controlled variable, system (1), (2) can be considered a triangular input-output form (by the composition of the arguments of functions in each equation except fictitious controls). Therefore, we solve the tracking problem based on this form.

To suppress parametric and exogenous disturbances on the same channels with fictitious controls, we construct local feedback laws as bounded *S*-shaped sigmoid functions with two tuned parameters [12]:

$$x_i^* = -m_{i-1}\sigma(k_{i-1}e_{i-1}),\ k_{i-1}, m_{i-1} = \text{const} > 0,\ i = \overline{2,5}, \quad (9)$$

where $\sigma(k_{i-1}e_{i-1}) = 2/(1+\exp(-k_{i-1}e_{i-1})) - 1$ is an odd and bounded sigmoid function, $|\sigma(k_{i-1}e_{i-1})| < 1,$ and $e_i \in R$ ($i = \overline{2,5}$) are the residuals between the variables x_i and the desired fictitious controls x_i^* (9):

$$e_i = x_i - x_i^* = x_i + m_{i-1}\sigma(k_{i-1}e_{i-1}),\ i = \overline{2,5}. \quad (10)$$

The true control (the drive armature voltage of the DC motor) is naturally taken [6] as the discontinuous function

$$u = -m_5\text{sign}(e_5),\ m_5 = \text{const} > 0,$$
$$\text{sign}(e_5) = \begin{cases} +1,\ e_5 > 0, \\ -1,\ e_5 < 0. \end{cases} \quad (11)$$

For $e_5 = 0$, the value of the sign function is undefined but restricted to the interval $[-1, 1]$. The closed loop system (1), (2), (11), written in the tracking error and the residuals (10), has the form

$$\dot{e}_1 = e_2 - m_1\sigma(k_1e_1) - \dot{g},$$
$$\dot{e}_i = b_i(e_{i+1} - m_i\sigma(k_ie_i)) -$$
$$\sum_{j=1}^{i} a_{ij}e_j + f_i + \Lambda_{i-1}, i = 2,3,4, \quad (12)$$
$$\dot{e}_5 = -a_{54}e_4 - a_{55}e_5 + f_5 + \Lambda_4 - b_5m_5\text{sign}(e_5),$$

where $b_3 = 1$, the elements a_{ij} figuring in formula (12) but absent in system (1), (2), are zero, and Λ_{i-1} are the full derivatives of the fictitious controls (9):

$$\Lambda_{i-1} = \tfrac{d}{dt}m_{i-1}\sigma(k_{i-1}e_{i-1}) =$$
$$0{,}5m_{i-1}k_{i-1}(1-\sigma^2(k_{i-1}e_{i-1}))\dot{e}_{i-1},\ i = \overline{2,\ 5}; \quad (13)$$
$$f_2 = -a_{21}g - a_2\sin(e_1 + g) + f(t),\ f_3 = 0,$$
$$f_4 = a_{43}(m_2\sigma(k_2e_2) + g) + a_{44}m_3\sigma(k_3e_3),$$
$$f_5 = a_{54}m_3\sigma(k_3e_3) + a_{55}m_4\sigma(k_4e_4).$$

Due to formulas (5)–(7), the values of f_i are bounded, and their estimates depend on the amplitudes of fictitious controls:

$$|f_2(t)| \le a_{21,\max}G_0 + a_{2,\max} + F = F_2,$$
$$|f_4(t)| \le a_{43}(m_2 + G_0) + a_{44}m_3 = F_4, \quad (14)$$
$$|f_5(t)| \le a_{54,\max}m_3 + a_{55,\max}m_4 = F_5.$$

The original problem (8) is reduced to the stabilization of the closed loop system (12). In this case, the control design for a single-channel system of the fifth order is decomposed into five elementary design subproblems solved sequentially: choosing the parameters of true and fictitious controls that ensure invariance with respect to the existing uncertainties with a given accuracy. The amplitude of the discontinuous control (11) is chosen to ensure the occurrence of a sliding mode on the surface $e_5 = 0$ in system (12) in a finite time $0 < t_5 < t_1$. According to the block control principle, the parameters of fictitious controls (9) are chosen to ensure the sequential convergence of the residuals to some neighborhoods of zero:

$$|e_5(t)| \le \Delta_5, t \ge t_5 > 0 \Rightarrow |e_4(t)| \le \Delta_4,$$
$$t \ge t_4 > t_5 \Rightarrow ... \Rightarrow |e_1(t)| \le \Delta_1,\ t \ge t_1 > t_2, \quad (15)$$

where Δ_1 and t_1 are given by (8), and Δ_i = const > 0, $i = \overline{2,5}$, are assigned arbitrarily. The first inequality in (15) reflects the following fact: due to various imperfections, the sliding mode in real systems occurs in some boundary layer of the switching surface [6].

The sigmoid function can be estimated from below by the piecewise linear function

$$0.8|\text{sat}(k_ie_i)| \le |\sigma(k_ie_i)| < 1,$$
$$\text{sat}(k_ie_i) = \begin{cases} \text{sign}(e_i),\ |e_i| > 2.2/k_i, \\ k_ie_i/2.2,\ |e_i| \le 2.2/k_i,\ i = \overline{1,\ 4}, \end{cases} \quad (16)$$

where $\sigma(\pm 2.2) \approx \pm 0.8$ and $e_i = \pm 2.2/k_i$ are the points separating $\sigma(k_ie_i)$ into almost linear and almost constant functions [12]. The choice of the value k_i (the gain in the argument of the sigmoid function) determines the stabilization accuracy of the corresponding residual. We fix an inversely proportional relation between the gains and the stabilization accuracy of the residuals: $|e_i| \le 2.2/k_i = \Delta_i, i = \overline{1,4}.$ Under the gains

$$k_i \ge 2.2/\Delta_i, i = \overline{1,4}, \quad (17)$$

yielding the desired stabilization accuracy, the design problem is reduced to choosing the amplitudes m_i, $i = \overline{1,\ 5}$, that ensure the sequential convergence of the residuals to the corresponding neighborhoods of zero (15). Sufficient conditions for $|e_i| \le \Delta_i$ have the form $e_i\dot{e}_i < 0$ for $|e_i| > \Delta_i, i = \overline{1,5}$ [6, 12]. From these inequalities we obtain a lower estimate for the amplitude in the *i*th block ($i = \overline{1,4}$) provided that in all subsequent blocks *j* = *i* + 1, *i* + 2, ..., 5, the residuals have already converged to the given neighborhoods of zero $|e_j| \le \Delta_j$ (15). Given formulas (5), (14)–(17), we have:

$$
\begin{gathered}
0.8m_1 > G_1 + \Delta_2 \Rightarrow e_1\dot{e}_1 = e_1(e_2 - m_1\sigma(k_1e_1) - \dot{g}) \le \\
|e_1|(\Delta_2 + G_1 - 0.8m_1) < 0, \\
0.8b_{i,\min}m_i > b_{i,\min}\Delta_{i+1} + \sum_{j=1}^{i-1} a_{ij,\max}|e_j| + \\
F_i + |\Lambda_{i-1}| \Rightarrow e_i\dot{e}_i = e_i(b_i(e_{i+1} - m_i\sigma(k_ie_i)) - \\
\sum_{j=1}^{i} a_{ij}e_j + f_i + \Lambda_{i-1}) \le \\
|e_i|(b_{i,\min}(\Delta_{i+1} - 0.8m_i) - a_{ij,\min}|e_i| + \\
\sum_{j=1}^{i-1} a_{ij,\max}|e_j| + F_i + |\Lambda_{i-1}|) < 0,\ i = 2,\ 3,\ 4; \\
b_{5,\min}m_5 > a_{54,\max}|e_4| + F_5 + |\Lambda_4| \Rightarrow e_5\dot{e}_5 = \\
e_5(-a_{54}e_4 - a_{55}e_5 + f_5 + \Lambda_4 - b_5m_5\mathrm{sign}(e_5)) \le \\
|e_5|(a_{54,\max}|e_4| - a_{55,\min}|e_5|F_5 + |\Lambda_4| - b_{5,\min}m_5) < 0.
\end{gathered}
\tag{18}
$$

To implement the sufficient conditions (18), we estimate the ranges of the variables of system (12) and their derivatives in the control process with a given time to stabilize the tracking error (8). The corresponding procedure and the resulting inequalities for choosing the amplitudes m_i ($i = \overline{1,5}$) are presented in the Appendix. The procedure rests on conservative estimates and proves the existence of solutions of inequalities (18). The values of the gains (17) and amplitudes can be decreased based on simulation results.

For the system with an incomplete set of sensors, the control law (11) involves the measured variables $g(t)$, $x_3(t)$, $x_4(t)$, and $x_5(t)$ together with the estimates $\hat{x}_1(t)$ and $\hat{x}_2(t)$ of the unmeasured state variables $x_1(t)$ and $x_2(t)$. Section 3 considers the design problem of a state observer that ensures a given accuracy and a given estimation time under the parametric uncertainty of the controlled plant:

$$
|x_i(t) - \hat{x}_i(t)| \le \delta_i,\ i = 1, 2,\ t \ge T,\ 0 < T < t_5. \tag{19}
$$

In the dynamic feedback system, the control law (11) takes the form

$$
u = -m_5\mathrm{sign}(\hat{e}_5), \tag{20}
$$

where the tracking error and the residuals (10) are constructed by the measured and estimated signals:

$$
\begin{gathered}
\hat{e}_1 = \hat{x}_1 - g,\ \hat{e}_2 = \hat{x}_2 + m_1\sigma(k_1\hat{e}_1),\ \hat{e}_3 = x_3 + m_2\sigma(k_2\hat{e}_2), \\
\hat{e}_4 = x_4 + m_3\sigma(k_3\hat{e}_3),\ \hat{e}_5 = x_5 + m_4\sigma(k_4\hat{e}_4).
\end{gathered}
$$

In the closed loop system (1), (2) with the dynamic feedback (20), the estimation errors (19) act as imperfections. As a result, the boundary layer

$$
|\hat{e}_5 - e_5| = m_4|\sigma(k_4\hat{e}_4) - \sigma(k_4e_4)| \le \Delta_5. \tag{21}
$$

appears in the sliding mode. Due to (21) and the *S*-shaped form of the sigmoid function, the greatest deviation is achieved in the vicinity of zero, and the estimation errors have an almost negligible effect at infinity. Using the first approximation $\sigma(kx) \underset{x\to 0}{\sim} 0.5kx$, we estimate the deviation (21) as follows:

$$
\begin{gathered}
|\sigma(k_4\hat{e}_4) - \sigma(k_4e_4)| \approx 0.5k_4|\hat{e}_4 - e_4| \approx \\
0.5k_4m_3|\sigma(k_3\hat{e}_3) - \sigma(k_3e_3)| \approx 0.5^2k_4m_3k_3|\hat{e}_3 - e_3| \approx \\
0.5^2k_4m_3k_3m_2|\sigma(k_2\hat{e}_2) - \sigma(k_2e_2)| \approx \\
0.5^3k_4m_3k_3m_2k_2|\hat{e}_2 - e_2| \approx \\
0.5^3k_4m_3k_3m_2k_2|\delta_2 + m_1\,|\sigma(k_1\hat{e}_1) - \sigma(k_1e_1)|\,| \approx \\
0.5^3k_4m_3k_3m_2k_2(\delta_2 + 0.5m_1k_1\delta_1).
\end{gathered}
$$

With the accepted values of the controller parameters and the boundary layer Δ_5, we finally arrive at the following constraint on the estimation errors in the observation problem:

$$
\delta_2 + 0.5m_1k_1\delta_1 \le \frac{8\Delta_5}{m_4k_4m_3k_3m_2k_2}. \tag{22}
$$

3. A STATE OBSERVER TO ESTIMATE THE VARIABLES OF THE MECHANICAL SUBSYSTEM

System (1), (2) is observable with respect to the measurements $x_3(t)$, $x_4(t)$, and $x_5(t)$, but the full-order state observer cannot be designed due to the parametric uncertainties in the model and the exogenous disturbances affecting the plant. To restore the values of the unmeasured variables $x_1(t)$ and $x_2(t)$, we will use the procedure for estimating exogenous disturbances without a dynamic disturbance generator [7, 15, 16] and construct a reduced-order observer. In this case, the desired estimates $\hat{x}_1$ and $\hat{x}_2$ can be obtained only with the given accuracy (19), (22).

According to this procedure, we construct a reduced-order observer based on the fourth and first equations of the original system (1), (2), which do not depend on the uncertain parameters and include the unmeasured variables with nonzero factors:

$$
\dot{x}_4 = -a_{43}(x_3 - x_1) - a_{44}x_4 + a_{45}x_5,\ \dot{x}_1 = x_2. \tag{23}
$$

The reduced-order observer is constructed for system (23) with the measured signals

$$
\dot{z}_1 = -a_{43}(x_3 - z_2) - a_{44}x_4 + a_{45}x_5 + v_1,\ \dot{z}_2 = v_2, \tag{24}
$$

where z_1 and z_2 are the observer's state variables, and v_1 and v_2 are its corrective actions.

We introduce the observation errors $\varepsilon_1 = x_4 - z_1$ and $\varepsilon_2 = x_1 - z_2$. Considering formulas (23) and (24), we obtain the system

$$
\dot{\varepsilon}_1 = a_{43}\varepsilon_2 - v_1,\ \dot{\varepsilon}_2 = x_2 - v_2. \tag{25}
$$

Due to the available measurements of the parameter x_4, the current errors $\varepsilon_1(t)$ are known, whereas the errors $\varepsilon_2(t)$ are not. Let us assign the following initial conditions for the observer (24) and, accordingly, for the virtual system (25):

$$\begin{gathered} z_1(0)=x_4(0)\Rightarrow \varepsilon_1(0)=0; \\ z_2(0)=0\Rightarrow \varepsilon_2(0)=x_1(0),\ \ |\,\varepsilon_2(0)\,|\le \pi. \end{gathered} \tag{26}$$

The goal is to form corrective actions v_1 and v_2 to stabilize the observation errors and their derivatives with the given accuracy and in the given time (19), (22). We use piecewise linear corrective actions [7, 15, 16]:

$$v_1=p_1\mathrm{sat}(l_1\varepsilon_1),\ v_2=p_2\mathrm{sat}(l_2v_1),\ l_i,\ p_i=\mathrm{const}>0,$$

$$\mathrm{sat}(l_1\varepsilon_1)=\begin{bmatrix}\mathrm{sign}(\varepsilon_1),\ |\varepsilon_1|>1/l_1, \\ l_1\varepsilon_1,\ |\varepsilon_1|\le 1/l_1.\end{bmatrix} \tag{27}$$

Like the sigmoid function, the functions (27) are *S*-shaped and have two tunable parameters. They are easier to implement but nonsmooth. However, the latter property is not critical: in the observation problem, the corrective actions have no physical sense and may be nonsmooth. (In contrast, smoothness is required for fictitious controls—the state variables (10).)

Lemma. *Let the external signal* $x_2(t)$ *in system* (25)–(27) *be bounded by condition* (3). *Then for any* $\delta_1>0$, $\delta_2>0$, *and* $T>0$, *there exist positive real numbers* $\bar p_i$ *and* $\bar l_i$ *such that*

$$\begin{gathered}\left|\varepsilon_2(t)\right|=\left|x_1(t)-z_2(t)\right|\le\delta_1, \\ \left|x_2(t)-v_2(t)\right|\le\delta_2,\ t\ge T,\end{gathered} \tag{28}$$

for any $p_i>\bar p_i$ and $l_i\ge\bar l_i$, $i=1,2$.

The proof of this lemma is given in the Appendix. It follows from (19) and (28) that the state variable and the corrective action of the second equation of the reduced-order observer (24) are the desired estimates of the unmeasured variables: $\hat x_1(t)=z_2(t)$, $\hat x_2(t)=v_2(t)$.

4. SIMULATION RESULTS

To check the effectiveness of this dynamic feedback design method, we simulated the closed loop system (1), (2), (20), (24) with the initial conditions $x_i(0)=0,\ i=\overline{1,5}$, in MATLAB-Simulink. The goal of control was to ensure condition (8) with

$$\Delta_1=0.04\ \text{rad},\ t_1=2\ \text{s}. \tag{29}$$

The following values and ranges of the model parameters and exogenous actions were selected:

$$\begin{gathered} k_l=0.2,\ J_m=0.01,\ d=0.045,\ k_m=0.3; \\ \bar m\in[0.18,\ 0.25],\ h\in[0.2,\ 0.3], \\ J_l\in[0.0072,\ 0.0225],\ c\in[0.25,\ 0.33], \\ R\in[3.8,\ 4.2],\ L\in[0.006,\ 0.013]; \\ \left|g^{(i)}(t)\right|\le 0.2,\ i=\overline{0,1};\ \left|f(t)\right|\le 0.1. \end{gathered} \tag{30}$$

Based on inequalities (17) and (A.9)–(A.13) (see the Appendix), we took the following gains:

$$\begin{gathered} k_1=80,\ k_2=25,\ k_3=5,\ k_4=8; \\ m_1=0.3,\ m_2=0.7,\ m_3=10,\ m_4=40,\ m_5=90. \end{gathered} \tag{31}$$

Due to the expressions (19) and (22), the target values for the observation problem were determined as $\delta_1=0.0008$ rad, $\delta_2=0.002$ rad/s, and $T=0.1$ s. The following corrective coefficients (27) were adopted in the observer (24) based on inequalities (A.22) and (A.26) with the constraint $\left|x_2(t)\right|\le 5=X_2$ rad/s:

$$l_1=155,\ l_2=150;\ p_1=60,\ p_2=40. \tag{32}$$

Two numerical experiments were performed with the same controller (31) and observer (32) gains but different plant's parameters and exogenous actions from the ranges (30). In experiment 1, the left limits of the ranges (30) and the exogenous actions $g(t)=0.05|\sin t|+0.15\cos(0.5t)$ and $f=0.05$ were taken as the plant's parameters. In experiment 2, the right limits of the ranges (30) and the exogenous actions $g(t)=0.18|\cos(t)|$ and $f(t)=0.05t,\ t\in[0,2)$ (the sawtooth function with the main period of 2 s) were taken as the plant's parameters. Note that in both experiments, the reference signals are piecewise smooth functions whose derivatives have discontinuities of the first kind. For comparison, we also simulated the system with the static feedback law (11) under the assumption that all state variables are measurable and the system with the dynamic feedback law (20) with the unmeasured variables $\hat x_1(t)$ and $\hat x_2(t)$ estimated using the observer (24), (27). The integration was carried out by the Euler method with a constant step of 10^{-5}.

Figures 1–4 show the simulation results of experiment 1. For system (1), (2) with the dynamic feedback law (20), (24), (27), the following graphs are presented: the reference signal $g(t)$ and the manipulator's angular position $x_1(t)$ (Fig. 1); the tracking error $e_{1\mathrm{d}}(t)=x_1(t)-g(t)$ (Fig. 2); the estimation errors $\alpha_1(t)=x_1(t)-\hat x_1(t)$ and $\alpha_2(t)=x_2(t)-\hat x_2(t)$, i.e., the deviations of the estimates $\hat x_1(t)=z_2(t)$ and $\hat x_2(t)=v_2(t)$ yielded by the observer (24), (27) from the variables $x_1(t)$ and $x_2(t)$ (Fig. 3); $e_{1\mathrm{d}}(t)-e_{1\mathrm{s}}(t)$, i.e., the deviation of $e_{1\mathrm{d}}(t)$ from the tracking error $e_{1\mathrm{s}}(t)$ in the system with the static feedback law (11). Figures 5–8 show similar graphs for experiment 2.

Table 2 provides several control performance indices in both experiments: the settling time t^*: $\left|e_1(t)\right|\le 0.04$, $t\ge t^*$; the overshoot $e_{1\max}\ge\left|e_1(t)\right|$, $t\ge 0$; the tracking accuracy $\bar\Delta_1\ge\left|x_1(t)-g(t)\right|$ in the steady-state mode for $t\ge 10$ s.

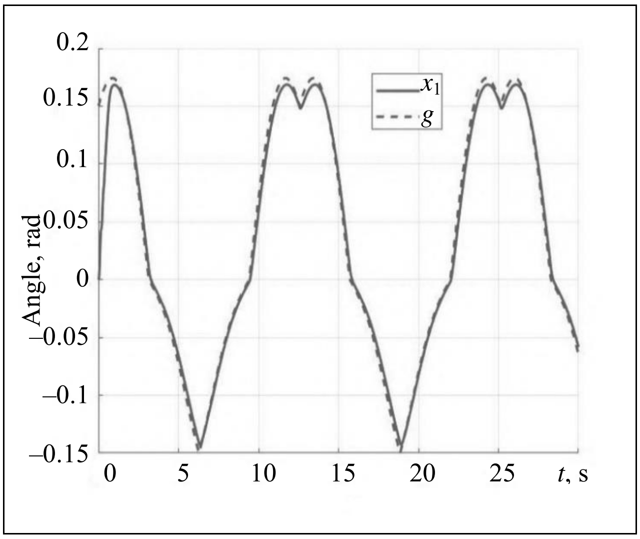

Fig. 1. The graphs of g(t) and x1(t) in experiment 1.

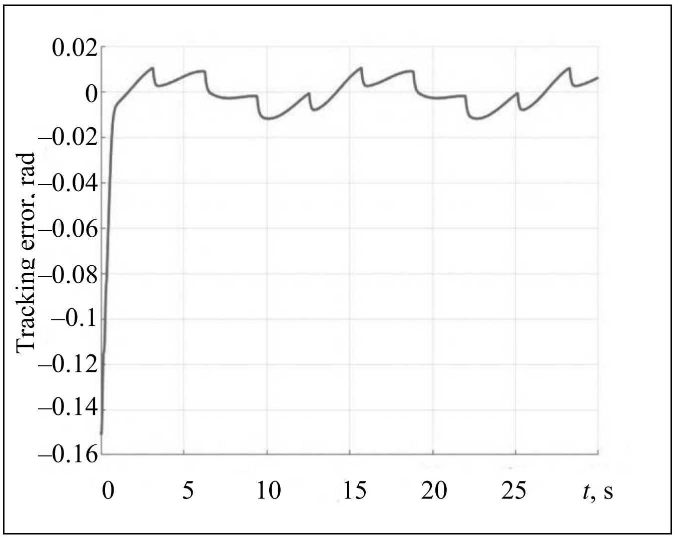

Fig. 2. The graph of tracking error $e_{1d}(t)$ in experiment 2.

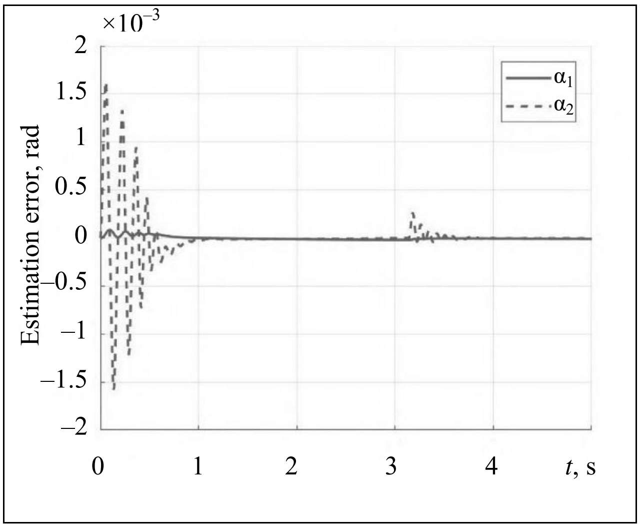

Fig. 3. The graphs of estimation errors $\alpha_1(t) = x_1(t) - \hat{x}_1(t)$ and $\alpha_2(t) = x_2(t) - \hat{x}_2(t)$ in experiment 1.

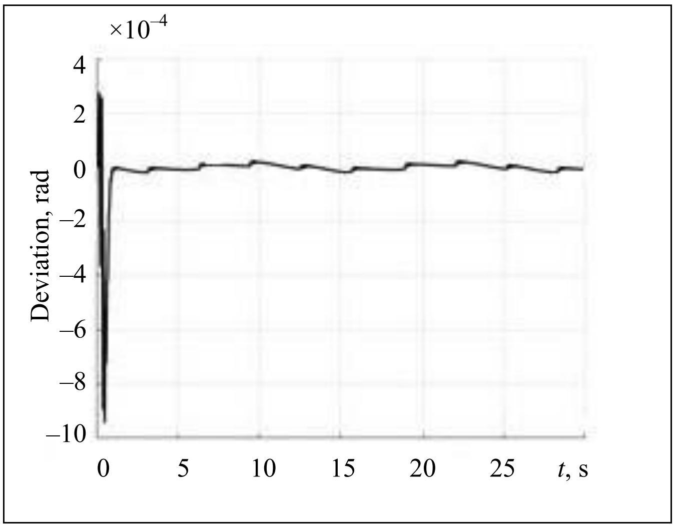

Fig. 4. The graph of deviation $e_{1d}(t) - e_{1s}(t)$ in experiment 1.

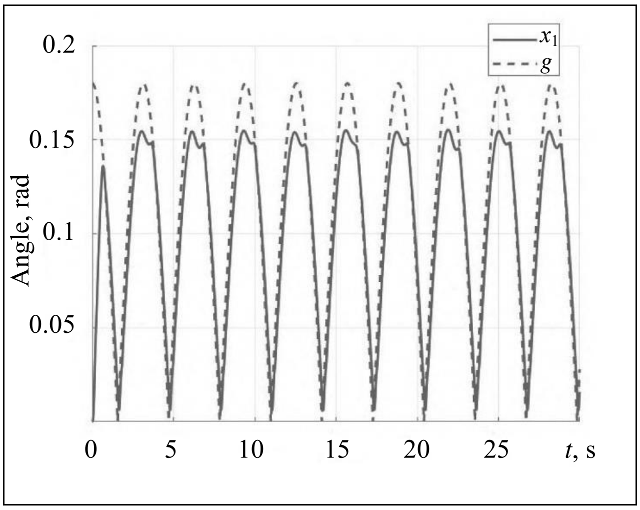

Fig. 5. The graphs of $g(t)$ and $x_1(t)$ in experiment 2.

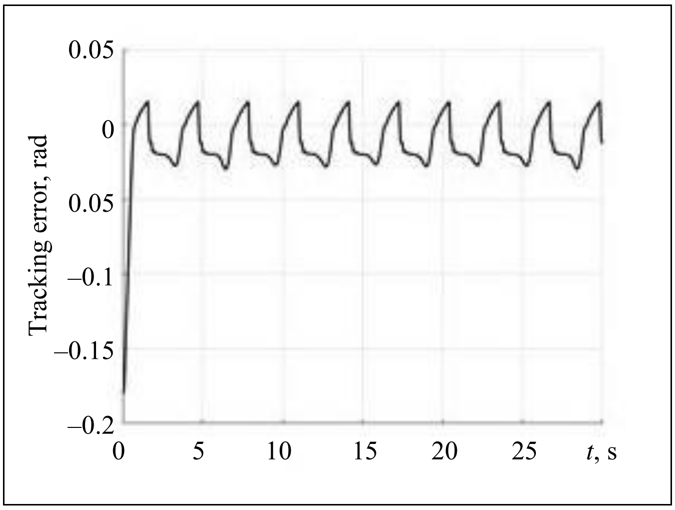

Fig. 6. The graph of tracking error $e_{1d}(t)$ in experiment 2.

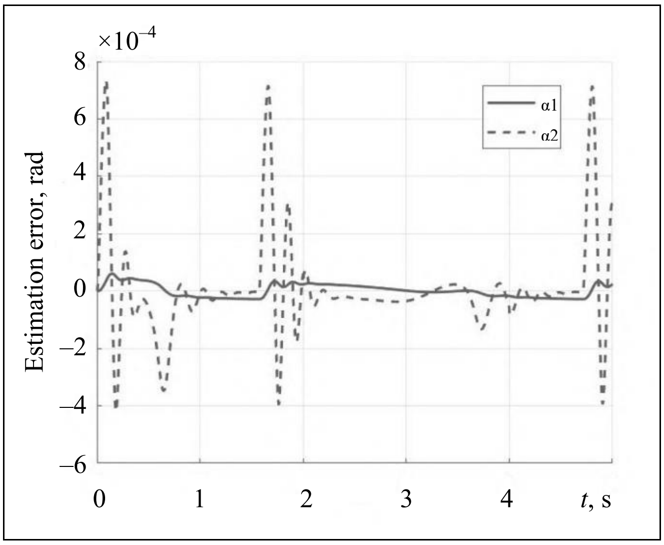

Fig. 7. The graphs of estimation errors $\alpha_1(t) = x_1(t) - \hat{x}_1(t)$ and $\alpha_2(t) = x_2(t) - \hat{x}_2(t)$ in experiment 2.

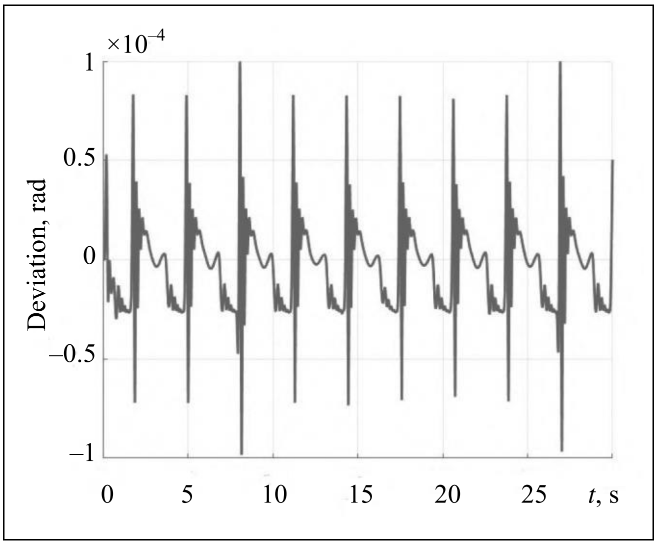

Fig. 8. The graph of deviation $e_{1d}(t)$ - $e_{1s}(t)$ in experiment 2.

Table 2

Control performance indices

Index, measurement unit	Static feedback (11)	Dynamic feedback (20), (24), (27)
Experiment 1		
t^*, s	0.5380	0.5408
$e_{1\max}$, rad	0.1510	0.1510
$\bar{\Delta}_1$, rad	0.0119	0.0119
Experiment 2		
t^*, s	0.5146	0.5147
$e_{1\max}$, rad	0.18	0.18
$\bar{\Delta}_1$, rad	0.0299	0.0299

According to Figs. 1–8 and Table 2, the target values of the performance indices (29) were achieved in all experiments. Introducing the reduced-order observer (24), (27) into the feedback loop caused no significant deterioration of the system performance.

CONCLUSIONS

This paper has considered the following problem: the angular position of a single-link manipulator should track a given reference signal under nonsmooth exogenous disturbances in the case where the sensors are mounted only on the actuator. This problem has been solved by applying a block feedback design procedure with sigmoid fictitious controls tuned for the worst-case admissible values of uncertain parameters and exogenous disturbances. A state observer of reduced order has been constructed to estimate the angular position and velocity of the manipulator. This observer needs no precise knowledge of the parameters of the mechanical subsystem. The results of numerical simulation have confirmed the effectiveness of the developed tracking and observation systems. As shown, the performance indices of the closed loop system with the dynamic feedback based on the reduced-order observer have comparable values with those of the system with full measurements.

Further research will aim at extending the block design procedure of sigmoid fictitious controls to linear plants with several inputs and outputs. Also, the performance of the reduced-order observer will be studied under noisy measurements.

APPENDIX

Procedure (choosing the amplitudes of the true (11) and fictitious (9) controls). We begin with estimating the state variables of system (12). Due to formulas (3)-(5) and (10), we have the following estimates for the initial values:

$$|e_1(0)| \le X_{1,0} + G_0, |e_i(0)| \le X_{i,0} + m_{i-1}, i = \overline{2,5}. \quad \text{(A.1)}$$

In the general case $|e_i(0)| > \Delta_i, i = \overline{1,5},$ the monotonic transients are guaranteed in system (12) only for the last block variable $e_5(t)$. In the worst case, the variables $e_i(t)$, $i = \overline{1,4}$, will grow by absolute value until all variables $e_j(t)$, j = 5,4,...,i+1, reach the given neighborhoods (15), i.e.,

$$|e_5(t)| \le |e_5(0)| = e_{5,\max}, |e_i(t)| \le |e_i(t_{i+1})| = e_{i,\max}, i = \overline{4,1}. \text{(A.2)}$$

In system (1), (2) and, consequently, in system (12), we have a_{ii} = $0, i = \overline{1,3}$, and a_{44} > 0. Due to the expressions

(18), (A.1), and (A.2), the state variables and their derivatives can be estimated as

$$\begin{gathered} e_{1,\max} \le X_{1,0} + G_0 + (e_{2,\max} - \Delta_2) t_2, \\ e_{i,\max} \le X_{i,0} + m_{i-1} + b_{i,\max}(e_{i+1,\max} - \Delta_{i+1}) t_{i+1}, i = 2, 3, \\ e_{4,\max} \le X_{4,0} + m_3 + b_4 (e_{5,\max} - \Delta_5)(1 - \exp(-a_{44} t_5)) / a_{44}, \\ e_{5,\max} \le X_{5,0} + m_4; \end{gathered} \qquad \text{(A.3)}$$

$$\begin{gathered} |\dot e_i(t)| < b_{i,\max}(2m_i + e_{i+1,\max} - \Delta_{i+1}), t \in [0, t_{i+1}), \\ |\dot e_i(t)| < 2 b_{i,\max} m_i,\ t \ge t_{i+1},\ i = \overline{1, 3},\ b_{1,\max} = b_{3,\max} = 1; \\ |\dot e_4(t)| < b_4 (2m_4 + e_{5,\max} - \Delta_5) + a_{44} e_{4,\max},\ t \in [0,\ t_5), \qquad \text{(A.4)} \\ |\dot e_4(t)| < 2 b_4 m_4 + a_{44} e_{4,\max},\ t \in [t_5,\ t_4), \\ |\dot e_4(t)| < 2 b_4 m_4 + a_{44} \Delta_4,\ t \ge t_4. \end{gathered}$$

Considering the separation (16), the derivative of the sigmoid function $\sigma'(k_i e_i) = 0.5 k_i (1 - \sigma^2(k_i e_i))$ satisfies the inequalities

$$\begin{gathered} 0 < \sigma'(k_i e_i) < 0.18 k_i,\ t \in [0, t_i),\ |e_i(t)| > 2.2 / k_i, \\ 0.18 k_i \le \sigma'(k_i e_i) \le 0.5 k_i,\ t \ge t_i,\ |e_i(t)| \le 2.2 / k_i, \\ i = \overline{1, 4}. \end{gathered} \qquad \text{(A.5)}$$

Let us restrict the maximum absolute values of the time-dependent residuals (A.3) by

$$e_{1,\max} \le 2\pi, e_{i+1,\max} \le 3 m_i + \Delta_{i+1}, i = \overline{1, 3}. \qquad \text{(A.6)}$$

Then the expressions (A.3) take the form

$$\begin{gathered} e_{1,\max} \le X_{1,0} + G_0 + 3 m_1 t_2 \le 2\pi, \\ e_{i,\max} \le X_{i,0} + m_{i-1} + 3 b_{i,\max} m_i t_{i+1} \le 3 m_{i-1} + \Delta_i,\ i = 2,\ 3, \\ e_{4,\max} \le X_{4,0} + m_3 + b_4 (X_{5,0} + m_4 - \Delta_5) \times \\ (1 - \exp(-a_{44} t_5)) / a_{44} \le 3 m_3 + \Delta_4. \end{gathered} \qquad \text{(A.7)}$$

Using formulas (A.4)–(A.7), we obtain the following estimates for the derivatives of fictitious controls (13):

$$\begin{gathered} |\Lambda_i(t)| = m_i \frac{k_i (1 - \sigma^2(k_i e_i))}{2} |\dot e_i| \le k_i m_i^2 b_{i,\max}, i = \overline{1, 3}; \\ |\Lambda_4(t)| \le k_4 m_4^2 b_4 + 0.5 k_4 m_4 a_{44} e_{4,\max}, t \ge 0. \end{gathered} \qquad \text{(A.8)}$$

To satisfy inequalities (A.6), the amplitudes m_i, $i = \overline{1, 4}$, must be bounded from above. Assume for convenience that $0 < \Delta_i = X_{i,0}$, $i = \overline{2, 5}$. Then the right-hand sides of inequalities (A.7) yield

$$\begin{gathered} m_1 \le m_{1,\max} = \frac{2\pi - X_{1,0} + G_0}{3 t_2},\ m_i \le m_{i,\max} = \frac{2 m_{i-1}}{3 b_{i,\max} t_{i+1}}, \\ i = 2,\ 3,\ m_4 \le m_{4,\max} = \frac{2 m_3 a_{44}}{b_4 (1 - \exp(-a_{44} t_5))}. \end{gathered} \qquad \text{(A.9)}$$

Obviously, the upper bounds on the amplitudes (A.9) can be made arbitrarily large by decreasing t_i, $i = \overline{2, 5}$, within the hierarchy $0 < t_5 < t_4 < ... < t_2 < t_1$.

Now we formalize the sequential choice procedure for the amplitudes m_i, $i = \overline{1, 5}$, to satisfy conditions (15) in the closed loop system (12). (As a result, the goal of control (8) will be achieved under the given values Δ_1, t_1, $\Delta_i = X_{i,0}$, $i = \overline{2, 5}$, and the corresponding gains (17)). The amplitudes should be chosen to ensure the convergence of the residuals $e_i(t)$, $i = \overline{5, 1}$, on the intervals $[t_{i+1}, t_i]$, $t_6 = 0$, to the given neighborhoods of zero, considering the expressions (18) and (A.7)–(A.9). The parameters varied are the time instants t_i, $i = \overline{2, 5}$.

Step 1. Given (A.7) and the convergence interval $[t_2, t_1]$, the first inequality (18) takes the form

$$\begin{gathered} 0.8 m_1 \ge \frac{X_{1,0} + G_0 + 3 m_1 t_2 - \Delta_1}{t_1 - t_2} + G_1 + X_{2,0} \Rightarrow \\ m_1 \ge m_{1,\min} = \frac{X_{1,0} + G_0 - \Delta_1 + (G_1 + X_{2,0})(t_1 - t_2)}{0.8 t_1 - 3.8 t_2}. \end{gathered} \qquad \text{(A.10)}$$

From inequality (A.10) it follows that $0.8 t_1 - 3.8 t_2 > 0 \Rightarrow t_2 < 0.2 t_1$, where $0 < t_2 < t_1$. Fixing the values t_2^* and m_1^* by

$$\begin{gathered} 0 < t_2^* < 0.2 t_1 : m_{1,\min}(t_2^*) < m_{1,\max}(t_2^*), \\ m_1^* \in [m_{1,\min}(t_2^*),\ m_{1,\max}(t_2^*)], \end{gathered}$$

we move to the next step of the procedure.

Step i (i = 2, 3). Given (A.7), (A.8), and the convergence interval $[t_{i+1},\ t_i^*]$, the ith inequality in (18) takes the form

$$\begin{gathered} 0.8 b_{i,\min} m_i \ge \frac{m_{i-1}^* + 3 b_{i,\max} m_i t_{i+1}}{t_i^* - t_{i+1}} + b_{i,\min} X_{i+1,0} + \\ \sum_{j=1}^{i-1} a_{ij,\max} e_{j,\max}(m_j^*) + F_i + k_{i-1} (m_{i-1}^*)^2 b_{i-1,\max} \Rightarrow \\ m_i \ge m_{i,\min} = \frac{m_{i-1}^* + (b_{i,\min} X_{i+1,0} + \sum_{j=1}^{i-1} a_{ij,\max} e_{j,\max}(m_j^*)}{0.8 b_{i,\min} t_i^* - (0.8 b_{i,\min} + 3 b_{i,\max}) t_{i+1}} + \\ \frac{F_i + k_{i-1} (m_{i-1}^*)^2 b_{i-1,\max})(t_i^* - t_{i+1})}{0.8 b_{i,\min} t_i^* - (0.8 b_{i,\min} + 3 b_{i,\max}) t_{i+1}},\ i = 2,\ 3. \end{gathered} \qquad \text{(A.11)}$$

From inequality (A.11) it follows that $0.8 b_{i,\min} t_i^* - (0.8 b_{i,\min} + 3 b_{i,\max}) t_{i+1} > 0 \Rightarrow\ t_{i+1} < 0.2 b_{i,\min} t_i^* / b_{i,\max}$, $i = 2,\ 3$, $b_{3,\min} = b_{3,\max} = 1$. Fixing the values t_{i+1}^* and m_i^* by

$$\begin{gathered} t_{i+1}^* < 0.2 b_{i,\min} t_i^* / b_{i,\max} : m_{i,\min}(t_{i+1}^*) < m_{i,\max}(t_{i+1}^*), \\ m_i^* \in [m_{i,\min}(t_{i+1}^*), m_{i,\max}(t_{i+1}^*)], \end{gathered}$$

we move to the next step of the procedure.

Step 4. Given (A.7), (A.8), and the convergence interval $[t_5, t_4^*]$, the fourth inequality in (18) takes the form

$$\begin{gathered} 0.8 b_4 m_4 \ge \frac{m_3^* + b_4 m_4 (1 - \exp(-a_{44} t_5)) / a_{44}}{t_4^* - t_5} + \\ + b_4 X_{5,0} + a_{41} e_{1,\max} + a_{43} e_{3,\max} + F_4 + k_3 (m_3^*)^2 \Rightarrow \\ m_4 \ge m_{4,\min} = \frac{m_3^* + [b_4 X_{5,0} + a_{41}(X_{1,0} + G_0 + 3 m_1^* t_2^*)}{b_4 (0.8 (t_4^* - t_5) - (1 - \exp(-a_{44} t_5)) / a_{44})} + \\ \frac{a_{43}(X_{3,0} + m_2^* + 3 m_3 t_4^*) + F_4 + k_3 (m_3^*)^2](t_4^* - t_5)}{b_4 (0.8 (t_4^* - t_5) - (1 - \exp(-a_{44} t_5)) / a_{44})}. \end{gathered} \qquad \text{(A.12)}$$

From inequality (A.12) it follows that $0.8 t_5 + (1 - \exp(-a_{44} t_5)) / a_{44} < 0.8 t_4^*$. Fixing the values t_5^* and m_4^* by

$$t_5^* + 1.25(1 - \exp(-a_{44} t_5^*)) / a_{44} < t_4^* : m_{4,\min}(t_5^*) < m_{4,\max}(t_5^*),$$
$$m_4^* \in [m_{4,\min}(t_5^*), m_{4,\max}(t_5^*)],$$

we move to the last step of the procedure.

Step 5. Given (14), (A.7), (A.8), and the convergence interval $[0, t_5^*]$, the last inequality in (18) takes the form

$$\begin{gathered} b_{5,\min} m_5 \geq \frac{X_{5,0} + m_4^*}{t_5^*} + a_{54,\max} m_3^* + a_{55,\max} m_4^* + \\ k_4 (m_4^*)^2 b_4 + (a_{54,\max} + 0.5 k_4 m_4^* a_{44}) \times \\ (X_{4,0} + m_3^* + b_4 m_4^*)(1 - \exp(-a_{44} t_5^*)) / a_{44}). \end{gathered} \quad (A.13)$$

The amplitude choice procedure is complete. ♦

Proof of the lemma. When solving the control problem, the variables of the closed loop system (12) converge to some neighborhood of zero sequentially bottom-to-top (15): first, the convergence of e_5 is ensured, then that of e_4, and so on until achieving the goal of control (the convergence of e_1). When solving the observation problem in system (25), on the contrary, the order of convergence of the observation errors and their derivatives in the neighborhood of zero is “top-to-bottom”:

$$|\varepsilon_1(t)| \leq 1/l_1, \; t \geq 0; \quad (A.14)$$

$$|a_{43}\varepsilon_2(t) - v_1(t)| = |\gamma_1(t)| \leq a_{43}\beta_2, \; t \geq t_{01}; \quad (A.15)$$

$$|\varepsilon_2(t)| \leq \beta_2 + 1/(a_{43} l_2), \; t \geq t_{02}, \; 0 < t_{01} < t_{02} < T < t_5, \quad (A.16)$$

where $\beta_2 = \text{const} > 0$.

Inequalities (A.14), (A.16) and the time when the arguments of the corrective actions (27) fall in the neighborhood of zero, where the correcting actions are described by linear functions without saturation (hereinafter, the linear zones), are ensured by choosing the corresponding amplitudes p_1 and p_2. Inequality (A.15), the second inequality in (28), and the given estimation accuracy (19) are ensured by choosing the gains l_1 and l_2. Let us formalize sufficient conditions for choosing the parameters of the corrective actions (27) that satisfy these requirements.

First, we tune the amplitudes. Due to the expression (26), $\varepsilon_1(0) = 0 \leq 1/l_1$, i.e., the variable $\varepsilon_1(t)$ is initially in the linear zone. Inside this zone, the first equation of system (25), (27) has the form $\dot{\varepsilon}_1 = a_{43}\varepsilon_2 - p_1 l_1 \varepsilon_1$. Based on its form outside the linear zone, $\dot{\varepsilon}_1 = a_{43}\varepsilon_2 - p_1 \text{sign}(\varepsilon_1)$, we obtain sufficient conditions for choosing the value p_1 to satisfy inequality (A.14):

$$\begin{gathered} p_1 > a_{43}|\varepsilon_2| \Rightarrow \varepsilon_1\dot{\varepsilon}_1 = \varepsilon_1(a_{43}\varepsilon_2 - p_1\text{sign}(\varepsilon_1)) \leq \\ |\varepsilon_1|(a_{43}|\varepsilon_2| - p_1) < 0. \end{gathered} \quad (A.17)$$

In the second equation of system (25), (27), the equality $\text{sign}(v_2(t)) = \text{sign}(\varepsilon_2(t))$ holds outside the domain $|\varepsilon_2(t)| \leq \beta_2$ for $t \geq t_{01}$ under condition (A.15). For the worst case, the expressions (A.15) and (A.16) yield

$$\dot{\varepsilon}_2 = \begin{bmatrix} x_2 + p_2\text{sign}(\varepsilon_2), \; t \in [0, t_{01}), \\ x_2 - p_2\text{sign}(\varepsilon_2), \; t \in [t_{01}, t_{02}), \\ x_2 - p_2 l_2 (a_{43}\varepsilon_2(t) \pm \gamma_1), \; t \geq t_{02}. \end{bmatrix} \quad (A.18)$$

Given (3), the maximum absolute value of the variable $\varepsilon_2(t)$ is reached at $t = t_{01}$:

$$|\varepsilon_2(t)| \leq |\varepsilon_2(t_1)| \leq \pi + (X_2 + p_2)t_{01} = E_2, \; t \geq 0. \quad (A.19)$$

Sufficient conditions for choosing the value p_2 are similar to (A.17). Due to (A.19), the convergence to the linear zone (A.16) on the interval $[t_{01}, t_{02})$ is ensured if

$$\begin{gathered} p_2 \geq \frac{\pi + (X_2 + p_2)t_{01} - \delta_1}{t_{02} - t_{01}} + X_2 \Rightarrow \\ p_2 \geq \frac{\pi + X_2 t_{02} - \delta_1}{t_{02} - 2t_{01}}. \end{gathered} \quad (A.20)$$

From the expression (A.20) it follows that $t_{02} > 2t_{01}$. This constraint must be considered when assigning the time intervals. For example, let

$$t_{02} - 2t_{01} = T - t_{02} = t_{01} \Rightarrow t_{01} = T/4. \quad (A.21)$$

Combining (A.17) and (A.19)–(A.21), we obtain the final inequalities for choosing the amplitudes of the corrective actions (27) sequentially to satisfy conditions (A.14) and (A.16) in the given time:

$$\begin{gathered} p_2 \geq \bar{p}_2 = \frac{4(\pi - \delta_1)}{T} + 3X_2, \\ p_1 > \bar{p}_1 = a_{43}(\pi + (X_2 + p_2)T/4). \end{gathered} \quad (A.22)$$

Next, we tune the gains of the corrective actions (27) to satisfy conditions (A.15) and (28). For this purpose, we estimate the solutions of system (25), (27) in linear zones (the first equation on the interval $[0, t_{01}]$, and the second equation on the interval $[t_{02}, t_{02} + t_{01} = T]$). Based on the third equation in (A.18) and (A.19) and (A.21) we have:

$$\begin{gathered} |\varepsilon_1(t_1)| \leq \frac{a_{43}E_2}{p_1 l_1} + \frac{p_1 - a_{43}E_2}{p_1 l_1} e^{-p_1 l_1 t_{01}} \Rightarrow \\ p_1 l_1 |\varepsilon_1(t_1)| - a_{43}E_2 \leq (p_1 - a_{43}E_2) e^{-p_1 l_1 t_{01}}, \\ |a_{43}\varepsilon_2(t) - v_1(t)| \leq a_{43}\beta_2, \; t \geq t_{01} \Leftrightarrow \\ (p_1 - a_{43}E_2) e^{-p_1 l_1 T/4} \leq a_{43}\beta_2; \end{gathered} \quad (A.23)$$

$$\begin{gathered} |\varepsilon_2(T)| \leq \frac{X_2}{p_2 l_2 a_{43}} + \beta_2 + \frac{p_2 - X_2}{p_2 l_2 a_{43}} e^{-p_2 l_2 a_{43} t_{01}} \leq \delta_1, \\ p_2 l_2 a_{43} (|\varepsilon_2(T)| - \beta_2) - X_2 \leq (p_2 - X_2) e^{-p_2 l_2 a_{43} t_{01}}, \\ |x_2(t) - v_2(t)| \leq \delta_2, t \geq T \Leftrightarrow (p_2 - X_2) e^{-p_2 l_2 a_{43} T/4} \leq \delta_2. \end{gathered} \quad (A.24)$$

According to (A.23) and (A.24), the observation errors for $t \geq T$ converge to the following neighborhood of zero:

$$|\varepsilon_1(t)| \leq \frac{a_{43}(E_2 + \beta_2)}{p_1 l_1}; \; |\varepsilon_2(t)| \leq \frac{X_2 + \delta_2}{p_2 l_2 a_{43}} + \beta_2 \leq \delta_1. \quad (A.25)$$

For example, let $\beta_2 = \delta_1 / 2$. Considering (A.23)–(A.25), the given accuracy (19) is achieved if the gains with the fixed amplitudes (A.22) satisfy

$$\begin{gathered} l_1 \geq \bar{l}_1 = \frac{4}{p_1 T} \ln \frac{2(p_1 - a_{43}E_2)}{a_{43}\delta_1}; \\ l_2 \geq \bar{l}_2 = \frac{1}{p_2 a_{43}} \max\left\{ \frac{2(X_2 + \delta_2)}{\delta_1}; \; \frac{4}{T} \ln \frac{p_2 - X_2}{\delta_2} \right\}. \end{gathered} \quad (A.26)$$

Thus, there exist $\bar{p}_i > 0$ (A.22) and $\bar{l}_i > 0$ (A.26) such that the lemma conditions (28) hold for any $p_i > \bar{p}_i$ and $l_i \geq \bar{l}_i$, $i = 1, 2$. ♦

REFERENCES

1. Spong, M., Hutchinson, S., and Vidyasagar, M., *Robot Modeling and Control*, New York: Wiley, 2005.
2. Angeles, J., *Fundamentals of Robotic Mechanical Systems: Theory, Methods and Algorithms*, 3rd ed.
3. Golubev, A.E., Stabilization of Single-Link Manipulator with Incomplete State Measurement: Feedback by the Angular Coordinate of the Motor Shaft, *Science and Education. Scientific Edition of Bauman MSTU*, 2012, no. 11, pp. 395–412. (In Russian.)
4. Anan'evskii, I.M., Control of Mechanical Systems with Uncertain Parameters by Means of Small Forces, *Journal of Applied Mathematics and Mechanics*, 2010, no. 74, pp. 95–107.
5. Varghese, E.S., Vincent, A.K., and Bagyaveereswaran, V., Optimal Control of Inverted Pendulum System Using PID Controller, LQR and MPC, *IOP Conference Series Materials Science and Engineering*, 2017, vol. 263, no. 5.
6. Utkin, V.I., Guldner, J., and Shi, J., *Sliding Mode Control in Electromechanical Systems*, New York: CRC Press, 2009.
7. Krasnov, D.V. and Antipov, A.S., Designing a Double-Loop Observer to Control a Single-Link Manipulator under Uncertainty, *Control Sciences*, 2021, no. 4, pp. 23–33.
8. Feng, H., Qiao, W., Yin, C., et al., Identification and Compensation of Nonlinear Friction for an Electro-Hydraulic System, *Mechanism and Machine Theory*, 2019, vol. 141, pp. 1–13.
9. Pesterev, A.V., Rapoport, L.B., and Tkachev, S.B., Canonical Representation of a Nonstationary Path Following Problem, *Journal of Computer and Systems Sciences International*, 2015, vol. 54, no. 4, pp. 656–670.
10. Utkin, V.A. and Utkin, A.V., Problem of Tracking in Linear Systems with Parametric Uncertainties under Unstable Zero Dynamics, *Automation and Remote Control*, 2014, vol. 75, no. 9, pp. 1577–1592.
11. Krasnova, S.A., Sirotina, T.G., and Utkin, V.A., A Structural Approach to Robust Control, *Automation and Remote Control*, 2011, vol. 72, no. 8, pp. 1639–1666.
12. Antipov, A.S., Krasnova, S.A., and Utkin, V.A., Synthesis of Invariant Nonlinear Single-Channel Sigmoid Feedback Tracking Systems Ensuring Given Tracking Accuracy, *Automation and Remote Control*, 2022, vol. 83, no. 1, pp. 32–53.
13. Tsypkin, Y. and Polyak, B., High-Gain Robust Control, *European J. Control*, 1999, vol. 5, pp. 3–9.
14. Busurin, V.I., Win, Y.N., and Zheglov, M.A., Effect of Linear Acceleration on the Characteristics of an Optoelectronic Ring Transducer of Angular Velocity and Its Compensation, *Optoelectronics, Instrumentation and Data Processing*, 2019, vol. 55, no. 3, pp. 309–316.
15. Krasnova, S.A., Estimating the Derivatives of External Perturbations Based on Virtual Dynamic Models, *Automation and Remote Control*, 2020, vol. 81, no. 5, pp. 897–910.
16. Kokunko, Ju.G., Krasnov, D.V., and Utkin, A.V., Two Methods of Synthesis of State and Disturbances Observers for an Unmanned Aerial Vehicle, *Control Sciences*, 2020, no. 1, pp. 3–16. (In Russian.)
17. Spong, M., Modeling and Control of Elastic Joint Robots, *ASME Journal of Dynamic Systems, Measurement and Control*, 1987, vol. 109, pp. 310–319.

This paper was recommended for publication
by L. B. Rapoport, a member of the Editorial Board.

Received May 5, 2022, and revised June 28, 2022.
Accepted June 29, 2022

Author information

Antipov, Aleksei Semenovich. Cand. Sci. (Eng.), Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ scholess18@mail.ru

Krasnov, Dmitry Valentinovich. Researcher, Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ dim93kr@mail.ru

Cite this paper

Antipov, A.S. and Krasnov, D.V. Tracking System Design for a Single-Link Sensorless Manipulator under Nonsmooth Disturbances. *Control Sciences* **3,** 2–12 (2022). http://doi.org/10.25728/cs.2022.3.1

Translated into English by *Alexander Yu. Mazurov,*
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com

DOI: http://doi.org/10.25728/cs.2022.3.2

MANAGEMENT OF TECHNOGENIC SAFETY BASED ON A RISK-ORIENTED APPROACH[1]

V.V. Moskvichev[1], U.S. Postnikova[1], and O.V. Taseiko[2]

[1]Federal Research Center for Information and Computational Technologies,
Krasnoyarsk Branch, Krasnoyarsk, Russia
[2]Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia

✉ krasn@ict.nsc.ru, ✉ ulyana-ivanova@inbox.ru, ✉ taseiko@gmail.com

Abstract. This paper proposes a managerial decision algorithm based on the developed risk assessment methodology with multidimensional statistical analysis. The methodology allows calculating an acceptable risk level, which can be used in regulatory documents. The decision algorithm is integrated into the information system of territorial risk and safety management. The industrial agglomerations of Siberia are chosen as the object of study, and their main types of technogenic hazards are analyzed. The complex risk is assessed using statistical data on man-made dangerous events, emergencies, material damage, and fatal outcomes from the official database (the Emercom of Russia). According to risk factor analysis, the main technogenic load in territorial units is due to fire and explosive events. The inverse problem is solved, showing the need to reduce the main risk factors for achieving an acceptable level. Minimizing the complex technogenic territorial risk is a management problem with two criteria: the minimum number of fatal outcomes and the minimum amount of damage. Within the complex risk assessment approach, the problem is solved by proposing preventive measures to improve territorial safety.

Keywords: socio-natural-technogenic system, territorial risk, management.

INTRODUCTION

The sustainable development of territories is based on balancing economic growth, safety, social responsibility, and environmental conditions. To implement effective management, it is advisable to analyze territorial units using the concept of a socio-natural-technogenic (S-N-T) system [1–5]. Such a system represents a unified complex of interrelated elements of the social and ecological technosphere with different groups of risks [2, 6, 7]. In the presence of hazardous natural processes and the growing number of complex man-made systems, the conditions for developing territorial units are related to realizing, identifying, and minimizing risks[2]. The requirements for risk identification, assessment, and management were enshrined in federal laws [8–10], and the need to counteract the factors that may, directly or indirectly, deteriorate national interests was reflected in the decrees of the President of the Russian Federation [11, 12].

Intelligent systems are created for comprehensive management tasks at different levels and in different areas. Such systems integrate, store, and process significant flows of information. In recent years, many software complexes and systems have been developed in Russia and abroad to process monitoring information [13–28]. However, such systems have a highly

[1] This work was supported by the Russian Federation President grant no. NSh-421.2022.4.

[2] Risk is a quantitative measure of hazard that simultaneously characterizes the occurrence of unfavorable phenomena, events, or processes in a complex S-N-T system and the severity of their consequences [29].

specialized orientation. Under the rapidly growing volumes and flows of information, assessing the state of S-N-T systems is a complex scientific and applied problem. It can be solved by developing information-analytical systems with risk assessment.

The greatest hazard[3] for human life and health is posed by man-made accidents and disasters. They characterize the technosphere, a component of the S-N-T system. Violations of technological, managerial, and organizational processes in industrial and administrative activities cause a wide range of technogenic dangerous events: transport accidents, explosions and large fires, collapses of supporting structures, accidents involving the release of hazardous chemical and radiation substances, destruction of main pipelines, and accidents in life support systems (power grids, housing and communal services systems, and heating networks).

1. ANALYSIS AND PROBLEM STATEMENT

In this paper, we analyze and assess the technogenic load in industrial agglomerations of the Siberian Federal District (SFD): Krasnoyarsk, Novosibirsk, and Omsk. The greatest hazard in these territories is all types of fires, large motor vehicle accidents, and accidents in life support systems.

Urbanization processes and the growing industry in cities negatively affect environmental and social safety. They cause several problems requiring the constant attention of federal and municipal authorities:

– the high concentration of potential hazards in limited areas (nuclear cycle enterprises, the military-industrial complex, pipelines, oil and gas storage facilities, hydroelectric power plants, chemical and metallurgical production, etc.);

– the increased probability of emergencies due to high wear and tear of the main production assets;

– the factors associated with a low safety culture.

To date, a major problem is to improve the sustainable development and operation of territorial units through effective management. To solve this problem, we propose using an information system of territorial risk and safety management (further called the information system, IS) [1]. It is intended to identify territorial risks and minimize them to scientifically reasonable acceptable levels.[4] This system allows integrating the accumulated experience in the network monitoring of the environment and technosphere, analysis technologies for large volumes of information, safety and risk theory, territorial management mechanisms, and methods of forecasting socio-economic development.

2. A METHODOLOGY FOR ASSESSING COMPLEX TECHNOGENIC TERRITORIAL RISK

The complex technogenic territorial risk and the limit state of the technosphere objects within the S-N-T system are assessed using hierarchical cluster analysis [5, 31]. We divide the SFD territories into cluster groups and select a reference group for comparison and determination of the acceptable risk level.

Hierarchical cluster analysis allows grouping objects with similar characteristics. At the first step, each object (territorial unit) in a sample is considered a separate cluster. The clusters are formed sequentially by uniting the closest objects. The objects are classified by their similarity depending on the metric distance between them. Each object is described by k features and represented as a point in the k-dimensional space, and its similarity with other objects is defined through a corresponding measure. If the similarity matrix has the initial dimensions $m \times m$, the clustering process will be completed in $(m - 1)$ steps; eventually, all objects will be combined into one cluster.

The risk assessment methodology based on cluster analysis includes eight stages as follows.

Stage 1 (formulation of the problem). It is required to analyze the technogenic safety of SFD cities with over 70 thousand residents according to the municipal unit classification [32].

Stage 2. Quantitative indicators are selected for the analysis (statistical data from the official database of the computerized information and management system for emergency prevention and control for the period 1999–2020).

Stage 3. The initial indicators are represented as the quantitative values of vulnerability[5]. They have a probabilistic nature and vary in the range [0, 1]:

$$\vartheta = \{p_a; p_f ;p_e\}, \qquad (1)$$

[3] *Hazard* is an objectively existing possibility of an adverse effect on an object or process, which may cause any damage or harm deteriorating its state and assigning undesirable dynamics or parameters (in terms of character, pace, form, etc.) [30].

[4] *The acceptable risk level* is a scientifically grounded quantitative risk value that can be accepted by a person, society, and the state during a given period [29].

[5] *Vulnerability* is a system parameter characterizing the possibility of any damage to a given system [33]; for territorial units, vulnerability is defined as the degree of possible losses due to the adverse effect of some process or phenomenon of a given level [30].

where ϑ denotes the vulnerability of a territory, and p_a, p_f, and p_e are the probabilities of a dangerous event, a fatal outcome in a dangerous event, and an emergency, respectively. Based on vulnerability values, the cities are divided into cluster groups.

Stage 4 concerns determining the distance between objects in a conditional multidimensional space. The Euclidean distance and its square, the Manhattan distance (between city blocks), and the Chebyshev distance are commonly used to measure the distance between two points (characterizing the proximity or similarity of objects) in the coordinate axes *x* and *y*. Different measures are applied to justify the correctness of clustering. The uniform distribution of clusters obtained by different measures validates the chosen classification method.

Stage 5. A clustering method is chosen to calculate the distances between clusters. Ward's method is the best clustering method for objects with a "blurred" structure and fuzzy condensation. This method yields small and compact clusters as follows. In the first step, each cluster consists of one object. Next, the two closest clusters are combined. For these clusters, the average values of each feature are determined, and the sum of squared deviations is calculated:

$$V_k = \sum_{i=1}^{n_k}\sum_{j=1}^{p}\left(x_{ij} - \bar{x}_{jk}\right)^2,$$

where the subscripts *k*, *i*, and *j* correspond to the cluster, object, and feature, respectively; *p* is the number of features characterizing each object; n_k is the number of objects in cluster *k*; $\bar{x}_{jk}$ is the average value of feature *j* in cluster *k*; finally, x_{ij} is the value of feature *j* for object *i*.

The clusters with the smallest increase in the total sum of distances are combined into one group.

Stage 6 is to determine the number of hierarchical tree clusters. In this paper, we determine the number of clusters using k-means: for a specified number of clusters (2, 3, 4, etc.), the division of the hierarchical tree is checked sequentially.

Stage 7 deals with a quantitative assessment of technogenic risks for each cluster group. The complex technogenic territorial risk R_c (further called the risk value) is assessed by the formula

$$R_c = \sum_{i=1}^{n} N_i\left(Q_i\right)P_i\left(Q_i\right)U_i\left(N_i, Q_i\right),$$

$$R_c \le [R], \tag{2}$$

where n denotes the number of hazard types; $N_i\left(Q_i\right)$ is the probability of fatal outcomes (the number of deaths divided by population size) due to the realization of different hazard types; $P_i\left(Q_i\right)$ is the probability of a dangerous event on a given territory per unit time; $U_i\left(N_i, Q_i\right)$ is the material damage from a source of hazards and fatal outcomes, in RUB; finally, $[R]$ is an acceptable risk level, in RUB per year. The assessment (2) covers the entire list of hazards in a given territory and the amount of damage due to the corresponding dangerous events.

Stage 8. A reference group of clusters with the lowest risk value is selected. The acceptable risk level is calculated as a confidence interval over the reference group [5, 31]. For large Siberian cities with over 70 thousand residents, the calculated acceptable risk level corresponds to the interval [0, 2.1].

Additional data analysis is required when obtaining a high risk value. Here, the best approach is to solve inverse problems (determine the dominant factors affecting the risk value and identify the parameters to be managed). In optimal conditions, within the concept of non-zero risk, the total value of the complex technogenic territorial risk over various types of man-made events should not exceed the acceptable value:

$$R_c = \sum_{i=1}^{n} R_{c_i} = R_{c_1} + R_{c_2} \ldots + R_{c_n}$$

$$R_{c_1} \ll [R];\ R_{c_2} \ll [R]; \ldots R_{c_n} \ll [R], \tag{3}$$

where R_{c_i} is the complex technogenic territorial risk due to the realization of given-type events.

Upon determining the dominant factors, it is necessary to minimize the risk value through appropriate measures. Risk management methods are directed actions to reduce hazards and their consequences. Minimizing the risk value (2) is a management problem with two criteria: the minimum number of fatal outcomes $F\left(N_i\right)$ and the minimum amount of damage $F\left(U_i\right)$:

$$\begin{cases} F_1\left(N_i\right) \to \min, \\ F_2\left(U_i\right) \to \min. \end{cases}$$

Imposing an upper bound constraint *C* on one criterion, we obtain two optimization problems:

$$\begin{cases} F_1\left(N_i\right) \to \min\ , \\ F_2\left(U_i\right) \le C_1, \end{cases} \quad \begin{cases} F_2\left(U_i\right) \to \min\ , \\ F_1\left(N_i\right) \le C_2. \end{cases} \tag{4}$$

The rapid response to an emergency to reduce material losses directly depends on the number of fire and rescue units. On the other hand, the availability of a sufficient number of medical facilities can reduce the number of fatal outcomes. To elaborate protection improvement measures, an important problem is to assess quantitatively the provision $Z_{(\tau)}$ of the necessary number of medical facilities and fire and rescue units in the territorial entity:

$$Z_{(\tau)} = \left(\frac{N_{\text{fire}}^{\text{fact}} + N_{\text{med}}^{\text{fact}}}{N_{\text{fire}}^{\text{norm}} + N_{\text{med}}^{\text{norm}}} \right) \cdot 100 \geq 100\%, \qquad (5)$$

where $N_{\text{fire}}^{\text{fact}}$ and $N_{\text{fire}}^{\text{norm}}$ are the factual and normative numbers of fire and rescue units in a given territory, and $N_{\text{med}}^{\text{fact}}$ and $N_{\text{med}}^{\text{norm}}$ are the factual and normative numbers of medical facilities in a given territory.

A territory is protected if $Z_{(\tau)}$ ≥ 100%, i.e., the factual numbers of medical facilities and fire and rescue units are not smaller than their normative counterparts. The normative number of fire and rescue units is calculated using the normative number of personnel of fire protection units involved in rescue work and the standard staffing structure:

$$N_{\text{fire}}^{\text{norm}} = \frac{N_{\text{res}}}{N_{\text{fire}} N_{\text{staff}}}, \qquad (6)$$

where N_{res} is the number of residents in a given territory; N_{fire} is the number of residents per one member of the fire and rescue unit; finally, N_{staff} is the typical number of rescuers in the unit.

The number N_{fire} is calculated as [34]

$$N_{\text{fire}} = 0.036757 \cdot P \left(0.036648 + 98.781 \cdot P^{-0.44823} \right)^2, \ (7)$$

where P is the population density in the territory.

The normative number of medical facilities is determined according to the regulatory document of the Ministry of Health [35].

Thus, the clustering of territorial units by the technogenic danger indicators (1) together with the cluster assessments of risks (2) and (3) and protection (5)–(7) are used to analyze the technogenic safety of territorial units comprehensively within the risk-oriented approach [31].

3. SOFTWARE AND HARDWARE IMPLEMENTATION

Evaluating the complex technogenic territorial risk is a main function of the information system of territorial risk and safety management (the IS). Its general block diagram is based on Docker containers: in this container (module) management system, each separate module is placed as an independent component (program) on the computing server and has a dedicated access port and a particular set of libraries. Thus, an application or website with all its environment and dependencies is packed into a container, which can be easily managed: transferred to another server, scaled, or updated. The graphical interface of the IS is based on ReactJS + Redux libraries. The system uses a complex crisis database with the PostgreSQL database management system [36].

In this paper, we propose a managerial decision algorithm embedded in the information system of territorial risk and safety management; see Fig. 1 and [1, 31].

The IS receives statistical data characterizing the S-N-T system (territory). It includes two subsystems:

- The information subsystem “Monitoring.” This subsystem collects and systematizes information flows of the monitoring systems with subsequent processing, analysis, and storage of the data.
- The information subsystem “Risk Analysis.” This subsystem has three blocks: the crisis databases of the S-N-T system, a cartographic database of a geographic information system, and a block with basic risk analysis models and computational technologies. This subsystem quantitatively assesses the risk (identification, classification, assessment, and determination of an acceptable level).

After the information passes through these subsystems, the data are processed to calculate the risk values within the methodological approach presented above.

An appropriate conclusion with territory management and planning measures is formed depending on the calculated risk value. If the risk value corresponds to an acceptable level, no additional measures to reduce the risk in the territory are required. If a high risk level is obtained, additional data analysis is carried out to identify the dominant risk factor.

The resulting information is used to generate an intermediate product (a conclusion on necessary measures to minimize the risk value for a particular factor by improving the protection of objects, reducing man-made hazards, and increasing the stability of objects; see Table 1) and control the risk level.

The conclusion is sent to the decision-maker, who analyzes the information received and approves the measures under the available budget. This system yields regulatory documents (orders or decrees) with risk management methods. Note that preventive measures differ depending on the type of dangerous factors (man-made event) and budget constraints; see Table 2.

Territorial units are dynamic systems, and the calculated risk value will change over time. Thus, for effective management, the results should be annually corrected.

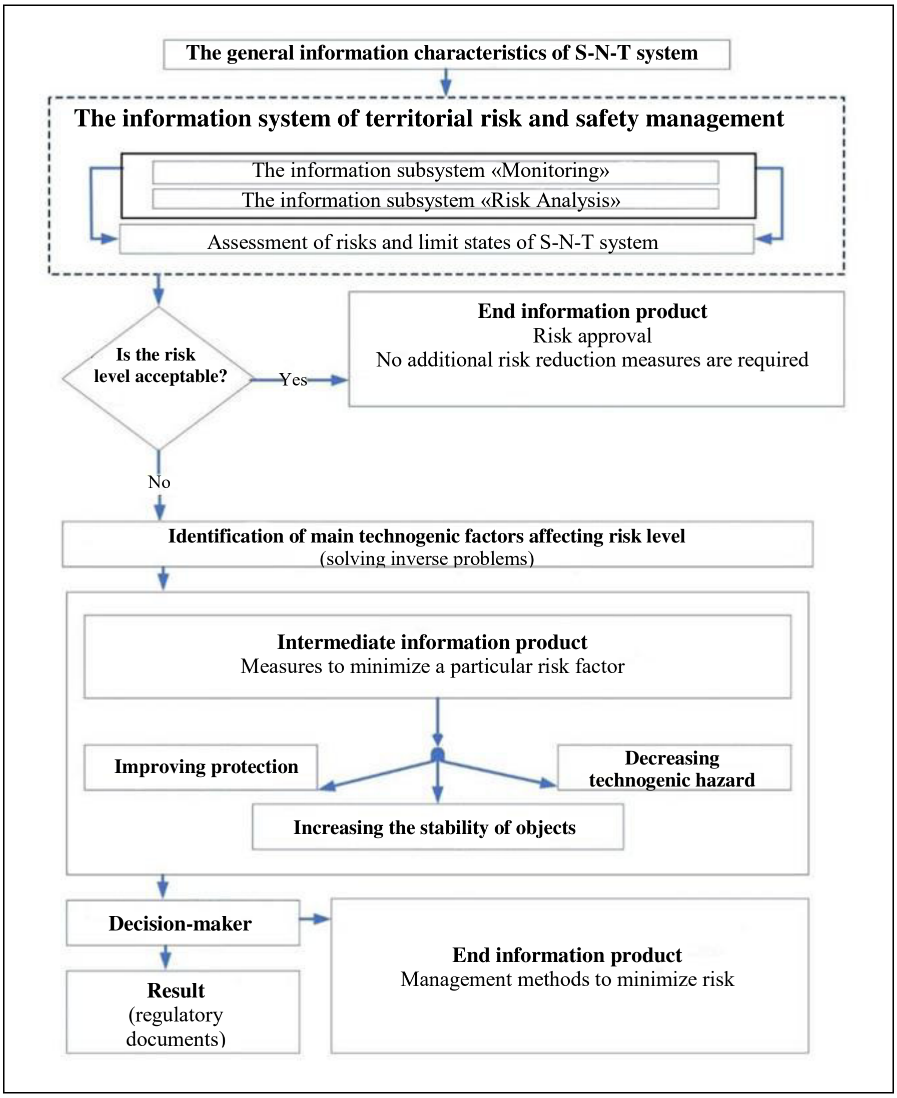
The general information characteristics of S-N-T system
The information system of territorial risk and safety management
The information subsystem «Monitoring»
The information subsystem «Risk Analysis»
Assessment of risks and limit states of S-N-T system
Is the risk level acceptable?
Yes
End information product
Risk approval
No additional risk reduction measures are required
No
Identification of main technogenic factors affecting risk level
(solving inverse problems)
Intermediate information product
Measures to minimize a particular risk factor
Improving protection
Decreasing technogenic hazard
Increasing the stability of objects
Decision-maker
Result (regulatory documents)
End information product
Management methods to minimize risk

Fig. 1. The managerial decision algorithm within the risk-oriented approach.

Table 1

The main types of preventive measures to improve the technogenic safety of a territory

The goals of preventive measures	Technological solutions, preventive measures
Reducing the probability of dangerous events	- Repair and reconstruction of technosphere objects; - Construction of all types of facilities using new technologies with safety requirements; - Continuous monitoring of adverse processes; - Automation of processes (reducing the role of the human factor)
Increasing the stability of objects	- Zoning of territories adjacent to technosphere objects; - Development of healthcare and safety systems; - Engineering solutions to improve the stability of the urban environment; - Development of warning and alarm systems; - Property insurance; - Control, supervision, prevention, and education of residents
Increasing protection	- Creation and upgrading of emergency response units and services; - Creation, replenishment, and replacement of reserves in case of emergency; - Increase in financial reserves; - Improving interagency interaction, working with volunteers

Table 2

Measures to prevent or reduce the consequences of major dangerous man-made events

The type of dangerous event	Preventive measures		
	Reducing the probability of occurrence	Reducing the scale of emergencies	Actions without resource constraints
Accidents at potentially dangerous facilities	Increasing the «sensitivity» of industrial control systems to the identification of accidents and emergencies. Inspections by the Federal Service for Environmental, Technological and Nuclear Supervi- sion (Rostekhnadzor)	Increasing the readiness of the facility units. Improving emergency response plans	Transition to alternative technologies. Reduction (complete rejection) of hazardous substances and materials
Man-made fires	Strengthening of fire supervision. Control of knowledge of fire safety rules	Installation of modern firefighting equipment. Improving the readiness of the emergency response units. Improving emergency response plans	Transition to alternative production and construction technologies
Domestic fires and fires at mass public facilities	Strengthening of fire supervision. Training of the population in fire safety rules	Increasing the number and status of firefighting units. Creating resources for firefighting	Transition to alternative construction technologies. Elimination of stove heating
Accidents of housing and communal services systems	Increasing the volume and quality of capital repairs	Increasing the readiness of units. Improving emergency response plans	Transition to alternative technologies and materials when replacing service lines
Motor vehicle accidents	Legislative regulation of safety issues	Training in first aid. Increasing the readiness of rescue units	Construction and reconstruction of roads in accordance with modern standards (four lanes, interchanges)

4. PRACTICAL RESULTS

The proposed methodology was used to analyze 31 territorial units of the SFD with over 70 thousand residents. As found, in Krasnoyarsk, Novosibirsk, and Omsk, the complex technogenic territorial risk value exceeds the maximum permissible level hundreds of times. Figure 2 shows the distribution of the complex technogenic territorial risk values for each type of dangerous events in these Siberian agglomerations.

The main technogenic load in urban units falls on various fire-explosive events and large motor vehicle accidents. The lowest risk value was obtained for such indicators as «Collapse of structures» and «Other» (aerial, rail, and river vehicle accidents, accidents at industrial facilities, accidents involving the release of hazardous chemical and radiation substances, domestic and man-made fires, and accidents in life support systems).

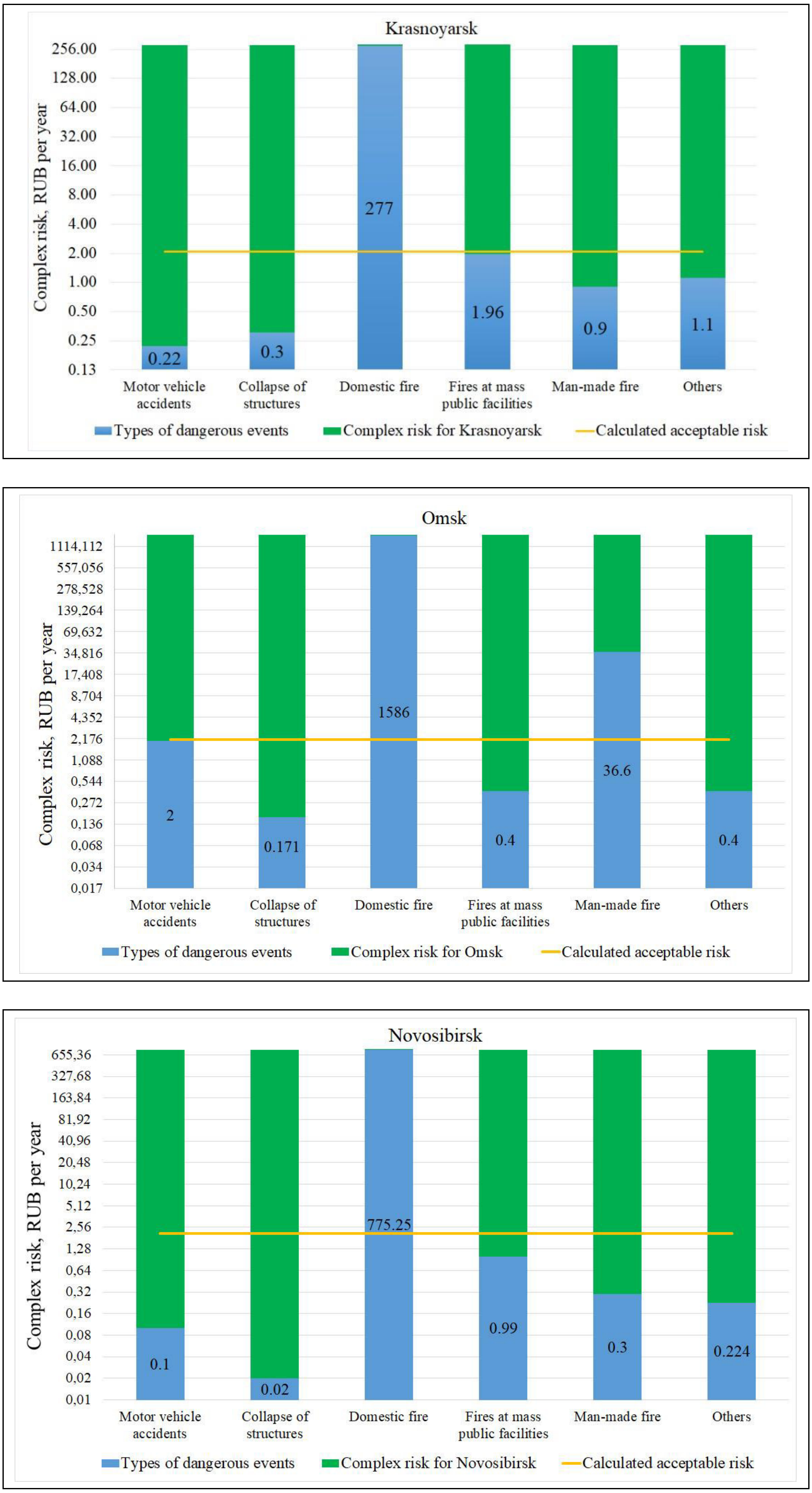

Fig. 2. The distribution of complex technogenic territorial risk values by type of hazards: three industrial agglomerations of Siberia.

For the three agglomerations, the dominant types of dangerous events were determined by solving the inverse problems. For Krasnoyarsk and Novosibirsk, the main hazard is associated with domestic fires and fires at mass public facilities; for Omsk, domestic fires, fires at mass public facilities, and large motor vehicle accidents. The main problem inherent in all these agglomerations, to be minimized and managed, is domestic fires. Figure 3 shows the resulting graphs of the complex territorial technogenic risk when managing two indicators, the amount of damage and the number of fatal outcomes (formulas (4) and (5), respectively).

Reducing the value of one indicator (the number of fatal outcomes or the amount of damage) allows reducing the risk value. Therefore, the main recommendations to minimize the risk should be aimed at (a) improving the culture and overall level of safety (reducing the number of fatal outcomes) and (b) property insurance to compensate for damage in case of a dangerous man-made event. To achieve an acceptable risk level in the territories, the amount of damage or the number of fatal outcomes must be decreased by 8 times for Novosibirsk, 6 times for Krasnoyarsk, and 10 times for Omsk.

To maintain the necessary level of stability to adverse effects, we calculated the protection indicator by formulas (5)–(7) and analyzed the number of rescue units and medical facilities in the three agglomerations; see Table 3.

The lowest protection was revealed for Novosibirsk (a lack of fire and rescue units and medical facilities). Thus, to prevent accidents and disasters and minimize the consequences of the realized events, it is necessary to improve the protection of this territory by increasing the number of emergency rescue units and emergency services and upgrading them.

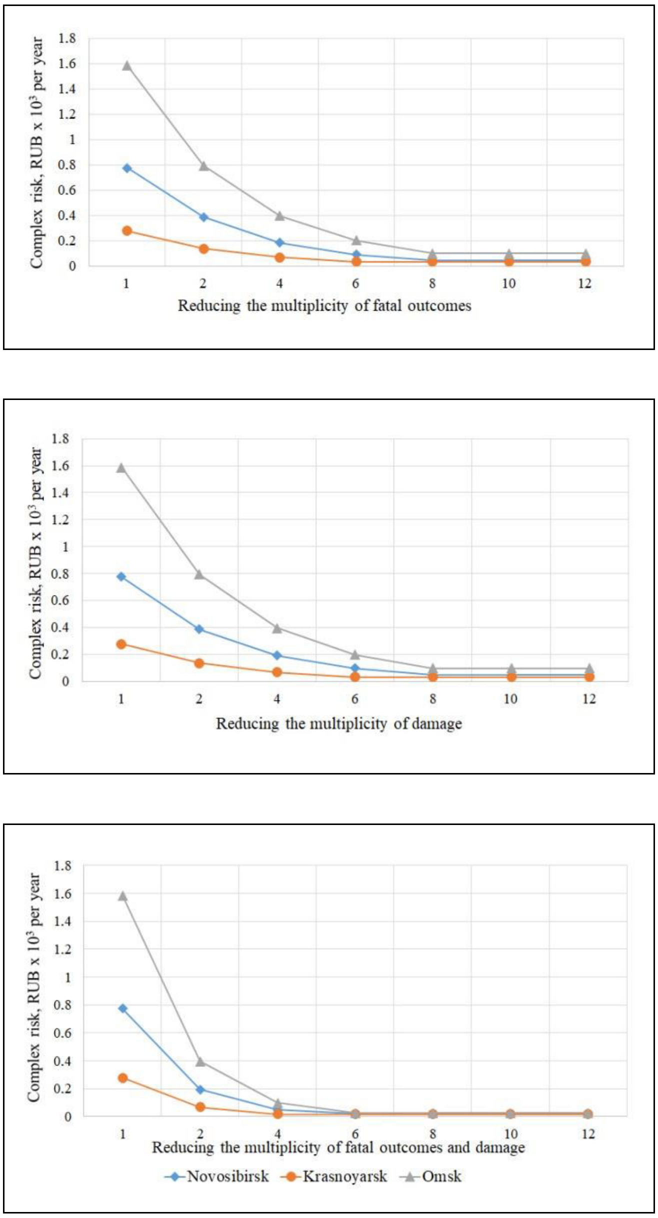

Fig. 3. Complex risk under decreasing multiplicity of fatal outcomes and damage.

Table 3

Values of the protection indicator and related data

Territory	Protection, %	The factual number of fire units	The normative number of fire units	The factual number of medical facilities	The normative number of medical facilities
Novosibirsk	84.5	25	30	68	80
Omsk	135	22	22	85	57
Krasnoyarsk	98.5	10	18	55	48

5. DISCUSSION

The main goal of territorial management is to achieve an acceptable risk level. However, regulatory and technical documents on the assessment of man-made territorial risk have several methodological problems and contradictions in their application due to the different legal statuses and inconsistency of norms. The key problem of the current regulatory and technical documents in the field of safety and risk assessment is that the acceptable risk levels are not scientifically sound. The mathematical framework of risk assessment requires refinement: besides emergencies, it is necessary to analyze all incidents occurring in a given territory that may cause major accidents and disasters in the future. The developed risk assessment methodology based on multidimensional statistical analysis allows reducing the acuteness of these problems and contradictions.

In Russia, the provision of territorial technogenic safety is entrusted to the territorial agencies for civil defense and emergency situations and the territorial departments of the Ministry of the Russian Federation for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters (Emercom). For effective management, it is reasonable to use information decision support systems, which should combine and analyze the monitoring data available to various agencies and assess risks in the main areas of life. Man-made risk management includes the development and implementation of activity programs to prevent dangerous events, reduce their possible consequences, perform monitoring, and improve the economic effectiveness of measures reducing risk values to acceptable levels. The information system of territorial risk and safety management serves to identify the main factors of high man-made risks and specify preventive measures.

Assessment of the efficiency and economic feasibility of managerial decisions to minimize risks is a separate practical task that requires basic information on different costs (the reconstruction of technical facilities, the development of facility monitoring systems, healthcare and safety systems, the creation and upgrading of emergency response and rescue units, etc.). The implementation of such measures is the responsibility of various federal ministries and departments of the Russian Federation, regional authorities, and enterprises.

CONCLUSIONS

In this paper, the complex technogenic territorial risk values have been calculated for three industrial agglomerations of the Siberian Federal District. Based on their analysis, the main causes affecting the risk level have been identified: man-made fires, accidents in the housing and communal service systems (heating networks, power grids, water supply systems, etc.), and motor vehicle accidents. The largest number of fatal outcomes is observed for domestic fires. The highest material damage is caused by man-made fires due to numerous victims and significant economic losses to eliminate the emergencies and their consequences.

Among the advantages of the developed risk assessment methodology, note the possibility of calculating an acceptable risk level, which can be used to elaborate regulatory documents. The current approaches to quantifying acceptable risk levels refer to individual risks, and qualitative indicators (rating points) are often adopted for normalizing the complex risk. In addition, the protection of a given territory is often assessed by qualitative methods. The methodology proposed in this paper yields numerical values of the protection indicator, for the first time in the literature.

The complex safety of territorial units should be assessed by developing and applying risk analysis criteria and methods. With the growing anthropogenic load, the use of technologies threatening the reproduction of natural resources, and numerous threats to the life and health of the population, there is an urgent need for effective territorial management mechanisms with decision support within the information system of territorial risk and safety management based on the comprehensive assessment of man-made territorial risks.

REFERENCES

1. Moskvichev, V.V., Bychkov, I.V., Potapov, V.P., et al. Information System for Territorial Risk and Safety Management Development, *Herald of the Russian Academy of Sciences*, 2017, no. 8, pp. 696–705. (In Russian.)
2. Makhutov, N.A., Kuzyk, B.N., Abrosimov, N.V., et al. *Nauchnye osnovy prognozirovaniya i prognoznye pokazateli sotsial'no-ekonomicheskogo i nauchno-tekhnichnogo razvitiya Rossii do 2030 goda s ispol'zovani kriteriev strategicheskikh riskov* (Scientific Grounds of Forecasting and Forecasted Indicators of Socio-Economic, Scientific, and Technological

Development of Russia until 2030 Using the Criteria of Strategic Risks), Moscow: INES, 2011. (In Russian.)

3. Makhutov, N.A., Kuzyk, B.N., and Abrosimov, N.V., *Sistemnye strategicheskie riski i prioritety proizgnogo sotsial'no-ekonomicheskogo i nauchno-tekhnologicheskogo razvitiya Rossii do 2030 goda* (Systemic Strategic Risks and Priorities of the Forecasted Socio-Economic, Scientific, and Technological Development of Russia until 2030), Moscow: INES, 2012. (In Russian.)
4. Moskvichev, V.V., Taseiko, O.V., Ivanova, U.S., and Chernykh, D.A., Basic Regional Risks of Territorial Development for Siberian Federal District, *Computational Technologies*, 2018, vol. 23, no. 4, pp. 95–109.
5. Moskvichev, V.V., Postnikova, U.S., and Taseiko, O.V., Cluster Analysis and Individual Anthropogenic Risk, *Proceedings of the All-Russian Conference with International Participation* «*Spatial Data Processing for Monitoring of Natural and Anthropogenic Processes*» (*SDM 2021*), *CEUR Workshop Proceedings*, 2021, pp. 526–532.
6. *Upravlenie risk: Risk. Ustoichivoe razvitie. Sinergetika* (Risk Management: Risk. Sustainable Development. Synergetics), Vladimirov, V.A., Vorob'ev, Yu.L., Salov, S.S., et al., Eds. (In Russian.)
7. Kononov, D.A., Safety Study of Control Systems Based on the Analysis of Their System Parameters, Proceedings of the 28th International Conference on *Problems* of *Complex* Systems Security Control, Kalashnikov, A.O. and Kul'ba, V.V., Eds., Moscow, December 16, 2020, Trapeznikov Institute of Control Sciences RAS, 2020, pp. 102–108.
8. Federal Law of the Russian Federation "On Technical Regulation" dated December 27, 2002, no. 184-FZ. http://www.consultant.ru/document/cons_doc_LAW_40241/ (In Russian.)
9. Federal Law of the Russian Federation "On Safety" dated December 28, 2010, no. 390-FZ. http://www.consultant.ru/document/cons_doc_LAW_108546/ (In Russian.)
10. Federal Law of the Russian Federation "On the Protection of the Population and Territories from Natural and Man-Made Emergencies" dated December 21, 1994, no. 68-FZ. http://www.consultant.ru/document/cons_doc_LAW_5295/ (In Russian.)
11. Decree of the President of the Russian Federation "On the National Safety Strategy of the Russian Federation" dated February 7, 2021, No. 400. http://publication.pravo.gov.ru/Document/View/0001202107030001 (In Russian.)
12. Decree of the President of the Russian Federation "On the Strategy for Environmental Safety of the Russian Federation for the Period until 2025" dated April 19, 2017, no. 176. http://www.consultant.ru/document/cons_doc_LAW_215668/ (In Russian.)
13. Bolshakov, B.E. and Shevenina, E.V., Methodological Principles of Defect-free Management of Safety and Development of Territorial and Production Systems, *Naukovedenie*, 2016, vol. 8, no. 2, pp. 1–18. (In Russian.)
14. Ordinance of the Government of the Russian Federation "On Implementing the State Monitoring of the Condition and Pollution of the Environment" dated June 6, 2013, no. 477. http://www.meteorf.ru/upload/iblock/30b/PPRF-477-20130606.pdf (In Russian.)
15. Order of the Federal Agency for Subsoil Use "On Approving the Regulations on the Functional Subsoil Monitoring Subsystem of the Unified State System for the Prevention and Elimination of Emergencies" dated November 24, 2005, No. 1197. http://www.consultant.ru/document/cons_doc_LAW_224058/ (In Russian.)
16. Nemtinov, V.A., Information Technologies for Decision-Making in Maintenance of Ecological Safety of Industrial Enterprises, *Transactions of the TSTU*, 2008, vol. 14, p. 789–795. (In Russian.)
17. Neirotti, R., Current Trends in Smart City Initiatives: Some Stylized Facts, *Cities*, 2014, vol. 38, pp. 25–36.
18. Fraker, N., *The Hidden Potential of Sustainable Neighborhoods: Lessons for Low-Carbon Communities*, Washington, DC: Island Press, 2013.
19. La Greca, P., Barbarossa, L., Ignaccolo, M., et al., The Density Dilemma. A Proposal for Introducing Smart Growth Principles in a Sprawling Settlement within Catania Metropolitan Area, *Cities*, 2011, vol. 28, pp. 527–535.
20. Baranovskiy, V.Yu., Intellectual Information Systems as a Source of Increasing the Rationalization of the Management Procedure of an Industrial Enterprise under Uncertainty, *Eurasian Union of Scientists*, 2021, no. 4-3 (85), pp. 17–20. (In Russian.)
21. Kretova, A.V., Economic Information Systems as a Basis for Improving the Quality of Organization Management, *Menedzher*, 2020, no. 3 (93), pp. 84–90. (In Russian.)
22. Vozhakov, A.V., Stolbov, V.Yu. *Intellektual'nye informatsionnye sistemy upravleniya predpriyatiem: modeli i praktiki* (Intelligent Information Systems of Enterprise Management: Models and Practices), Moscow: Universitetskaya Kniga, 2021. (In Russian.)
23. Kiselev, V.M., Danko, T.P., and Afanasyev, M.A., The Role of Geographic Information Systems in Ensuring Food in Countries During Epidemiological Crises, *Innovation & Investment*, 2020, no. 10, pp. 249–253. (In Russian.)
24. Oliveira da Silva, A. and Souza Fernandes, R.A., Smart Governance Based on Multipurpose Territorial Cadastre and Geographic Information System: An Analysis of Geoinformation, Transparency and Collaborative Participation for Brazilian Capitals, *Land Use Policy*, 2020, vol. 97, p. 104752.
25. Béjar, R., Latre, M.Á., Lopez-Pellicer, F.J., et al., SDI-Based Business Processes: A Territorial Analysis Web Information System in Spain, *Computers & Geosciences*, 2012, vol. 46, pp. 66–72.
26. Lee, B.S., Alexander, M.E., Hawkes, B.C., et al., Information Systems in Support of Wildland Fire Management Decision Making in Canada, *Computers and Electronics in Agriculture*, 2002, vol. 37, pp. 185–198.
27. Green, B. and Chen, Y., The Principles and Limits of Algorithm-in-the-Loop Decision Making, *Proceedings of the ACM on Human-Computer Interaction*, 2019, vol. 3, no. CSCW, pp. 1–24.
28. Alkhatib, A. and Bernstein, M., Street-Level Algorithms: A Theory at the Gaps Between Policy and Decisions, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–13.
29. Makhutov, N.A., *Nauchnye osnovy analiza strategicheskikh prioritetov i riskov razvitiya Rossii: Informatsionno-analiticheskaya spravka po problemam strategicheskogo prognozirovaniya, planirovaniya i programmirovaniya v tselyakh sotsial'no-ekonomicheskogo razvitiya i obespecheniya natsional'noi bezopasnosti* (Scientific Foundations of the Analysis of Strategic Priorities and Risks of Russia's Development: An Information and Analytical Report on the

Problems of Strategic Forecasting, Planning and Programming for Sustainable Socio-economic Development and National Security), Moscow: Znanie, 2018. (In Russian.)

30. Makhutov, N.A., Ursul, A.D., Protsenko, A.N., et al., *Bezopasnost' Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Slovar' terminov i opredelenii* (Security of Russia. Legal, Socio-Economic and Scientific and Technical Aspects. Glossary of Terms and Definitions), Moscow: Znanie, 1999. (In Russian.)
31. Taseiko, O.V., Postnikovaa, U.S., Georgieva, M., et al., Methods for Analyzing Heterogeneous Data in the Tasks of Assessing Territorial Risks, *CEUR Workshop Proceedings*, 2021, vol. 2930, pp. 124–128.
32. The Urban Planning Code of the Russian Federation. Federal Law of the Russian Federation dated May 7, 1998, no. 73-FZ. (In Russian.)
33. Kononov, D.A., Ponomarev, N.O., Ponomarev, R.O., and Barbashev, M.P., Regional Systems: Modeling of Crisis Phenomena and Vulnerability, *Proceedings of the 8th International Conference on Management of Large-Scale System Development* (*MLSD*'2015), Vassilyev, S.N. and Tsvirkun, A.D., Eds. (In Russian.)
34. Organizational and Methodological Recommendations for Determining the Size of the Fire Service of the Subject of the Russian Federation and Its Technical Equipment. https://www.mchs.gov.ru/dokumenty/metodicheskie-materialy/metodicheskie-rekomendacii/prochee/organizacionno-metodicheskie-rekomendacii-po-opredeleniyu-chislennosti-protivopozharnoy-sluzhby-subekta-rossiyskoy-federaciii-i-ee-tehnicheskoy-osnashnosti. (In Russian.)
35. Order of the Ministry of Health of the Russian Federation "On the Requirements for the Placement of Medical Organizations of the State Health System and Municipal Health System Based on the Needs of the Population" dated February 27, 2016, no. 132n. (In Russian.)
36. Popov, S.E., Potapov, V.P., Zamaraev, R.Yu., Information and Computing System "Risks." Certificate of State Registration of the Computer Program No. 2020661041. (In Russian.)

This paper was recommended for publication by V. V. Kul'ba, a member of the Editorial Board.

Received February 29, 2022, and revised July 4, 2022.
Accepted July 11, 2022

Author information

Moskvichev, Vladimir Viktorovich. Dr. Sci. (Eng.), Federal Research Center for Information and Computational Technologies, Krasnoyarsk Branch, Krasnoyarsk, Russia
✉ krasn@ict.nsc.ru

Postnikova, Ulyana Sergeevna. Junior Researcher, Federal Research Center for Information and Computational Technologies, Krasnoyarsk Branch, Krasnoyarsk, Russia
✉ ulyana-ivanova@inbox.ru

Taseiko, Olga Viktorovna. Cand. Sci. (Phys.–Math.), Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia
✉ taseiko@gmail.com

Cite this paper

Moskvichev, V.V., Postnikova, U.S., and Taseiko, O.V. Management of Technogenic Safety Based on a Risk-Oriented Approach. *Control Sciences* **3,** 13–23 (2022). http://doi.org/10.25728/cs.2022.3.2

Original Russian Text © Moskvichev, V.V., Postnikova, U.S., and Taseiko, O.V., 2022, published in *Problemy Upravleniya*, 2022, no. 3, pp. 16–28.

Translated into English by *Alexander Yu. Mazurov*,
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com

DOI: http://doi.org/10.25728/cs.2022.3.3

AN APPROACH TO COMPARE ORGANIZATIONAL MODES OF ACTIVE AGENTS AND CONTROL METHODS

G. A. Ougolnitsky

Southern Federal University, Rostov-on-Don, Russia

✉ gaugolnickiy@sfedu.ru

Abstract. When interacting, active agents can behave independently, cooperate, or be connected by hierarchical relations. In turn, hierarchical impact may be exerted by administrative or economic methods with or without feedback. We systematically describe these organizational modes and control methods based on game-theoretic models with different information structures without considering uncertainty. It seems crucial to compare quantitatively the payoffs of individual agents and the whole set of them (social welfare) under these organizational modes and control methods. We propose a methodology for building the systems of social and private preferences in normal-form games and shares in the allocation of cooperative payoff. A system of relative efficiency indices is developed for detailed quantitative assessment. The proposed methodology is illustrated by several Cournot oligopoly models.

Keywords: inefficiency of equilibria, methods of control and resource allocation, organizational modes for active agents.

INTRODUCTION

At first glance, it seems obvious that cooperation is better than confrontation. Combining the efforts of active agents produces better results than their independent selfish behavior, much less hostility, and the additional coalition payoff can be allocated among all agents.

Unfortunately, the things are not so simple. For the society, the cooperative payoff is always at least not smaller than under the independent behavior of the active agents composing the society or hierarchical relations between them. But this is not true for each agent. For example, the payoff of an upper-level agent in the hierarchy can exceed its share in the uniform allocation under cooperation, even considering the additional effect. Also, it is not so easy to negotiate a division of the additional payoff, even if there is an agreement to cooperate in principle, and ensure the agreement's stability. Perhaps due to these considerations, there are many examples of abandoning cooperation in favor of conflict and competition for leadership in economics, public life, international relations, and other areas.

Therefore, a topical problem is to analyze in mathematical terms the conditions of profitable cooperation and compare the efficiency of different organizational modes of active agents, control methods, and allocation of the cooperative payoff. The fundamental foundations of such mathematical analysis are provided by the theory of active systems and control in organizations [1, 2], the information theory of hierarchical systems [3–7], and the theory of incentives and mechanism design [8]. The concept of sustainable management of active systems based on considering and coordinating the interests of active agents was proposed in [9, 10]. Game theory [11–15] is the main mathematical tool of the analysis. Complex dynamic problems of conflict control are solved using simulation modeling [16].

The problem of inefficiency of equilibria was analyzed in detail in [17–20]. The outcome of the rational behavior of independent selfish economic agents is usually worse for the society than that of centralized management or voluntary cooperation. An important question arises: how much worse is it? The price of anarchy is a common measure of the inefficiency of equilibria, defined as the ratio of the social payoff function value in the worst-case equilibrium to its value in the optimal outcome [21]. A wider set of indicators for dynamic games was proposed in [22]. The payoffs under different organizational modes of agents were compared in many papers on a game theory; for example, see [23–25].

However, the (in)efficiency of equilibria should be given a more general problem statement. First of all, the payoffs are to be compared in the basic organizational modes of active economic agents (equality, hierarchy, and cooperation) under different control methods specifying the rules of their interaction. In addition, and more importantly, the comparison should be made in terms of social welfare and the interests of individual agents. As mentioned, a game outcome beneficial for the society under some organizational mode may not be such for each agent.

Equality, hierarchy, and cooperation are the basic organizational models of interaction between active agents. Under equality, the agents (players) choose their actions simultaneously and independently, and Nash equilibrium is the solution of the arising normal-form game. In a hierarchical organization, two main control modes are possible. In the first one, the Leader chooses an intended action and informs one or several players of his choice; then the other players optimally respond to this action. As a result, the Germeier game Γ_1 arises, and Stackelberg equilibrium is considered its solution. (In English-language literature, it is also known as the Stackelberg game.) In the second control mode, the Leader chooses his strategy as a function of the expected actions of the Followers and informs them of his choice; then the Followers optimally respond to this strategy. As a result, the Germeier game Γ_2 arises, also called the inverse Stackelberg game in English-language literature. Its solution is calculated using Germeier's principle of guaranteed result [4]. It is also reasonable to distinguish between administrative (compulsion) and economic (impulsion) control methods. Compulsion is affecting the sets of admissible strategies of agents, whereas impulsion is affecting the payoff functions of agents [9, 10]. Another formalization of hierarchical relations is the extensive form games where the players act sequentially. Such games are not considered below. Finally, in cooperation, all players join together and maximize the total payoff function over all control variables. This interpretation corresponds to the utilitarian approach, as opposed to the egalitarian approach when the agents maximize the smallest payoff [26]. As a result, the original game is reduced to an optimization problem, in which the cooperative solution is Pareto-optimal. In this sense, the dynamic statements of conflict control problems (differential or difference games) do not fundamentally differ from the static ones [11–15].

Besides the payoff functions, which characterize the efficiency of agents' actions, game-theoretic models may contain additional constraints: coordination conditions [7] or sustainable development conditions [9, 10]. These conditions mean that the state of the controlled dynamic system should belong to some domain in the state space. In static models, these conditions are formulated as control constraints.

The contributions of this paper are as follows:

- We systematically describe the interaction modes of active agents and their control methods using game-theoretic models without uncertainty.
- We propose a comparative analysis methodology for the social and private efficiency of the control methods based on the agents' payoffs in normal-form games and their shares in the allocation of cooperative payoff in characteristic function games.
- We develop a system of relative efficiency indices for detailed quantitative assessment.
- We illustrate the proposed methodology by static and dynamic Cournot oligopoly models.

Section 1 describes a game-theoretic formalization of organizational modes for the interaction of active agents and their control methods. Comparing the agents' payoffs, we build the systems of social and private preferences. Note that comparative efficiency indices can be used for detailed quantitative characterization. Section 2 considers the comparative efficiency methodology based on game-theoretical models of conflict control. In Section 3, this methodology is illustrated by several Cournot oligopoly models. The results of this paper and further research are discussed in the Conclusions.

1. ORGANIZATIONAL MODES, CONTROL METHODS, AND SYSTEMS OF PREFERENCES

1.1. Organizational Modes and Control Methods

As noted, equality, hierarchy, and cooperation are the main organizational models of interaction between active agents. In a hierarchical organization, two main control methods are possible: compulsion (administrative mechanisms) and impulsion (economic mechanisms). These control mechanisms can be implemented with or without feedback.

Two questions arise during cooperation. First, how should the payoff of each coalition be defined? (How should the characteristic function be constructed?) Second, how should the total payoff be allocated among the players? (Which optimality principle should be chosen?) It is also natural to treat payoff allocation as a control problem.

Section 1 describes the interaction modes and control methods within static game-theoretic models.

The interaction of equal agents is modeled by a normal-form game of *n* players:

$$u_i(x_1,...,x_n) \to \max, x_i \in X_i, i \in N. \qquad (1.1)$$

Here $N = \{1,..., n\}$ denotes the set of players (active agents); X_i is the set of admissible actions of player *i*; x_i is a particular action chosen by player *i*; finally, $u_i : X \to R$ is the payoff function of player *i*. Players from the set N simultaneously and independently choose their actions x_i, resulting in a game outcome $x = (x_1,...,x_n) \in X = X_1 \times ... \times X_n$. Players can be of different nature. In economics, they are individual entrepreneurs, households, firms, regions, or countries. In politics, they are individual voters, political parties, movements and associations, and executive and legislative bodies. In organizational management, they are individual employees, departments and structural units, and entire organizations. What is important, the interests of each player are completely described by maximization of the payoff u_i (the postulate of economic rationality).

The solution of the game (1.1) is the set of Nash equilibria:

$$\mathrm{NE} = \{x^{\mathrm{NE}} \in X : \forall i \in N$$
$$\forall x_i \in X_i\ u_i(x^{\mathrm{NE}}) \ge u_i(x_i, x_{-i}^{\mathrm{NE}})\},$$
$$x_{-i} = (x_1,...,x_{i-1},x_{i+1},...,x_n). \qquad (1.2)$$

In cooperation, players unite to maximize the total payoff (the utilitarian social welfare function) [26]

$$u(x) = \sum_{i \in N} u_i(x). \qquad (1.3)$$

The cooperative solution is given by

$$x^C \in X : u^C = u(x^C) = \max_{x \in X} u(x). \qquad (1.4)$$

Under hierarchical control, a dedicated player with subscript 0 (the Principal in the theory of active systems) is added to the set N. In the case of no feedback, the Principal chooses its action $x_0 \in X_0$ and informs the other players of it. Knowing the action x_0, the players choose their optimal responses. Anticipating this behavior, the Principal chooses the action $x_0 \in X_0$ to maximize its payoff on the set of optimal responses. Two cases are possible here.

- If the Principal expects the benevolence of the other agents, its payoff is given by

$$u_0^B = \sup_{x_0 \in X_0} \sup_{x \in R(x_0)} u_0(x_0, x), \qquad (1.5)$$

where $R(x_0)$ denotes the set of agents' optimal responses to the Principal's action x_0. How is this set determined for interconnected agents? The question has no obvious answer. According to a standard assumption, $R(x_0) = \mathrm{NE}(x_0)$ provided that $\forall x_0\ \mathrm{NE}(x_0) \ne \varnothing$; otherwise, the set $R(x_0)$ should be defined separately for a particular model. The well-known monograph [13] gave the following definition of Stackelberg equilibrium for finite three-player games. (It can be easily generalized to the case $n > 3$.)

Consider a three-player game with one Leader (the first player) and two Followers (the second and third players). For player $i = 1, 2, 3,$ we introduce the following notations: x_i and X_i are the strategy and the set of all admissible strategies of player *i*, respectively; $J_i(x_1, x_2, x_3)$ is the payoff of player *i* in the outcome $(x_1, x_2, x_3).$ Then x_1^* is a hierarchical equilibrium strategy of the Leader if

$$\min_{(x_2, x_3) \in R(x_1^*)} J_1(x_1^*, x_2, x_3) = \max_{x_1 \in X_1} \min_{(x_2, x_3) \in R(x_1)} J_1(x_1, x_2, x_3),$$

where $R(x_1)$ is the set of optimal responses of the Followers. For each strategy $x_1 \in X_1$ of the Leader, this set is given by

$$R(x_1) = \{(y_2, y_3) \in X_2 \times X_3 \colon J_2(x_1, y_2, y_3) \ge$$
$$J_2(x_1, x_2, x_3) \wedge J_3(x_1, y_2, y_3) \ge J_3(x_1, x_2, x_3),$$
$$\forall x_2 \in X_2, x_3 \in X_3\}.$$

Any triplet $(x_1^*, x_2^*, x_3^*), (x_2^*, x_3^*) \in R(x_1^*)$, is a Stackelberg equilibrium [13, pp. 145 and 146].

- Otherwise (under the conscious or involuntary malevolence of the agents), the Principal's payoff is given by

$$u_0^{\mathrm{NB}} = \sup_{x_0 \in X_0} \inf_{x \in R(x_0)} u_0(x_0, x). \qquad (1.6)$$

Let ST denote the set of all Stackelberg equilibria (solutions of the hierarchical game between the Principal and the agents).

Remark 1. Many researchers suppose that Stackelberg equilibrium is defined by formula (1.5) only, referring formula (1.6) to Germeier's principle of guaranteed result. This is not true: in the widely known monograph [13], Stackelberg equilibrium was defined by formula (1.6).

Remark 2. In many applied models, there exists a unique optimal response of agents (e.g., a Nash equilibrium). In this case, the problem of agent's benevolence or malevolence does not arise.

In hierarchical control with feedback, the Principal chooses its strategy $\tilde{x}_0 \in \tilde{X}_0 = X_0{}^X$, i.e., $\tilde{x} : X \to X_0$, and informs the other players of it. Then the game has an information structure similar to the previous case with a natural modification. Knowing the strategy $\tilde{x}_0$, the players choose the optimal response. Anticipating this behavior, the Principal chooses the strategy $\tilde{x}_0 \in \tilde{X}_0$ to maximize its payoff on the set of optimal responses. If the Principal expects the benevolence of the agents, its payoff is given by

$$\tilde{u}_0^B = \sup_{\tilde{x}_0 \in \tilde{X}_0} \sup_{x \in R(\tilde{x}_0)} u_0(\tilde{x}_0(x), x) . \qquad (1.7)$$

Otherwise (under the conscious or involuntary malevolence of the agents), the Principal's payoff is given by

$$\tilde{u}_0^{\rm NB} = \sup_{\tilde{x}_0 \in \tilde{X}_0} \inf_{x \in R(\tilde{x}_0)} u_0(\tilde{x}_0(x), x) . \qquad (1.8)$$

Let IST denote the set of solutions of the hierarchical game between the Principal and the agents under control with feedback.

Hierarchical control involves administrative methods (compulsion) or economic methods (impulsion) [9, 10]. We formalize these concepts in the case of control without feedback for unfavorable agents. The hierarchical game has the form

$$u_0(p, q, x) \to \max, \ p \in P, \ q \in Q; \qquad (1.9)$$

$$u_i(p_i, x) \to \max, x_i \in X_i(q_i), i \in N . \qquad (1.10)$$

Here $p = (p_1, ..., p_n)$ is the vector of the Principal's economic controls applied to the agents' payoff functions; $q = (q_1, ..., q_n)$ is the vector of the Principal's administrative controls applied to the sets of agents' admissible actions.

The set of compulsion equilibria in the game (1.9), (1.10) is the set of outcomes $\text{COMP} = \{(x_0^{\rm COMP}, x^{\rm COMP}) \colon u_0(x_0^{\rm COMP}, x^{\rm COMP}) = u_0^{\rm COMP}\}$, where

$$u_0^{\rm COMP} = \sup_{q \in Q} \inf_{x \in R(q)} u_0(q, x) \qquad (1.11)$$

with a fixed value p.

The set of impulsion equilibria in the game (1.9), (1.10) is the set of outcomes $\text{IMP} = \{(x_0^{\rm IMP}, x^{\rm IMP}) \colon u_0(x_0^{\rm IMP}, x^{\rm IMP}) = u_0^{\rm IMP}\}$, where

$$u_0^{\rm IMP} = \sup_{p \in P} \inf_{x \in R(p)} u_0(p, x) \qquad (1.12)$$

with a fixed value q. The case of control with feedback is formalized by analogy.

Remark 3. Other information structures are known, e.g., the Germeier game Γ_3 [7]. Therefore, the proposed classification does not claim to be exhaustive: it covers the main organizational modes of active agents.

Games in characteristic function form (cooperative games) [11, 12] are a reasonable framework to describe the allocation of the cooperative payoff (1.4). A characteristic function is a mapping $v : 2^N \to R$, and its value $v(K)$ gives the payoff of a coalition $K \subseteq N$. The most common example is the von Neumann–Morgenstern characteristic function [27]:

$$v^{\rm NM}(K) = \text{val}(K, N \setminus K) = \sup_{x_i, i \in K} \inf_{x_j, j \in N \setminus K} \sum_{i \in K} u_i(x_1, ..., x_n). \qquad (1.13)$$

Also, the Petrosyan–Zaccour [28]

$$v^{\rm PZ}(K) = \sup_{x_i, i \in K} \sum_{i \in K} u_i(x_K, x_{N \setminus K}^{\rm NE}) \qquad (1.14)$$

and the Gromova–Petrosyan [29]

$$v^{\rm PG}(K) = \inf_{x_j, j \in N \setminus K} \sum_{i \in K} u_i(x_K^C, x_{N \setminus K}) \qquad (1.15)$$

characteristic functions were proposed with the following notations: x_K is the set of strategies of all players from a coalition *K*, and $x_{N\setminus K}$ is the set of strategies of all players from the anti-coalition *N\K*. (The superscripts NE and *C* indicate Nash equilibrium and the cooperative solution, respectively.) Note that for all characteristic functions (1.13)–(1.15),

$$v^{\rm NM}(N) = v^{\rm PZ}(N) = v^{\rm PG}(N) = \sup_{x_1, ..., x_n} \sum_{i \in N} u_i(x_1, ..., x_n) = u^C .$$

In other words, the payoff of the maximal coalition always coincides with the cooperative payoff (1.4). The Shapley value [30] is a convenient solution of cooperative games: it always exists and is unique. The components of the Shapley value are given by

$$\Phi_i(v) = \sum_{i \in K} \gamma_n(k)[v(K) - v(K \setminus \{i\})], \ i \in N,$$

$$\gamma_n(k) = \frac{(n-k)!(k-1)!}{n!}, \ k =| K |, n =| N | . \qquad (1.16)$$

The player's share in the cooperative payoff allocation based on the Shapley value shows his contribution to all his coalitions considering their power.

1.2. Systems of Preferences and Relative Efficiency Indices

The efficiency of different organizational modes of active agents, control methods, and cooperative payoff allocation should be compared from two points of view: the society and individual agents. For the system of social preferences, indicators are the total payoffs (1.3). For the sake of convenience, assume that $N = \{0, 1, ..., n\}$, and player 0 does not differ from other players in the cases of equality and cooperation.

The social payoffs are as follows:

– under equality,

$$u^{\rm NE} = \min_{x \in \rm NE} u(x) ; \qquad (1.17)$$

– under cooperation,

$$u^C = \max_{x \in X} u(x) ; \qquad (1.18)$$

– under hierarchical control without feedback,

$$u^{\mathrm{ST}} = \sum_{i \in N} u_i(x^{\mathrm{ST}}) ; \tag{1.19}$$

– under hierarchical control with feedback,

$$u^{\mathrm{IST}} = \sum_{i \in N} u_i(x^{\mathrm{IST}}) . \tag{1.20}$$

Formula (1.5) or (1.6) can be used to calculate the social payoff (1.19) and formula (1.7) or (1.8) to calculate the payoff (1.20), depending on the agent’s benevolence (malevolence) assumption. Also, we can take the set COMP (1.11), the set IMP (1.12), or their analogs (1.7), (1.8) under control with feedback instead of IST as the solution of the hierarchical game instead of ST. As a result, we obtain the social payoffs u^{COMP}, u^{IMP}, u^{ICOMP}, and u^{IIMP}, respectively.

According to definition (1.4), the social payoff *under cooperation is always not smaller than under any* other organizational mode or control method. To assess the losses (the inefficiency of equilibria), we introduce the social efficiency indices

$$K^{\mathrm{NE}} = \frac{u^{\mathrm{NE}}}{u^C}, K^{\mathrm{ST}} = \frac{u^{\mathrm{ST}}}{u^C}, K^{\mathrm{IST}} = \frac{u^{\mathrm{IST}}}{u^C} , \ K^{\mathrm{COMP}} = \frac{u^{\mathrm{COMP}}}{u^C} ,$$

$$K^{\mathrm{IMP}} = \frac{u^{\mathrm{IMP}}}{u^C} , \ K^{\mathrm{ICOMP}} = \frac{u^{\mathrm{ICOMP}}}{u^C} ,$$

$$K^{\mathrm{IIMP}} = \frac{u^{\mathrm{IIMP}}}{u^C} . \tag{1.21}$$

Remark 4. The indices (1.21) assume that all payoffs are positive; in this case, all these fractions do not exceed 1. This standard assumption in the theory of (in)efficiency of equilibria [17, *p. 444*] restricts the universality of the proposed approach. In fact, the initial values of the payoffs can be used for comparative efficiency analysis. The indices (1.21) serve for additional quantitative characterization when necessary.

For the system of individual preferences of agents $i \in N$, we select the following indicators:

- under equality,

$$u_i^{\mathrm{NE}} = \min_{x \in \mathrm{NE}} u_i(x) \tag{1.22}$$

(the player’s payoff in the worst-case Nash equilibrium, the principle of optimality for this organizational mode);

- under cooperation,

$$u_i^C = \frac{u^C}{|N|} , \tag{1.23}$$

or the Shapley value $\Phi_i(v)$ for the characteristic function (1.13), (1.14), or (1.15);

- under hierarchical control without feedback, u_i^{ST} ;
- under hierarchical control with feedback, $u_{\mathrm{i}}^{\mathrm{IST}}$.

The sets ST and IST can be replaced by their analogs COMP and ICOMP (compulsion) IMP and IIMP (impulsion). For a detailed quantitative comparative assessment, we propose the individual efficiency indices

$$K_i^{\mathrm{NE}} = \frac{u_i^{\mathrm{NE}}}{u_i^C} , \ K_i^{\mathrm{ST}} = \frac{u_i^{\mathrm{ST}}}{u_i^C} , \ K_i^{\mathrm{IST}} = \frac{u_i^{\mathrm{IST}}}{u_i^C} ,$$

$$K_i^{\mathrm{NM}} = \frac{\Phi_i^{\mathrm{NM}}}{u_i^C} , \ K_i^{\mathrm{PZ}} = \frac{\Phi_i^{\mathrm{PZ}}}{u_i^C} \ \ K_i^{\mathrm{PG}} = \frac{\Phi_i^{\mathrm{PG}}}{u_i^C} ,$$

$$K_i^{\mathrm{COMP}} = \frac{u_i^{\mathrm{COMP}}}{u_i^C} , \ K_i^{\mathrm{IMP}} = \frac{u_i^{\mathrm{IMP}}}{u_i^C} , \ K_i^{\mathrm{ICOMP}} = \frac{u_i^{\mathrm{ICOMP}}}{u_i^C} ,$$

$$K_i^{\mathrm{IIMP}} = \frac{u_i^{\mathrm{IIMP}}}{u_i^C} , \ i \in N . \tag{1.24}$$

The social and individual efficiency indicators and the corresponding indices are combined in Table 1.

Table 1

Social and individual efficiency: indicators and indices

	Equality	Cooperation	Hierarchical control without feedback	Hierarchical control with feedback
Social efficiency indicators	u^{NE}	$u^C = v(N)$	u^{ST}, u^{COMP}, u^{IMP}	u^{IST}, u^{ICOMP}, u^{IIMP}
Individual efficiency indicators, $i \in N$	u_i^{NE}	u_i^C, Φ_i^{NM}, Φ_i^{PZ}, Φ_i^{PG}	u_i^{ST}, u_i^{COMP}, u_i^{IMP}	u_i^{IST}, u_i^{ICOMP}, u_i^{IIMP}
Social efficiency indices	$K^{\mathrm{NE}} = \frac{u^{\mathrm{NE}}}{u^C}$	–	$K^{\mathrm{ST}} = \frac{u^{\mathrm{ST}}}{u^C}$	$K^{\mathrm{IST}} = \frac{u^{\mathrm{IST}}}{u^C}$
Individual efficiency indices, $i \in N$	$K_i^{\mathrm{NE}} = \frac{u_i^{\mathrm{NE}}}{u_i^C}$	$K_i^{\mathrm{NM}} = \frac{\Phi_i^{\mathrm{NM}}}{u_i^C}$, $K_i^{\mathrm{PZ}} = \frac{\Phi_i^{\mathrm{PZ}}}{u_i^C}$, $K_i^{\mathrm{PG}} = \frac{\Phi_i^{\mathrm{PG}}}{u_i^C}$	$K_i^{\mathrm{ST}} = \frac{u_i^{\mathrm{ST}}}{u_i^C}$, $K_i^{\mathrm{COMP}} = \frac{u_i^{\mathrm{COMP}}}{u_i^C}$, $K_i^{\mathrm{IMP}} = \frac{u_i^{\mathrm{IMP}}}{u_i^C}$	$K_i^{\mathrm{IST}} = \frac{u_i^{\mathrm{IST}}}{u_i^C}$, $K_i^{\mathrm{ICOMP}} = \frac{u_i^{\mathrm{ICOMP}}}{u_i^C}$, $K_i^{\mathrm{IIMP}} = \frac{u_i^{\mathrm{IIMP}}}{u_i^C}$

The conditions of coordination (sustainable development) have the form

$$u \in U^*, \qquad (1.25)$$

where U^* is a given set. These conditions can supplement any model considered.

2. AN APPROACH TO COMPARE EFFICIENCY

A comparative analysis of the efficiency of organizational modes of active agents, control methods, and allocation of the cooperative payoff includes the following steps.

1. The set of active agents (players) $N = \{0, 1,..., n\}$ is introduced.

2. Under equality, agent 0 does not differ from the others. The normal-form game (1.1) is constructed, and the set of Nash equilibria (1.2) is found. Finally, the indicators (1.17) and (1.22) are calculated.

3. Under cooperation, agent 0 does not differ from the others as well. The optimization problem (1.4) is solved, and the indicators (1.18) and (1.23) are calculated.

4. Under hierarchical control, agent 0 acts as the Principal. (Any of the initially equal players can claim this role.) For the information structure with control without feedback, the payoffs (1.5) and (1.6) are calculated, and the corresponding sets ST are found. Finally, the indicators (1.19) and u_i^{ST} are calculated.

5. For the information structure with control without feedback, the payoffs (1.7) and (1.8) are calculated, and the corresponding sets IST are found. Finally, the indicators (1.20) and u_i^{IST} are calculated.

6. For the compulsion mode in the hierarchical game (1.9), (1.10), the set COMP (1.11) is found. Then the analogs of the indicators (1.19) and u_i^{ST} are calculated.

7. For the impulsion mode in the hierarchical game (1.9), (1.10), the set IMP (1.12) is found. Then the analogs of the indicators (1.20) and u_i^{IST} are calculated.

8. The games in characteristic function form (1.13)–(1.15) are constructed based on the normal-form game (1.1). Then the Shapley value (1.16) is calculated for these games.

9. The games in characteristic function form (1.13)–(1.15) are constructed based on the hierarchical game without or with feedback. In this case, three types of coalitions are possible: the agents only; the Principal only; the Principal and at least one agent (including the maximal coalition). Finally, the Shapley value (1.16) is calculated for the constructed cooperative games.

10. The additional constraints (1.25) are considered.

11. The system of social preferences is built by ordering the indicators (1.17), (1.19), and (1.20) and the values $u^{\mathrm{COMP}}, u^{\mathrm{IMP}}, u^{\mathrm{ICOMP}}$, and u^{IIMP}. In addition, the losses due to the inefficiency of equilibria are assessed using the indices (1.21).

12. The system of private preferences is built by ordering the indicators (1.22) and (1.23). The comparative efficiency is assessed using the indices (1.24).

Remark 5. In most cases, game-theoretic problems of conflict control can be solved only numerically. Then, the comparison involves the average values of all indicators over the set of computational experiments for different input datasets.

Remark 6. Some steps may be omitted depending on the problem statement and research capabilities.

3. COURNOT OLIGOPOLY MODELS

As an illustrative example, we compare the efficiency of several Cournot oligopoly models.

Example 1. The Cournot oligopoly with symmetric agents.

Let $N = \{1,..., n\}$ be the set of equal symmetric agents (firms). For fixed costs including tax, the model has the form

$$u_i(x) = (1-p)[(D-\bar{x})x_i - cx_i] \to \max,$$
$$0 \le x_i \le 1/n,\ i \in N.$$

Here x_i denotes the production output of firm i; D is the demand volume; c is the specific costs of each firm; the parameter $p \in [0, 1]$ specifies a fixed tax rate; finally, $\bar{x} = x_1 + ... + x_n$. For the sake of definiteness, assume that $D = 1,\ c = 1/n$. (In the paper [31], this parametrization was used for $n = 2$.) Then

$$u_i(x) = (1-p)\left(\frac{n-1}{n} - \bar{x}\right)x_i \to \max, \qquad (3.1)$$
$$0 \le x_i \le 1/n,\ i \in N.$$

In addition, we denote $\bar{u}(x) = u_1(x) + ... + u_n(x)$. The first-order optimality conditions yield

$$\frac{\partial u_i}{\partial x_i} = 0 = \frac{n-1}{n} - 2x_i - \sum_{j \ne i} x_j,\ i \in N;$$

$$2x_i + \sum_{j \ne i} x_j = \frac{n-1}{n},\ i \in N.$$

Hence, in the Nash equilibrium,

$$x_i^{\mathrm{NE}} = x^{NE} = \frac{n-1}{n(n+1)};\ \bar{x}^{\mathrm{NE}} = \frac{n-1}{n+1};$$
$$u_i^{\mathrm{NE}} = u^{\mathrm{NE}} = \frac{(1-p)(n-1)^2}{n^2(n+1)^2};\ \bar{u}^{\mathrm{NE}} = \frac{(1-p)(n-1)^2}{n(n+1)^2}. \qquad (3.2)$$

Now let the agents from the set N cooperate. The model takes the form

$$\overline{u}(x) = (1-p)\left(\frac{n-1}{n} - \overline{x}\right)\overline{x} \to \max,$$

$$0 \le x_i \le 1/n,\ i \in N.$$

Obviously, in this case, $\forall i \in N\ x_i = x$ and

$$\overline{u}(x) = (1-p)\left(\frac{n-1}{n} - nx\right)nx\,.$$

The first-order optimality condition reduces to

$$\frac{\partial \overline{u}}{\partial x} = 0 = n-1-2nx\,.$$

Hence, the solution of the cooperative optimization problem and the corresponding payoffs are:

$$x_i^C = x^C = \frac{n-1}{2n^2};\ \overline{x}^C = \frac{n-1}{2n};$$

$$u_i^C = u^C = \frac{(1-p)(n-1)^2}{4n^3};\ \overline{u}^C = \frac{(1-p)(n-1)^2}{4n^2}.$$

Suppose that agent 1 becomes the Principal: first chooses x_1 and informs the other agents of it. Then, each agent solves the problem

$$u_i = (1-p)\left(\frac{n-1}{n} - x_1 - \sum_{j=2}^{n} x_j\right)x_i \to \max,$$

$$0 \le x_i \le 1/n,\ i = 2,\ldots, n.$$

The first-order optimality conditions

$$\frac{\partial u_i}{\partial x_i} = 0 = \frac{n-1}{n} - x_1 - 2x_i - \sum_{j=2,\, j\ne i}^{n} x_j\ ,\ i = 2,\ldots, n\ ,$$

yield the best response of each agent:

$$x_i^{\mathrm{BR}} = x^{\mathrm{BR}} = \frac{n-1-nx_1}{n^2},\ i = 2,\ldots,n\,.$$

The Principal's problem takes the form

$$u_1(x_1) = (1-p)\left(\frac{n-1}{n} - x_1 - \frac{(n-1)(n-1-nx_1)}{n^2}\right)x_1 =$$

$$\frac{1-p}{n^2}(n-1-nx_1)x_1 \to \max,\ 0 \le x_1 \le 1/n.$$

The first-order optimality conditions

$$\frac{\partial u_1}{\partial x_1} = 0 = n-1-2nx_1$$

lead to the Stackelberg equilibrium

$$x_1^{\mathrm{ST}} = \frac{n-1}{2n};\ x_i^{\mathrm{ST}} = \frac{n-1}{2n^2},\ i = 2,\ldots, n,$$

the total output $\overline{x}^{\mathrm{ST}} = \dfrac{(n-1)(2n-1)}{2n^2}$ and the payoffs

$$u_1^{\mathrm{ST}} = \frac{(1-p)(n-1)^2}{4n^3};$$

$$u_i^{\mathrm{ST}} = \frac{(1-p)(n-1)^2}{4n^4},i = 2,\ldots,n\,;$$

$$\overline{u}^{\mathrm{ST}} = \frac{(1-p)(n-1)(n^2-n+1)}{4n^4}.$$

Now consider the following case: the Principal is an additional non-production agent 0 that assigns the tax rate p. Then the Principal's problem can be written as

$$u_0 = \left(\frac{n-1}{n} - \overline{x}\right)\overline{x}p - ap^2 \to \max,\ 0 \le p \le 1\,, \qquad (3.3)$$

where $a > 0$ is the coefficient of tax collection costs.

The optimal response of the agents is the Nash equilibrium in their game; see formula (3.2). The Principal's problem takes the form

$$u_0 = \frac{(n-1)^2}{n(n+1)^2}p - ap^2 \to \max,\ 0 \le p \le 1\,. \qquad (3.4)$$

As a result, $p^{\mathrm{ST}} = \dfrac{(n-1)^2}{2an(n+1)^2}$, and the Stackelberg (impulsion) equilibrium is

$$\mathrm{ST{=}IMP} = \left(\frac{(n-1)^2}{2an(n+1)^2}, \frac{n-1}{n(n+1)},\ldots, \frac{n-1}{n(n+1)}\right).$$

The payoffs of the Principal and agents are given by

$$u_0^{\mathrm{IMP}} = \frac{(n-1)^2[(n-1)^2 - an(n+1)^2]}{2an^2(n+1)^2};$$

$$u_i^{\mathrm{IMP}} = \frac{(n-1)^2[2an(n+1)^2 - (n-1)^2]}{2an^2(n+1)^4},\ i = 1,\ldots, n\,;$$

$$\overline{u}^{\mathrm{IMP}} = \frac{(n-1)^2[2an(n+1)^2 - (n-1)^2]}{2an(n+1)^4}.$$

Next, we impose an environmental constraint of the form

$$d\overline{x} \le P_{\max}\,, \qquad (3.5)$$

where the coefficient d characterizes the ratio of the volume of pollutant emissions to the total output, and $P_{\max}$ is the maximum permissible limit of emissions. This constraint expresses a sustainable development condition to be ensured by the Principal (an additional constraint in the optimization problem (3.4)). In the Nash equilibrium, this condition reduces to

$$\frac{n-1}{n+1} \le \frac{P_{\max}}{d}\,; \qquad (3.6)$$

under cooperation, to

$$\frac{n-1}{2n} \le \frac{P_{\max}}{d}\,. \qquad (3.7)$$

If inequalities (3.6) or (3.7) hold, the equal or cooperative behavior of agents is compatible with the sustainable development conditions.

Otherwise, the Principal can use the impulsion mechanism to stimulate sustainable development among equal agents:

$$\tilde{p}(x) = \begin{cases} p^+ \text{ for } x \le \dfrac{P_{\max}}{dn}, \\ p^- \text{ otherwise.} \end{cases}$$

To examine the allocation of the cooperative payoff, we first construct the von Neumann–Morgenstern characteristic function (1.13). Obviously, $x_i = 1/n,\ i \in N\backslash K,$ for any coalition K . Therefore,

$$v^{\mathrm{NM}}(i) = (1-p)\max_{x_i}\left(\frac{n-1}{n} - \frac{n-1}{n} - x_i\right)x_i = 0, i \in N \ ;$$

$$v^{\mathrm{NM}}(K) = (1-p)\max_{x_i, i\in K}\left(\frac{n-1}{n} - \frac{n-k}{n} - \bar{x}_K\right)\bar{x}_K,\ k =| K | .$$

Since $\forall i \in K\ x_i = x$, we have $v^{\mathrm{NM}}(K) = k(1-p)\times$ $\times\max_x\left(\frac{k-1}{n} - kx\right)x$.

The first-order optimality condition $\frac{k-1}{n} - 2kx = 0$ yields $x^* = \frac{k-1}{2kn}, \bar{x}^* = \frac{k-1}{2n}$, and consequently,

$$v^{\mathrm{NM}}(K) = k(1-p)\left(\frac{k-1}{n} - \frac{k(k-1)}{2kn}\right)\frac{k-1}{2kn} = (1-p)\frac{(k-1)^2}{4n^2}.$$

Hence,

$$v^{\mathrm{NM}}(N) = \frac{(1-p)(n-1)^2}{4n^2} = \bar{u}^C.$$

By definition, the Petrosyan–Zaccour characteristic function (1.14) here coincides with the von Neumann–Morgenstern function. We construct the Gromova–Petrosyan characteristic function (1.15):

$$v^{\mathrm{GP}}(i) = (1-p)\left(\frac{n-1}{n} - \frac{n-1}{n} - \frac{n-1}{2n^2}\right)\frac{n-1}{2n^2} =$$
$$-\frac{(1-p)(n-1)^2}{4n^4},\ i \in N;$$

$$v^{\mathrm{GP}}(K) = (1-p)\left(\frac{n-1}{n} - \frac{n-k}{n} - \frac{k(n-1)}{2n^2}\right)\frac{k(n-1)}{2n^2} =$$
$$(1-p)\frac{k(n-1)(kn-2n+k)}{4n^4};$$

$$v^{\mathrm{GP}}(N) = \frac{(1-p)(n-1)^2}{4n^2} = \bar{u}^C .$$

Due to the symmetry of cooperative games, for all characteristic functions,

$$\Phi^{\mathrm{NM}} = \Phi^{\mathrm{PZ}} = \Phi^{\mathrm{GP}} = \left(\frac{(1-p)(n-1)^2}{4n^3},\ldots,\frac{(1-p)(n-1)^2}{4n^3}\right).$$

Obviously, in models with symmetric agents, social and private preferences coincide under equality and cooperation; the Shapley value-based allocations of the cooperative payoff are always the same for all characteristic functions.

Note that in this model, $u^C = u_1^{\mathrm{ST}} > u_i^{\mathrm{ST}}, i = 2,\ldots, n$. Thus, cooperation is more beneficial than hierarchical control for all agents except the Principal (who does not care). In this case,

$$\bar{u}^C - \bar{u}^{\mathrm{ST}} = \frac{(1-p)(n-1)}{4n^2}\left(n-1-\frac{n^2-n+1}{n^2}\right) =$$
$$\frac{(1-p)(n-1)}{4n^4}(n^2(n-2)+n-1) > 0,$$

i.e., cooperation is more beneficial than hierarchical control for the society. The indices

$$K^{\mathrm{NE}} = \frac{4n}{(n+1)^2} \xrightarrow[n\to\infty]{} 0,\ K^{\mathrm{ST}} = \frac{n^2-n+1}{n^2(n-1)} \xrightarrow[n\to\infty]{} 0$$

show that the benefit of cooperation compared to equality and hierarchical control will grow with the number of agents.

Example 2. The Cournot duopoly with asymmetric agents.

The model has the form

$$u_i = (1-p)(1-c_i-x_1-x_2)x_i \to \max,$$
$$0 \le x_i \le 1/2,\ \ i = 1, 2.$$

Compared to formula (3.1), $c_i \in (0, 1/2)$ is the costs of firm *i*. If the agents behave equally, the Nash equilibrium is found from the system of equations

$$\frac{\partial u_i}{\partial x_i} = 0, i = 1,2 .$$

As is easily verified,

$$x_i^{\mathrm{NE}} = (1+c_j-2c_i)/3,\ \ i,\ j = 1, 2;$$
$$\bar{u}^{\mathrm{NE}} = (2-c_1-c_2)/3, \qquad (3.8)$$

and the payoffs are:

$$u_i^{\mathrm{NE}} = (1-p)(1+c_j-2c_i)^2/9, i = 1,2 \ ;$$
$$\bar{u}^{\mathrm{NE}} = (1-p)(2-2c_1-2c_2+5c_1^2+5c_2^2-8c_1c_2)/9.$$

The cooperation of agents leads to the optimization problem

$$\bar{u} = (1-p)[(1-\bar{x})\bar{x} - c_1x_1 - c_2x_2] \to \max,$$
$$0 \le x_i \le 1/2,\ \ i = 1, 2.$$

The system of equations $\partial\bar{u}/\partial x_i = 0,\ \ i = 1, 2,$ reduces to

$$\begin{cases} x_1 + x_2 = (1-c_1)/2, \\ x_1 + x_2 = (1-c_2)/2. \end{cases}$$

Under the assumption $c_1 \ne c_2$, it has no solution. On the boundary of the set of admissible controls, the total payoff function takes the following values:

$$\bar{u}(0,\ 0) = 0;\ \bar{u}(1/2,\ 1/2) = -(1-p)(c_1+c_2) < 0;$$
$$\bar{u}(1/2,\ 0) = (1-p)(1/4-c_1/2);$$
$$\bar{u}(0,\ 1/2) = (1-p)(1/4-c_2/2).$$

Thus, the solution to the cooperative problem and the corresponding payoffs are given by

$$x^C = \begin{cases} (1/2,\ 0),\ \ c_1 < c_2 \Rightarrow \bar{u}^C = (1-p)(1-2c_1)/4, \\ \qquad u_i^C = (1-p)(1-2c_1)/8,\ i = 1,\ 2; \\ (0,\ 1/2),\ \ c_1 > c_2 \Rightarrow \bar{u}^C = (1-p)(1-2c_2)/4, \\ \qquad u_i^C = (1-p)(1-2c_2)/8,\ \ i = 1,\ 2. \end{cases}$$

In both cases, the total cooperative output is $\bar{x}^C = 1/2$.

Suppose that agent 1 becomes the Principal: first chooses x_1 and informs the other agents of it. Similarly to Example 1, we arrive at the Stackelberg equilibrium

$$x_1^{\mathrm{ST}} = (1-2c_1+c_2)/2;\ x_2^{\mathrm{ST}} = (1+2c_1-3c_2)/4 .$$

In this case, the total output and payoffs are:

$$\bar{x}^{\mathrm{ST}} = (3-2c_1-c_2)/4\,;$$

$$u_1^{\mathrm{ST}} = (1-p)(1-2c_1+c_2)/8\,;$$

$$u_2^{\mathrm{ST}} = (1-p)(1+2c_1-3c_2)/16;$$

$$\bar{u}^{\mathrm{ST}} = (1-p)(3-4c_1-2c_2+12c_1^2-20c_1c_2+11c_2^2)/16.$$

Now consider the following case: the Principal is an additional non-production agent 0 that assigns the tax rate p. By analogy with (3.3), the Principal's problem can be written as

$$u_0 = (1-c_1-c_2-\bar{x})\bar{x}p - ap^2 \to \max, 0 \le p \le 1\,.$$

The optimal response of agents to the Principal's strategy p is the Nash equilibrium in their game (3.8). Similarly to Example 1, we obtain the Principal's impulsion strategy

$$p^{\mathrm{IMP}} = \frac{(1-2c_1-2c_2)(2-c_1-c_2)}{18a}$$

and the impulsion equilibrium $\mathrm{IMP} = (p^{\mathrm{IMP}},\, x_1^{\mathrm{NE}},\, x_2^{\mathrm{NE}})$.

Finally, we introduce the environmental constraint (sustainable development condition) (3.5). In the Nash equilibrium, this condition takes the form

$$d(2-c_1-c_2) \le 3P_{\max}\,;$$

under cooperation,

$$d \le 2P_{max}\,.$$

For $n = 2$, constructing the game in characteristic function form is unreasonable.

CONCLUSIONS

An obvious main result of this paper consists in the following. In deterministic models, cooperation is not worse for the society than any other organizational mode of the interaction of active agents because it leads to a nonnegative cooperative effect. The collective losses due to rejecting cooperation can be assessed using various indices (the classical problem of the inefficiency of equilibria).

However, individual agents may benefit more from seizing the leadership or keeping independence. The rules for allocating the cooperative payoff among agents are not obvious as well. Therefore, along with the social preferences, it is necessary to consider the private ones (generally, unequal for different agents). Here, comparative efficiency indices can be also used.

Even in simple models, it is not easy to calculate the payoffs of individual agents and the society and compare them analytically. This paper has illustrated the proposed comparative analysis methodology in the case of symmetric agents. Further research will focus on a numerical study of the comparative efficiency of organizational modes, control methods, and allocations of the cooperative payoff for several static and dynamic Cournot oligopoly models.

REFERENCES

1. Burkov, V.N. and Novikov, D.A., *Teoriya aktivnykh sistem: sostoyanie i perspektivy* (Theory of Active Systems: State and Prospects), Moscow: Sinteg, 1999. (In Russian.)
2. Novikov, D.A., *Theory of Control in Organizations*, New York: Nova Science Publishers, 2013.
3. Germeier, Yu.B., *Vvedenie v teoriyu issledovaniya operatsii* (Introduction to Operations Research), Moscow: Nauka, 1971. (In Russian.)
4. Germeier, Yu.B., *Non-Antagonistic Games*, Dordrecht: Springer, 1986.
5. Moiseev, N.N., *Elementy teorii optimal'nykh sistem* (Elements of the Theory of Optimal Systems), Moscow: Nauka, 1975. (In Russian.)
6. Kukushkin, N.S. and Morozov, V.V., *Teoriya neantagonisticheskikh igr* (Theory of Non-Antagonistic Games), Moscow: Moscow State University, 1984. (In Russian.)
7. Gorelik, V.A., Gorelov, M.A., and Kononenko, A.F., *Analiz konfliktnykh situatsii v sistemakh upravleniya* (Analysis of Conflict Situations in Control Systems), Moscow: Radio i Svyaz', 1991. (In Russian.)
8. Laffont, J.-J. and Martimort, D., *The Theory of Incentives: The Principal-Agent Model*, Princeton University Press, 2002.
9. Ougolnitsky, G.A., *Upravlenie ustoichivym razvitiem aktivnykh sistem* (Sustainable Management of Active Systems), Rostov-on-Don: Southern Federal University, 2016. (In Russian.)
10. Ougolnitsky, G.A., Methodology and Applied Problems of the Sustainable Management in Active Systems, *Control Sciences*, 2019, no. 2, pp. 19–29.
11. Mazalov, V.V., *Mathematical Game Theory and Applications*, Wiley, 2014.
12. Petrosyan, L.A., Zenkevich, N.A., and Shevkoplyas, E.V., *Teoriya igr* (Game Theory), St. Petersburg: BKhV- Peterburg, 2011. (In Russian.)
13. Basar, T. and Olsder, G.Y., *Dynamic Non-Cooperative Game Theory*, SIAM, 1999.
14. Dockner, E., Jorgensen, S., Long, N.V., and Sorger, G., *Differential Games in Economics and Management Science*, Cambridge: Cambridge University Press, 2000.
15. Gorelov, M.A. and Kononenko, A.F., Dynamic Models of Conflicts. III. Hierarchical Games, *Automation and Remote Control*, 2015, vol. 76, no. 2, pp. 264–277.
16. Ougolnitsky, G.A. and Usov, A.B., Computer Simulations as a Solution Method for Differential Games, in *Computer Simulations: Advances in Research and Applications*, Pfeffer, M.D. and Bachmaier, E., Eds., New York: Nova Science Publishers, 2018.
17. *Algorithmic Game Theory*, Nisan, N., Roughgarden, T., Tardos, E., and Vazirany, V., Eds., Cambridge: Cambridge University Press, 2007.
18. Dubey, P., Inefficiency of Nash Equilibria, *Math. Operations Research,* 1986, no. 11(1), pp. 1–8.
19. Johari, R. and Tsitsiklis, J.N., Efficiency Loss in a Network Resource Allocation Game, *Math. Operations Research*, 2004, no. 29(3), pp. 407–435.
20. Roughgarden, T., *Selfish Routing and the Price of Anarchy*, MIT Press, 2005.
21. Papadimitriou, C.H., Algorithms, Games, and the Internet, *Proc. 33rd Symp. Theory of Computing*, 2001.
22. Basar, T. and Zhu, Q., Prices of Anarchy, Information, and Cooperation in Differential Games, *Dynamic Games and Applications*, 2011, no. 1(1), pp. 50–73.

23. Dahmouni, I., Vardar, B., and Zaccour, G., A Fair and Time-Consistent Sharing of the Joint Exploitation Payoff of a Fishery, *Natural Resource Modeling*, 2019, vol. 32, article no. e12216.
24. Zhang, W., Zhao, S., and Wan, X., Industrial Digital Transformation Strategies Based on Differential Games, *Applied Mathematical Modeling,* 2021, vol.98, pp. 90–108.
25. Sharma, A. and Jain, D., Game-Theoretic Analysis of Green Supply Chain under Cost-Sharing Contract with Fairness Concerns, *International Game Theory Review*, 2021, vol. 23, no.2, pp. 1–32.
26. Moulin, H., Axioms of Cooperative Decision Making, Cambridge: Cambridge University Press, 1988.
27. von Neumann, J. and Morgenstern, O., *Theory of Games and Economic Behavior*, Princeton: Princeton University Press, 1953.
28. Petrosyan, L. and Zaccour, G., Time-Consistent Shapley Value Allocation of Pollution Cost Reduction, *Journal of Economic Dynamics and Control*, 2003, vol. 27, no. 3, pp. 381–398.
29. Gromova, E.V. and Petrosyan, L.A., On an Approach to Constructing a Characteristic Function in Cooperative Differential Games, *Automation and Remote Control,* 2017, vol. 78, pp. 1680–1692.
30. Shapley, L., A Value for *n*-person Games, Santa Monica, CA: The RAND Corporation, 1952.
31. Moulin, H., Game Theory for the Social Sciences (Studies in Game Theory and Mathematical Economics), New York: New York University Press, 1986.

This paper was recommended for publication
by D.A. Novikov, a member of the Editorial Board.

Received March 31, 2022, and revised June 29, 2022.
Accepted July 1, 2022

Author information

Ougolnitsky, Gennady Anatol'evich. Dr. Sci. (Phys.–Math.), Southern Federal University, Rostov-on-Don, Russia
✉ gaugolnickiy@sfedu.ru

Cite this paper

Ougolnitsky, G.A. An Approach to Compare Organizational Modes of Active Agents and Control Methods. *Control Sciences* **3,** 24–33 (2022). http://doi.org/10.25728/cs.2022.3.3

Original Russian Text © Ougolnitsky, G.A., 2022, published in *Problemy Upravleniya*, 2022, no. 3, pp. 29–39.

Translated into English by *Alexander Yu. Mazurov*,
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander. mazurov08@gmail.com

DOI: http://doi.org/10.25728/cs.2022.3.4

ASSESSMENT OF OPERATOR AUTHENTICATION METHODS IN INDUSTRIAL CONTROL SYSTEMS[1]

V.G. Promyslov[1], K.V. Semenkov[2], N.E. Mengazetdinov[3]

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

[1]✉ vp@ipu.ru, [2]✉ semenkovk@ipu.ru , [3]✉ mengazne@mail.ru

Abstract. This paper considers the authentication of operators in instrumentation and control (I&C) systems for industrial facilities. The main emphasis is on such systems for critical facilities, on an example of nuclear power plants (NPPs). Authentication methods known for public information systems (password, token, and biometrics) are surveyed, and their applicability in typical working conditions of an I&C system operator is analyzed. The analysis includes experimental testing of password and biometric authentication methods and an expert assessment of their advantages and disadvantages for I&C systems. According to the testing results, all the methods under consideration have somewhat worse values of the false rejection rate (FRR) compared with the known characteristics from available sources. The best results are shown by biometric identification by the face geometry. However, the percentage of FRR for this method is significant, which can affect the availability of the control function for a legitimate operator. As concluded, a promising approach for industrial control systems is to implement multi-factor authentication: token or password protection for blocking authentication jointly with biometric authentication by the face geometry with a non-blocking security policy.

Keywords: authentication, biometrics, token, password, industrial control system, I&C, operator.

INTRODUCTION

Modern industrial enterprises, including hazardous ones (e.g., nuclear power plants (NPPs), transport and chemical industry enterprises, etc.) depend on digital automated control systems. The control loop of such systems often includes a human operator, who exerts an impact on the controlled facility and its control system through the computers within an instrumentation and control (I&C) system.

In I&C systems, authentication arises when allowing a trusted operator to control an industrial facility (particularly when granting some action rights to the operator). In information technology, this procedure is commonly referred to as authorization. Authentication can be defined as “actions to verify the genuine character of an access subject and (or) access object as well as verify that the access identifier and authentication information presented belongs to the access subject and (or) access object.” [1].

The authenticating subject performs verification by matching some personal identifier (e.g., a shared secret) negotiated in advance during user registration. This can be done to create trusted communications between parties or grant access rights to communication and computing resources of the system during authorization.

Unauthorized operator actions can violate the basic information security properties (integrity, availability, and confidentiality) and, moreover, cause economic damage or harm to human health. An additional problem is to trace control decisions on the facility, i.e., ensure the non-repudiation of previously performed actions. In general, these problems force using more formal authentication methods even for routine operations in I&C systems.

The authentication of operators in I&C systems for critical facilities has peculiarities associated with the

[1] This work (Sections 2.3–2.5) was supported in part by the Russian Foundation for Basic Research, project no. 19-29-06044.

controlled facility and information security policy [2]. They distinguish operator authentication in I&C systems from user authentication in public information systems. The main peculiarities are as follows:

- A demilitarized zone to access the facility reduces the threat from an external intruder in personnel authentication. However, it does not eliminate the threat posed by an internal intruder: a person without operator authority but admitted to the zone may attempt to access operator control functions.
- The priority of accessibility over other information security properties applies strong requirements to the duration of the authentication process and the probability of first-kind errors (the percentage of the false rejection rate, FRR).
- Stressful situations in the operator's work (e.g., an industrial accident) may cause the person to forget obvious things, and his functional and external characteristics may change (trembling hands, another voice timbre, perspiration, etc.).
- Authentication complication may occur due to some changes in the environment. Such complication neither destroys the facility nor immediately violates functions of the I&C system and the facility; but it causes inconvenience to the operator (e.g., partial failure of the lighting system, smoke, activation of the firefighting system, earthquake, etc.).

Like for conventional information systems, authentication problems for I&C systems include operator (user) authentication on the computer (digital device) and computer authentication. For public information systems, computer authentication is well developed [3, 4]. In I&C systems with controllers and industrial computers, protocols with weak authentication mechanisms or even without any authentication are often used. However, reliable computer-to-computer authentication in I&C systems is a problem of particular implementations rather than of scientific study.

User authentication protocols are much less secure than computer-to-computer authentication protocols because they deal with people and their limited capabilities and weaknesses [5]. In information security, people are often the weakest element in protection.

In this paper, we select and validate authentication methods and protocols with application to operator authentication in I&C systems. We analyze the main user authentication methods and protocols and experimentally test them considering the peculiarities of industrial facilities and information security policies. As an example of I&C systems, we choose the upper-unit control system for NPPs that was developed at the Trapeznikov Institute of Control Sciences RAS [6].

The experimental studies below proceed from the assumption that the operator's working conditions at the facility and the exposure of people and equipment to physical fields are close to the normal office environment. This assumption may be violated for some industrial facilities, but such factors go beyond the scope of the paper.

1. AUTHENTICATION METHODS AND PROTOCOLS IN INDUSTRIAL CONTROL SYSTEMS

We consider the main user authentication methods and compare their effectiveness with application to I&C systems.

User authentication methods can be divided into classes based on three questions [7]:

– What do you know?
– What do you have?
– Who are you?

Often the three authentication methods are associated with their characteristic representatives: password, token, and biometric trait. Therefore, when describing each of them, we will refer to their particular implementations. In all cases, the object of authentication is a person.

1.1. Password authentication methods

A password is a secret word known to the user and possibly to the computer on which the user undergoes authentication. This word is related to the key by which authentication occurs. In theory, password authentication can be very strong. For example, in the case of the extended encryption standard [8], the maximum key length is 256 bits, and it would take an intruder over 10^{76} attempts on average to guess the key (too long now and in the foreseeable future). If the password and the authentication key are directly related, a password of comparable length is needed to ensure high reliability of the key, which is too much for a human to remember. In practice, this key is stored, e.g., in a file protected by a shorter password. The main vulnerability of password protection is that a memorable password can be guessed or found by an intruder [5, 9], whereas a long, random, and changeable password is difficult to remember. (Therefore, it can be written down and stored in plaintext.) According to [10, 11], about 20% of users apply no more than five thousand passwords out of all possible combinations. Consequently, the search space for hacking a system is reduced, and an intruder can often focus on these five thousand combinations.

The drawbacks of password authentication can be avoided by choosing other classes of methods in which a person becomes not the subject but object of authentication. These are token-based and biometric methods.

1.2. Authentication methods using tokens

A token is a physical device that performs or assists authentication. The term also refers to software tokens issued to the user after successful authentication as the key to access services. Tokens can be passive or active (e.g., providing one-time access codes or changing synchronously with the host master, etc.). Token security is ensured by various protection means, such as a token case or special hardware that disables the token when compromised or if the number of failed authentication attempts exceeds a given threshold.

In general, a token can be considered a secret similar to a password, except that it is machine-generated or machine-stored, so it can be longer, more random, and possibly change over time.

1.3. Biometric methods

For a person as a user, biometrics is the most convenient and easy way to authenticate: it extends natural ways of establishing identity.

Biometrics, or biometric personal data, is some measurable individual characteristic of the human body that can be used for user authentication. The standard [1] defines biometric personal data as information characterizing the physiological and biological traits of a person to establish his or her identity.

Biometrics is intended to link the authenticator (trait) and the owner of the authentication trait inseparably. In the case of passwords and tokens, this cannot be done in principle because both can be borrowed or stolen. Such an inseparable linkage between the authentication trait and the trait holder would ensure non-repudiation. (With this property, there is such evidence of given actions that the parties involved cannot subsequently reject the transaction as unauthorized or claim that they did not perform those actions.) However, biometric traits, like passwords, can be copied or forged at some cost and used to gain unauthorized access. In general, biometrics at the current technological level does not guarantee non-repudiation.

Biometric authentication data are usually typified into physical and behavioral. The physical type includes biometrics based on stable body traits (fingerprints, face, iris, hand shape, etc.). The behavioral type includes skills acquired through training, such as handwriting signature, keyboarding dynamics, and gait. Being the product of learned behavior, voice is usually typified as behavioral biometrics [12–14].

Biometric authentication, like other methods, may cause errors [15], but the user’s attitude to errors varies for different authentication methods. The user may forget or incorrectly enter a password and may lose a token. Such situations are uncomfortable, but the user understands his or her fault. In the case of biometric authentication errors, the user is not at fault and cannot fix the problem independently.

A biometric error can occur for different reasons:

– a dirty scanner,

– poor lighting,

– the system initially remembered the wrong template for comparison,

– the system poorly adapts to changes in the environment (cold, rain, sun glare, dryness, etc.) or to natural changes in the user’s biometric traits (hairstyle, beard, cut finger, etc.).

A recent example of biometrics problems is the need to wear masks due to the pandemic.

Detailed requirements for biometric authentication methods were presented in regulatory documents, e.g., the standard [16].

1.4. Authentication protocols and their application in I&C systems

For the user authentication problem, we consider the most general authentication protocol [17]. It establishes the exchange rules to ensure authentication based on bilaterally negotiated secret information.

For public information systems, widespread variants of the authentication protocol are challenge-response protocols [18]. They underlie authentication protocols in Unix with PAM modules [19] and MS Windows [20] and can be used to authenticate I&C system operators based on these operating systems. According to our experience, this protocol has limited use for password authentication due to availability requirements and operator’s scenarios when performing critical functions of the system. Nevertheless, the protocol can be applied, e.g., to access the reprogramming function of a digital device.

In real systems, authentication protocols often combine different authentication methods [21] to achieve a high level of protection and its echeloning (multifactor authentication). In this case, the logical AND algorithm is implemented: all authentication methods must be successfully passed to complete. Currently, the vast majority of multifactor authentication approaches involve the "physical token–password" pair [22, 23]. The password and biometric identifier are rarely combined: biometrics is usually chosen for convenience to avoid remembering the password.

Three-factor authentication has not found wide application, although such implementation may be needed for accessing functions with a high level of protection. Table 1 summarizes the main advantages and disadvantages of some multifactor authentication methods. Also, an expert assessment of their suitability for operator authentication in I&C systems is presented on a qualitative scale (bad–satisfactory–good).

Basic authentication protocols are easily modified for multifactor authentication. However, for implementing a security policy with high availability requirements, typical for I&C systems, introducing an additional transaction and complexity in the protocol may cause adverse effects.

For I&C systems and other objects with availability priority, multifactor authentication can be implemented according to the logical OR scenario. In this case, authentication is considered complete if at least one of the multifactor authentication methods is successfully passed.

2. AUTHENTICATION METHODS: ANALYSIS AND COMPARISON

2.1. Principles of comparison

We compare the three main authentication methods by their applicability for I&C systems using the following features: strength, advantages (convenience) and drawbacks, and the quality of identification. The comparative analysis below is mostly qualitative and largely rests on practical (expert) experience, which may have a subjective nature. The set of indicators is taken from the paper [7].

Table 2 summarizes the main attributes of the three authentication methods.

Table 1

Comparison of multifactor user authentication methods for stronger protection in I&C systems

A combination of authentication methods	Advantages	Drawbacks	Example	Assessed applicability for I&C systems
"What do you know?" + "What do you have?"	Losing a token does not immediately compromise it: the token is protected by a password	The user must have a token and remember the password	Bank card + PIN	Satisfactory
"What do you have?" + "Who are you?"	Losing a token does not immediately compromise it: the token is protected by the owner's uniqueness	The user must have a token. May lead to false authentication rejection due to imperfect biometric methods	Pass with chip and photo	Good
"What do you know?" + "Who are you?"	User ID spoofing (using a double) will not result in false authentication	May lead to false authentication rejection due to imperfect biometric methods	Password + fingerprint sensor on the computer	Satisfactory
"What do you know?" + "What do you have?" + "Who are you?"	All three methods work sequentially	The user must have a token and remember the password. May lead to false authentication rejection due to imperfect biometric methods	Authentication for accessing a critical facility, including a chipped badge with a photo at the entrance, a biometric fingerprint scanner for accessing the room, and a password for computer access	Bad

Table 2

Three basic user authentication methods and their attributes

Authentication methods	What do you know?	What do you have?	Who are you?
Implementation	Password	Token	Biometrics
Authentication basis	Knowing the secret	Owning the proper object	Having traits of the subject
Protection type	Keeping the secret	Physical security	Uniqueness of the subject
Examples of vulnerabilities	Can be peeked or guessed	Can be lost or stolen	Can be forged; difficult to change when compromised

2.2 Practical entropy of the key

Comparing the strength of different authentication methods is not an easy task: the protocol key may have different relationships to the initial data depending on the particular implementation of an authentication method. For example, in password authentication, a key may simply be a stored copy of a password, its hash code, or validation values that depend on passwords but cannot be directly used by an intruder to authenticate. In other authentication methods, some value from a token or biometric device may be used instead of a password.

Therefore, to assess the strength of authentication methods, we adopt an entropy-based measure of the key that can be directly obtained from the initial data (a password, information stored in a token, or biometric data). According to the studies of leading IT companies with a large volume of personal data (Yahoo and Google) [5], the entropy of the key based on passwords is 10–20 bits. As noted, using hash codes reduces the entropy of the key closer to the left limit (10 bits) since the hash code is optimized to provide fast performance at the cost of lower strength of the key. Although, e.g., implementations of *Secure Hash Algorithm* 1 (SHA1) [24] are configurable and can be very strong.

Early studies [5] demonstrated that biometric and password protection methods have approximately the same entropy of the key and, consequently, the same strength. However, according to more recent results, biometrics ensures a degree of protection 2–3 three times better than password authentication [25].

To our knowledge, strength was not examined for password operator authentication methods in I&C systems. However, it seems reasonable to take the strength of passwords closer to the lower limit (simple passwords). The security policy of an industrial facility can and must contain password strength requirements and a password management procedure: a too complex (strong) password is impossible to use due to system availability requirements and stressful situations in the operator’s work.

The key obtained from the data and contained in the token can have a very large entropy when using algorithms similar to computer-to-computer authentication. For example, the entropy of the key reached 128 bits in [26]. However, it is necessary to consider the probability of token theft, which can be significant, especially under malicious intent.

2.3. The quality of identification: main indices

Traditionally two indices are used to assess the quality of identification: *the False Rejection Rate* (FRR) and *the False Acceptance Rate* (FAR).

The first rate is the probability of denying access to an authorized person. The second rate is the probability of making a false authentication. The better the system is, the lower the FRR value will be under the same FAR values. FAR makes sense only for biometric authentication: for other authentication methods, its value reflects human capabilities (typing and memorizing the password) or the reliability of hardware implementation.

Any authentication method has some share of errors due to hardware failures (e.g., a token reader or keypad). As practice shows, this share is negligible. The quality of biometric authentication is the most unstable characteristic since it depends heavily on the person. Table 3 contains typical errors for different biometric authentication methods available in the literature. Typical errors demonstrate only a trend: the comparison of different biometric authentication implementations and algorithms is beyond the scope of this paper.

Table 3

Typical biometric authentication errors

Type of biometrics	FAR	FRR	Sample size [27]	Source
Fingerprint recognition	10^{-3}	10^{-2}	$5\cdot10^{6}$	[27]
Facial recognition	0.058		$12\cdot10^{6}$	[27]
Retinal recognition	0.059		$500\cdot10^{3}$	[27]

We conducted additional testing to investigate the practical aspects of the applicability of commercially available biometric authentication devices for I&C system operators. During the testing, we simulated some typical working conditions of the I&C system operator. The results are presented in subsection 3.4.

2.4. The applicability of authentication methods for I&C system operators: Practical testing

We tested password authentication and some implementations of biometric authentication methods in typical working scenarios for I&C system operators at an industrial facility. Token-based authentication was not tested: its properties are determined by the capabilities inherent in the design and manufacture of a token, and they are supposed stable during operation.

Table 4 shows the commercial devices used and the type of biometric authentication available on the device. At the time of writing the paper, these devices were officially supplied to the Russian Federation without license restrictions. For testing biometric authentication methods, we chose devices and algorithms available to the mass consumer and used for authentication in mobile devices. For password authentication tests, typical PC keyboards used at the workplaces of I&C system operators were used. According to our experience, mass products are mainly adopted when implementing technical security measures for industrial systems.

Table 4

Devices used in testing

Device	Authentication type
HONOR 10. Android ver. 10	Fingerprint recognition; facial recognition
MI 5S Plus. Android ver. 8. MIUI Global ver. 10.2	Fingerprint recognition
PC with a membrane keyboard	Password protection

At least 50 tests were conducted for each method. Each test involved a group of two testers: on the command of one tester, the other (operator) attempted to authenticate using an authentication method.

During testing, the testers in the group periodically exchanged their roles. In each test, two measurements were performed: the time to authenticate and the number of attempts to do it. The testing was conducted both in normal working conditions and under complication hindering authentication; see Table 5.

Table 5

Types of complication during testing

Complication no.	Description
1	Warmed hands
2	Pouch on the sensor
3	Thin-layer water on the finger
4	Cooled finger
5	Facial mask
6	Changed angle between the camera and the face
7	Changed lighting
10	Password entered while standing
11	Password entered with gloves on
12	Password entered “blindly”
13	Password entered during physical complication (one tester nudged the other)

For password authentication methods, the password was changed after every ten tests according to the selected complexity level.

The testing results are shown in Table 6.

Table 6

Testing of authentication methods

Test (Working conditions)	Result	
	Maximum, minimum, and average time, s	The maximum number of attempts for successful authentication
Simple password (5 characters; dictionary word-based; normal conditions)	2.63; 1.82; 2.1	1
Simple password (5 characters; dictionary word-based; complication 8)	6.34; 2.1; 2.3	2
Simple password (5 characters; dictionary word-based; complication 9)	9.29; 1.68; 4.2	3
Simple password (5 characters; dictionary word-based; complication 10)	12.64; 2.37; 5.62	4
Simple password (5 characters; dictionary word-based; complication 11)	20.33; 2;06; 6.12	6
Complex password (at least 9 characters; capital and small letters and numbers; normal conditions)	24.5; 5.33; 9.1	3
Complex password (at least 9 characters; capital and small letters and numbers; complication 10)	11.59; 5.98; 6.6	1
Complex password (at least 9 characters; capital and small letters and numbers; complication 11)	49.03; 9.1; 12;6	3
Complex password (at least 9 characters; capital and small letters and numbers; complication 12)	95.31; 7.8; 23.4	11
Complex password (at least 9 characters; capital and small letters and numbers; complication 13)	46.39; 8.1; 24.3	4
Fingerprint (normal conditions)	3.92; 0.99; 1.44	2
Fingerprint (complication 1)	1.23; 1.09; 1.2	1
Fingerprint (complication 2)	2.69; 1.09; 1.82	3
Fingerprint (complication 3)	9.48; 1.05; 3.61	6
Fingerprint (complication 4)	3.59; .2.1; 1.7	3
Face geometry (normal conditions)	2.87; 1.85; 1.91	1
Face geometry (complication 5)	4.23; 1.7; 2.64	2
Face geometry (complication 6)	5.42; 1.64; 3.26	2
Face geometry (complication 7)	2.09; 0.99; 1.2	1

For the password method, we obtained a relatively high ($\sim 10^{-1}$) probability of denying access for an authorized person under complication. The FRR grows with increasing password complexity. Due to a high probability of errors when entering a password (especially a complex one) under complication, the operator has to enter the password twice and more for successful authentication. (In tests, this value reached 11 times.) In this case, authentication time increases by an order of magnitude, with a typical value of about two or three seconds for a simple password and about five seconds for a complex password.

Such delays may be critical for I&C systems. This can be a reason to abandon password protection in favor of tokens, biometrics, or organizational and physical authentication measures and their combinations.

Among the biometric authentication methods, the best testing results were demonstrated by facial identification. For biometric authentication methods, additional testing was conducted to determine the possibility of false authentication. None of the biometric methods allowed false authentication within the means available to the average user ($\mathrm{FAR} = 0$). However, biometric authentication for I&C system operators is not free of second-kind errors, and these results do contradict the typical values in the previous section. The reasons can be the limited sample size and the fact that bypassing the protection systems requires knowledge of the implementation features of the particular algorithms for comparing the biometric template and, possibly, special equipment.

The FRR values for biometrics obtained in practical conditions exceed the typical ones by approximately an order of magnitude. The main reason is the presence of complication. These results should be considered when using biometric authentication methods for I&C system operators.

2.5. Authentication methods in I&C systems: Analysis of applicability

Let us analyze the main problems associated with applying each authentication method in typical working conditions of I&C system operators.

- Knowledge-based authenticators ("What do you know?") include secret information (password), which is unknown and can be roughly defined as "hidden from most people." The disadvantage is that each time secrets are used for authentication, they become less and less secret. In addition, "most people" often means "most honest people": for an intruder applying some effort (e.g., social engineering means), such information is no longer secret. I&C systems are characterized by a high level of trust between users established during personnel selection and production activities (people do common work for a long time). Therefore, an intruder penetrating an isolated team has an easier task of obtaining knowledge (particularly passwords) from other team members.
- Object authenticators ("What do you have?") are material objects (e.g., a token). Such authenticators have the same main drawback as their predecessors (physical keys). If the key is lost, anyone who finds it can bypass the protection system. In this sense, the weaknesses of object authenticators are similar to password protection: an intruder can use a lost or stolen token. As mentioned, I&C system users trust each other. In contrast to password protection, if a physical object is lost, the owner will know about it the first time he accesses it and will take measures to neutralize the threat as quickly as possible.
- Identity-based authenticators ("Who are you?") are related to one person: they are unique. This class includes all biometric authentication methods (fingerprints, eye and iris scans, voice prints or signatures). Biometric authentication has a relatively high degree of protection against copying and tampering and obviously cannot be lost [28].

Summarizing the aforesaid, we conclude that there are no ideal authentication methods: they have "inherent" drawbacks. Table 7 shows the characteristic vulnerabilities of different authentication methods with application to I&C systems. Clearly, the opportunities for attacks on the authentication system of an I&C system are unequal within a given security policy. If an enterprise has an effective intrusion detection system, and there are officials responsible for computer security, brute force attacks will be easy to detect, and appropriate measures will be taken. At the same time, attacks involving the theft of a token or password (especially the latter) are very likely, given the high degree of trust usually established between I&C system users. As we believe, I&C systems should have non-blocking protection against many attacks attempting to bypass the authentication procedure. Non-blocking protection methods are primarily intended to draw the security officer's attention to an abnormal situation, who will take appropriate measures in response to a security event.

Table 7

Compromised security properties in different authentication methods

Compromised security property	Authentication method	Example of an attack	Typical protection methods
Irrefutability	Password, token	Lost or stolen token	Personal liability of the user for loss (administrative protection measure)
	Biometrics	Fake	Multifactor authentication
Detecting compromise	Password, biometrics	Forgery, theft	Informing the user about the use of the authenticator (*last login*)
	Token		Detecting a loss by the user
User spoofing during initial identification	Password	Passing data to an unauthorized person. Default password	Personal appearance of the user. Password management policy
	Token	Passing a token to an unauthorized person	Personal appearance of the user
	Biometrics	Replacing user biometric data	

Table 7 (continued).

Compromised security property	Authentication method	Example of an attack	Typical protection methods
Data leakage when updating the identifier	Password	Passing data to an unauthorized person. Default password	Password management policy. Multifactor authentication
	Token	Passing a token to an unauthorized person	Personal appearance of the user and return of the token if it is broken but not lost
	Biometrics	Replacing user biometric data when compromised	Personal information management policy
Denial of service	Password, token, biometrics	Multiple unsuccessful attempts to block access	Non-blocking security policy with security officer notification
False authentication	Password, token, biometrics	Attack with message retransmission	The challenge-response protocol
	Password	Brute force attack	Blocking security policy under a given number of failed authentication attempts

2.6. Authentication methods for I&C systems: Qualitative analysis and comparison

Various indicators can be proposed to compare authentication methods. We consider three high-level indicators traditionally used to compare such methods [5]:

– usability,

– the ease of deployment,

– security.

For each set of high-level indicators, we choose a set of lower-level indicators. The values of all indicators in the set are assessed using the ranking scale: “good” (2), “satisfactory” (1), and “bad” (0). The value of a high-level indicator is calculated as the sum of individual indicators in the set.

Consider indicators of usability (Table 8) and the ease of deployment (Table 9Table). In turn, Table 10 presents indicators of security: what types of attacks the authentication method can prevent.

Table 8

Different authentication methods with application to I&C systems: indicators of usability

Indicator	Password	Token	Biometrics
Ease of interaction with the authentication scheme for the user	Satisfactory	Good	Satisfactory
Easy to learn: users not familiar with the method can understand and master it without much trouble	Good	Good	Satisfactory
Infrequent errors: the task to authenticate is usually completed successfully when performed by a legitimate and honest user	Satisfactory. Users are usually successful but with a weak password	Good	Satisfactory
Scalability for users: Using a scheme for hundreds of accounts does not increase the burden on the user	Bad. People often reuse passwords or create a simple uniqueness scheme for each website involving a basic password	Satisfactory. The problem of choosing one token from the set of available tokens is not always trivial	Good
Easy recovery from compromise	Good. The advantage of passwords is that they are easy to reset	Satisfactory	Bad
The need to have something at hand	Good	Bad	Good
Score:	8	8	7

Table 9

Different authentication methods with application to I&C systems: indicators of the ease of deployment

Indicator	Password	Token	Biometrics
Easy implementation of the authentication method in real systems	Good	Good	Satisfactory
Compatibility with the authentication server	Good. Authentication servers are originally designed for password-based authentication methods	Good. From the server's point of view, the key obtained from the token is indistinguishable from that obtained from the password	Satisfactory. It may be necessary to implement the protection of biometric information if stipulated by law
Compatibility with the client computer	Good. Authentication clients are originally designed for password-based authentication methods	Satisfactory. Requires support from special devices	Satisfactory. Requires support from special devices
Availability. Restrictions on use depending on the individual	Good	Good	Bad The availability of the method may vary depending on health conditions and injuries. Certain biometric authentication methods may be unavailable for people with disabilities. For I&C system operators, this may be relevant in the case of temporary personnel without proper medical selection (unlike regular operators)
Upgrade option	Satisfactory	Good (Given administrative support)	Bad. Biometrics change very slowly (voice, face) or not at all (fingerprints)
Score:	9	9	3

Table 10

Different authentication methods with application to I&C systems: indicators of security

Indicator	Password	Token	Biometrics
Resistance to observation	Bad. An attacker can impersonate a user after observing his or her authentication several times (say, 10–20). Attacks include shoulder surfing, video recording of the keyboard, recording keystroke sounds, TV images of the keyboard, etc.	Good	Good
Resistance to social engineering methods	Good. An acquaintance (or an experienced hacker) cannot impersonate a user via personal data knowledge (date of birth, names of relatives, etc.).	Good	Good
Resistance to simple guesswork	Satisfactory. Depends on password length	Good	Good
Resistance to internal attacks by actors within the computer system	Satisfactory. Depends on password length	Good	Satisfactory. Biometric methods, like passwords, have low entropy and length of the key
Score:	4	8	7

The total scores of the authentication methods over the three groups of indicators are given in Table 11. According to the analysis results, token-based authentication can be the most balanced method when used independently.

Table 11

The total scores of authentication methods over three groups of indicators

	Password	Token	Biometrics
Total score:	21	25	17

CONCLUSIONS. DISCUSSION OF THE RESULTS

As emphasized, this paper has considered the peculiarities of known authentication methods with application to I&C system operators.

The accumulated experience of using authentication methods for public information systems has been studied. According to the survey of available sources, the degrees of protection provided nowadays by each method are comparable. Note a general problem: an inconvenient authenticator is either not used or used improperly, which can cause vulnerability. In practice, if I&C system operators need to remember multiple passwords to access different workstations or perform different operations, they will choose simple passwords or passwords linked by simple logic. The enterprise security policy may impose certain requirements on passwords (e.g., length, special characters, etc.) to increase entropy. However, as we believe, such password requirements rarely increase the entropy of the key. A competent intruder can consider password restrictions imposed by the security policy when compiling the hash code tables to hack the system. Alternatively, he or she can simply spy a password: the operator will write down a complex password and carry it.

According to the experimental evidence, there is a high percentage of first-kind errors (incorrectly typed passwords) under complication, even for a fairly simple password. Therefore, when determining a password protection security policy, the effect of first-kind errors on the system availability must be considered, which automatically restricts the frequency of password changing and its complexity.

In practice, biometric authentication methods have shown first-kind errors several times worse than the theoretical ones ($\leq 10^{-2}$), in typical working conditions and under operator's complication. Based on the testing results, the most promising biometric method is facial recognition. However, even this method has a high error rate, so it should not be combined with a blocking security policy. We propose using multifactor authentication where biometrics is combined with a password or a token. In the case of multifactor authentication, note that biometric and password protection have approximately the same entropy of the key. For passwords, the entropy is restricted by human memory capabilities; for biometrics, by the current hardware implementation of biometric scanners and sensors.

Using a token eliminates the problem of remembering passwords, but the user must have a physical carrier with him or her. Sometimes, this approach is inconvenient because the token can be stolen, copied, or lost.

Finally, we arrive at the following conclusion. For the authentication of I&C system operators, it is possible to build a protection system using different methods and their combinations. As a rule, I&C system operators work in the room with controlled physical access. Therefore, within the controlled security area, it is possible to establish a token-based access procedure with additional video monitoring by the security service. As we believe, a promising approach for industrial control systems is to implement multi-factor authentication: token or password protection for blocking authentication jointly with biometric authentication by the face geometry with a non-blocking security policy.

REFERENCES

1. *GOST* (State Standard) *R 58833-2020: Information Protection. Identification and Authentication. General Provisions*, 2020.
2. Iskhakov, S.Yu., Shelupanov, A.A., and Iskhakov, A.Yu., Engineering of Imitation Model of a Complex Network of Security Systems, *Proceedings of TUSR University*, 2014, vol. 32, no. 2, pp. 82–86. (In Russian.)
3. Dierks, T. and Rescorla, E., The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, 2006.
4. Conte de Leon, D., Makrakis, G.M., and Kolias, C., Cybersecurity, in *Resilient Control Architectures and Power Systems*, Rieger, C., Boring, R., Johnson, B., and McJunkin, T., Eds., IEEE, 2022, pp. 89–111. DOI: 10.1002/9781119660446.ch7.
5. Hu, G., *On Password Strength: A Survey and Analysis*, Springer International Publishing, 2018. DOI: 10.1007/978-3-319-62048-0_12.
6. Mengazetdinov, N.E., Poletykin, A.G., Promyslov, V.G., et al., *Kompleks rabot po sozdaniyu pervoi upravlyayushchei sistemy verkhnego blochnogo urovnya ASU TP DLYA AES «BUSHER» na osnove otechestvennykh tekhnologii* (Works on Creating the First Upper-Unit Control System of the I&C System for Busher NPP Based on Domestic Technologies), Moscow: Trapeznikov Institute of Control Sciences RAS, 2013. (In Russian.)
7. O'Gorman, L., Comparing Passwords, Tokens, and Biometrics for User Authentication, *Proceedings of the IEEE*, 2003, vol. 91, no. 12, pp. 2021–2040. DOI: 10.1109/JPROC.2003.819611.

8. Dworkin, M., Barker, E., Nechvatal, J., et al., *Advanced Encryption Standard* (*AES*), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, 2001. DOI: 10.6028/NIST.FIPS.197.
9. Jobusch, D.L. and Oldehoeft, A.E., A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 1, *Computers & Security*, 1989, vol. 8, iss. 7, pp. 587–604. DOI: 10.1016/0167-4048(89)90051-5.
10. The 200 Worst Passwords of 2021 Are Here and Oh My God. https://gizmodo.com/the-200-worst-passwords-of-2021-are-here-and-oh-my-god-1848073946 (Accessed March 7, 2022.)
11. Most Common Passwords of 2021. https://nordpass.com/most-common-passwords-list/ (Accessed March 7, 2022.)
12. Köhler, D., Klieme, E., Kreuseler, M., et al., Assessment of Remote Biometric Authentication Systems: Another Take on the Quest to Replace Passwords, *2021 IEEE 5th International Conference on Cryptography, Security and Privacy* (*CSP*), 2021, pp. 22–31. DOI: 10.1109/CSP51677.2021.9357504.
13. Alanezi, N.A., Alharbi, N.H., Alharthi, Z.S., and Alhazmi, O.H., POSTER: A Brief Overview of Biometrics in Cybersecurity: A Comparative Analysis, *2020 First International Conference of Smart Systems and Emerging Technologies* (*SMARTTECH*), 2020, pp. 257–258. DOI: 10.1109/SMARTTECH49988.2020.00067.
14. Antonova, V.M., Balakin, K.A., Grechishkina, N.A., and Kuznetsov, N.A., Development of an Authentication System Using Voice Verification, *Information Processes*, 2020, vol. 20, no. 1, pp. 10–21. (In Russian.)
15. Machine Learning Masters the Fingerprint to Fool Biometric Systems: https://engineering.nyu.edu/news/machine-learning-masters-fingerprint-fool-biometric-systems (Accessed July 12, 2022.)
16. *GOST* (State Standard) *R 52633.0-2006*: *Requirements for High-Security Biometric Authentication Means*, 2006.
17. Mao, W., *Modern Cryptography: Theory and Practice*, Prentice Hall, 2003.
18. Burrows, M., Abadi, M., and Needham, R.M., A Logic for Authentication, *DEC System Research Center Technical Report* no. 39, 1989.
19. Krawczyk, H., Bellare, M., and Canetti, R., HMAC: Keyed-Hashing for Message Authentication, *RFC 2104*, 1997.
20. Algorithms for Challenge/Response Authentication. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/4d1a2cb0-0951-462a-8582-121fd1afe28e (Accessed March 7, 2022.)
21. Iskhakov, A.Yu., Two-Factor Authentication System Based on QR-Codes, *IT Security (Russia)*, 2014, vol. 21, no. 3, pp. 97–101. (In Russian.)
22. Giri, D., Sherratt, R.S., Maitra, T., and Amin, R., Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices, *IEEE Transactions on Consumer Electronics*, 2015, vol. 61, no. 4, pp. 491–499. DOI: 10.1109/TCE.2015.7389804.
23. Razaque, K.K., Myrzabekovna, S.Y., Magbatkyzy, M., et al., Secure Password-Driven Fingerprint Biometrics Authentication, *2020 Seventh International Conference on Software Defined Systems* (*SDS*), 2020, pp. 95–99. DOI: 10.1109/SDS49854.2020.9143881.
24. Eastlake, D. and Jones, P., US Secure Hash Algorithm 1 (SHA1), *RFC 3174*, 2001.
25. Dinca, L. and Hancke, G., User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks, *Entropy*, 2017, vol. 19, no. 2. DOI: 10.3390/e19020070.
26. Fouque, P.-A., Pointcheval, D., and Zimmer, S., HMAC Is a Randomness Extractor and Applications to TLS, *Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security* (*ASIACCS'08*), Tokyo, Japan, 2008, pp. 21–32.
27. Jain, A.K., Deb, D., and Engelsma, J.J., Biometrics: Trust, but Verify, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2021. DOI: 10.1109/TBIOM.2021.3115465.
28. Alsellami, B., Deshmukh, P.D., and Ahmed, Z.A.T., Overview of Biometric Traits, *2021 Third International Conference on Inventive Research in Computing Applications* (*ICIRCA*), 2021, pp. 807–813. DOI: 10.1109/ICIRCA51532.2021.9545069.

This paper was recommended for publication
by A. O. Kalashnikov, a member of the Editorial Board.

Received May 6, 2022, and revised June 30, 2022.
Accepted July 11, 2022

Author information

Promyslov, Vitaly Georgievich. Cand. Sci. (Phys.–Math.), Trapeznikov Institute of Control Sciences, Moscow, Russia
✉ vp@ipu.ru

Semenkov, Kirill Valer'evich. Cand. Sci. (Phys.–Math.), Trapeznikov Institute of Control Sciences, Moscow, Russia
✉ semenkovk@ipu.ru

Mengazetdinov, Nadyr Enverovich. Senior Researcher, Trapeznikov Institute of Control Sciences, Moscow, Russia
✉ mengazne@mail.ru

Cite this paper

Promyslov, V.G., Semenkov, K.V., and Mengazetdinov, N.E., Assessment of Operator Authentication Methods in Industrial Control Systems. *Control Sciences* **3,** 34–45 (2022). http://doi.org/10.25728/cs.2022.3.4

Original Russian Text © Promyslov, V.G., Semenkov, K.V., and Mengazetdinov, N.E., 2022, published in *Problemy Upravleniya*, 2022, no. 3, pp. 40–54.

Translated into English by *Alexander Yu. Mazurov*,
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com

DOI: http://doi.org/10.25728/cs.2022.3.5

THE SIMULTANEOUS START OF ACTIONS IN A DISTRIBUTED GROUP OF AUTOMATIC DEVICES: A DECENTRALIZED CONTROL METHOD WITH A SIGNAL REPEATER

G.G. Stetsyura

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

✉ gstetsura@mail.ru

Abstract. This paper proposes a method for accelerating decentralized synchronization processes in the distributed control of a group of stationary or mobile automatic objects. With this method, the objects pass to specified states or affect the environment simultaneously or with required time delays. Some examples of such objects include actuators, computers in a computing cluster, distributed data processing facilities in supercomputers, and mobile robots. The object's action depends on the current state of all objects and the environment. The actions should start with minimum delay after detecting the possibility to perform them. Arbitrarily located sources of executive commands and their receivers are synchronized by exchanging signals and messages between objects through an intermediary (a signal repeater). Means are used to accurately measure the time intervals of signal transfer between each object and the repeater. Group operations are used to accelerate synchronization processes. These operations involve a large number of objects simultaneously. The object's data are used in operations simultaneously. Data are processed during their transmission without extra time. Operations are executed by network devices of the system objects and the common network device without any computing facilities (the repeater).

Keywords: simultaneous start of group operations, decentralized control, synchronization of mobile objects, fast distributed intranet computing, multilayer synchronization.

INTRODUCTION

In this paper, we accelerate the decentralized control of starting joint actions in a distributed group of digital objects: computers in a computing cluster, distributed data processing facilities in supercomputers, mobile robots, and actuators affecting an environment.

The problem statement is as follows. Consider a distributed group of sources that jointly create a common command and send it to a distributed group of receivers (command executors). The objects in the groups have an arbitrary arrangement, can change their location, and communicate through a network. Having a command, all receivers must perform the corresponding actions simultaneously or with the time delays specified for each receiver in the command. The time instant of command sending is unknown in advance and depends on the current state of all objects and the environment. The objects should start the actions with the minimum possible delay after the sources send the parts of the command. When objects operate in a distributed control system, it is also important to reduce the delay with which system objects form a common command. All objects, sources and receivers, must act without centralized control.

The solution of this problem consists of two parts: for the sources and receivers of the command, respectively. The actions of sources were presented in the author's previous publications and are briefly described in Section 3 below. We introduce an additional communication link for objects, the signal repeater *RS*. This is a simple device without computing facilities and even logical elements. Receiving signals of objects at some frequencies, *RS* just retransmits them to objects at other frequencies. It cannot generate commands and therefore does not serve as a control center. Receivers have signals only from *RS*. Due to the use of *RS*, we establish the following key results.

With the proposed synchronization of object actions, sources send messages to *RS* with the simultaneous arrival of the same-name binary digits of all messages. For receivers, *RS* acts as a single source replacing the previous group of sources. Now objects must consider only changes in their distances to *RS*. Sources send messages to a single receiver (*RS*). Receivers have messages from *RS* only. This approach simplifies the network facilities and reduces the command execution time. By adding *RS*, we eliminate interference from source signals coming to the receivers. Without *RS*, signals from a group of sources, even sent simultaneously, would arrive at the receivers as interference at different, almost uncontrollable, time instants.

This paper considers group operations and commands executing distributed control and computational operations in a time independent of the number of objects (the simultaneous participants of the operation). As shown below, distributed object computers execute group operations at high speeds due to *RS*.

To solve this problem, it is necessary to determine the transfer time of signals between objects and *RS*. Many solutions have been developed in different technical fields. For this paper, the most useful results are two standardized solutions for the clock synchronization of distributed objects and high-precision measurement of distances between objects. The IEEE 1588-2008 Precise Time Protocol (PTP) [1] is widely used in the industry. In PTP, signal transfer times are measured to synchronize the clocks of objects. Depending on the application, the accuracy varies from tens of microseconds to eight nanoseconds. Within the White Rabbit (WR) project [2, 3], picosecond methods were developed for measuring signal transfer times between objects in accurate physical experiments at CERN. The IEEE 1588-2019 High Accuracy Default PTP Profile (HA) [4] is a novel standard combining both solutions. In PTP and WR, objects interact in the master-slave mode. Both PTP and WR can operate on large networks.

PTP and WR solutions are applied below with some modifications due to the problem statement. This paper considers intensive data exchange between objects to control their actions and perform distributed computations, requiring small delays in data delivery. Therefore, the matter concerns only the systems in which the distances between objects vary from fractions of a meter to several hundred meters.

The solutions proposed below are oriented to tasks with the unpredictable execution time of commands by receivers, so the clock is not applied. There is no master object, and all objects have equal rights.

The presence of *RS*, an additional device between objects, raises the natural question of reducing the fault tolerance of the system. Due to the simplicity of *RS*, the number of such additional devices can be increased to replace the failed ones. In addition, the *RS* functions can be transferred to any object. This paper does not discuss the issues of fault tolerance.

At the beginning of the Introduction, we have mentioned different digital objects to apply the methods. However, many technicalities need to be specified for a particular object. For example, many mobile objects require communication only by exchanging non-directional radio signals through a single *RS*. In a supercomputer, it is reasonable to apply directional optical communications with signal switching through thousands of simultaneously accessible *RS*s. In each of these cases, the methods described below remain the same.

This paper is organized as follows. Section 1 outlines the principles of time measurement in PTP and WR useful for further considerations. The communication structure to synchronize the actions of sources and receivers of commands is described in Section 2. Section 3 presents a method for receivers to execute source commands simultaneously or with the time delays specified in the command for each receiver. In Section 4, we introduce a distributed control method for source interactions. Section 5 considers the multilayer synchronization of command execution by receivers. Having executed a command, the receivers of a layer become command sources for the next layer of receivers. In Section 6, a summary of group operations is given. Section 7 shows the connection between the network operations proposed in the paper and the operations of associative computing facilities.

1. TIME INTERVAL MEASUREMENT IN PTP AND WR

The basic scheme for measuring time intervals in PTP is shown in Fig. 1*a*.

Here two objects interact, conventionally termed a master and a slave. At a time instant t_1, the master sends to the slave a signal to start synchronization and its clock time. This message arrives at a time instant t_2. At a time instant t_3, the slave sends the master a reply

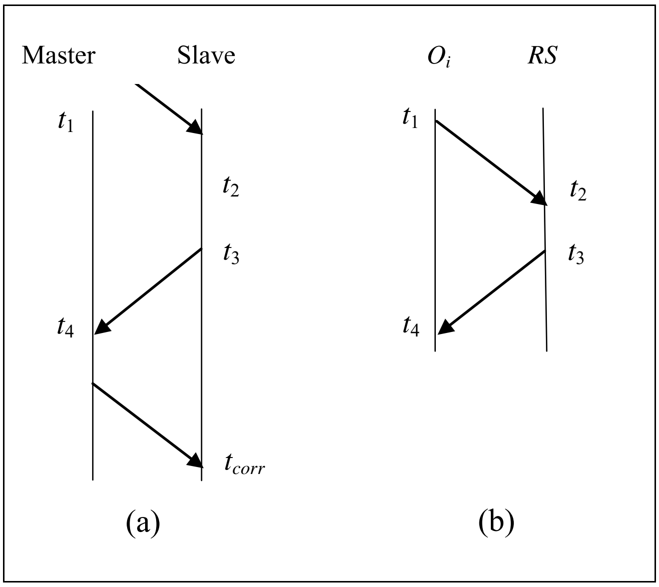

Fig. 1. Time measurement in PTP: the basic scheme and its simplified version.

signal and its new clock time. At a time instant t_4, the master receives the slave's reply, determines the distance between this pair of objects, determines the distance to the slave, and reports it to the slave. The slave corrects the clock time. Except for several important details, this is the basic time correction scheme in PTP.

For this paper, we need a simplified version of the measurement scheme (Fig. 1*b*) without clock but with a signal repeater (*RS*). For optical signals, a passive retroreflector can be used as *RS*. An arbitrary object O_i launches its timer, sending a signal to *RS* at a time instant t_1. The signal arrives at the *RS* at a time instant t_2. After the triggering delay of *RS*, the signal is sent to *RS* at a time instant t_3. At a time instant t_4, the object O_i determines the signal transfer time between O_i and *RS* as $T_{OiRS} = t_4 - t_1 - (t_3 - t_2)$.

WR uses a more accurate phase method for measuring time intervals. In [5], a simple electronic device was proposed to measure the signal transfer time between objects. The femtosecond accuracy was achieved. Below, this method can be applied directly or to control the stability of all objects participating in the measurement process.

2. COMMUNICATIONS BETWEEN COMMAND SOURCES AND RECEIVERS

Figure 2 shows the structure of communications to exchange signals and messages between command sources and receivers.

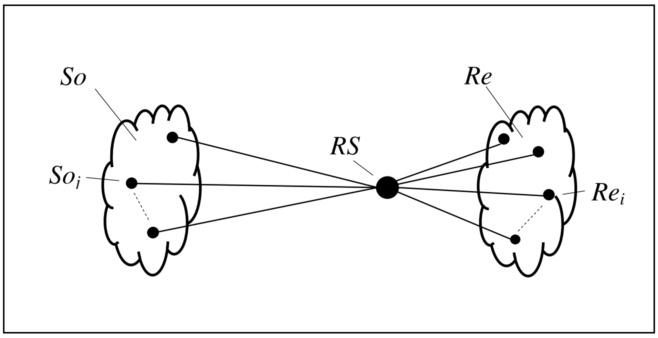

Fig. 2. Communications between command sources and receivers.

The object system includes a group *Re* of command receivers $\{Re_i\}$, a group *So* of command sources $\{So_j\}$, and a repeater *RS* of signals coming from sources and receivers. Up to Section 4, we assume that only one arbitrary source from *So* sends a command to receivers from *Re*. The source sends the command signal to *Re* indirectly (through *RS*). The bit "1" of the command code is sent to *RS* on a carrier frequency f_1; the bit "0," on another frequency f_0. The repeater translates these signals into other signals $^*f_1$ and $^*f_0$, respectively, and sends them to receivers. The signals do not change during WR operations. As noted in the Introduction, objects receive only the signals transmitted by *RS*.

Therefore, *RS* is a simple device without logical elements. It does not actively participate in the control of objects' actions.

RS underlies the synchronization approach proposed in this paper. In addition, *RS* reduces the amount of transferred data and time required for Re_i to organize the synchronous execution of the command. As noted in the Introduction, the problem solution will be time-consuming without collecting messages in a single point (*RS*). These features are discussed in detail below.

Communications between objects can be wireless or wired. Wireless communications offer additional capabilities. For example, only wireless communications are acceptable for mobile objects. In stationary supercomputers, wireless communications between a group of objects and a group of *RS*s allow quickly reconfiguring the system when solving a single task. They also simplify system recovery in case of *RS* failures. They eliminate the duplication and triplication of repeaters. For example, if there is at least one redundant repeater, objects will switch to it without intermediate switches in case of failure. A failure can be detected due to the broadcast transmission of the logical scale accessible to all objects simultaneously (see Section 4).

3. SYNCHRONIZED COMMAND EXECUTION BY RECEIVERS

This section presents an accurate synchronization method for receivers (command executors) with the communication scheme in Fig. 2. Before receiving an executive command to start the synchronized execution of the corresponding actions, each receiver gets a description of its action in a preliminary command. Such commands can be sent by different sources in random order or as a single message consisting of messages from individual sources. This method is discussed in Section 4.

Before implementing the executive command, each receiver must measure the transfer time of the signal (optical or radio signals having the speed of light c) between the receiver and RS (the distance to RS). We propose a procedure with additional frequency channels in which measurements can be performed independently and simultaneously with other communications between objects.

The first task of the receivers is to launch the time without involving a special control center, which sets the order of measurement for them. For this purpose, the receivers from Re need to determine the distance to RS, and they send a special synchronization signal S to RS. The signal duration must be at least T (the greatest signal transfer time between RS and any receiver). A receiver sends the signal S only when not receiving the signal S sent by other sources and returned from RS. If the signal duration is not smaller than T, the individual signals S of different objects are superimposed in the common signal S of variable duration. The repeater converts S into a single signal S_{rs} and transmits it to receivers Re.

The time instant when the signal S_{rs} is completely received is treated by the receiver as the signal ${}^{*}S_{rs}$ to start synchronization. This signal is created without any control center; also, see the paper [6]. Let the receivers from Re be numbered. The object Re_i with the smallest known number i (e.g., $i = 1$) measures its distance to RS. All receivers do the same. This process can be performed continuously and simultaneously with other interaction processes of the objects. Some versions of this action were considered in the paper [6]. In particular, suppose that high synchronization accuracy is not required (the time intervals of a duration below T are indistinguishable). Then the objects may exchange signals directly without RS.

Upon measuring their distances T_i to RS, the receivers Re_i will start the synchronous execution of the source command. To do this, each receiver follows several steps described below.

Step 1. The receiver Re_i calculates the delay $d_i = C – T_i + a_i$. Here $C \geq T$, and $a_i \geq 0$ is an additional time delay for Re_i (possibly zero). The value $C \geq 0$ is used to consider the time cost of additional object actions.

Step 2. Upon receiving a command, each Re_i will perform the command actions with the delay d_i.

Leaving RS, the command will arrive at Re_i after the time T_i. Hence, given the delay d_i, any Re_i performs the action at the time instant $\tau = T_i + C – T_i + a_i = C + a_i$. All Re_i will perform the command simultaneously at the time instant C after the command leaves RS or with the delays a_i, as required.

Thus, after the command leaves RS, all objects will pass to synchronous execution at the time instant of its delivery to the farthest object from RS. If all objects know $T_{\max}$ (the signal transfer time between RS and the farthest object), and it is acceptable to replace C with $T_{\max}$, the transition to the synchronous state will occur in the minimum possible time.

Now we determine the time instant of measuring T_i by receivers Re_i. Recall that the measurement procedure is continuous. Hence, we can select the last measurement before receiving the command by the object. But it is possible to take the measurement when the receiver gets the command. If all Re_i know the time for determining the values T_i and d_i, then it suffices to set an upper bound on this time for all Re_i so that the receivers correct possible time variations.

The accuracy of measuring T_i can be significantly improved by the following method, oriented to tough time requirements. (They are necessary to coordinate computers in receivers Re_i.) In this method, Re_i will also measure the distance to RS after the other receivers complete their measurements. But all these measurements are performed within one common message for all receivers. In this message, each Re_i has a very short time interval Δt for the measurement.

We make several assumptions. First, before applying the proposed method, receivers Re_i determine the time intervals T_i and calculated the values d_i. Second, the constant C is given; in the best case, $C = T$ [6]. Third, each Re_i is allocated a time interval Δt_i of the same duration Δt to recalculate T_i. The method includes the following steps.

Step 1. As described above, receivers Re_i send the signal S to RS and receive the signal S_{rs} back. By the signal ${}^{*}S_{rs}$ (the completion of S_{rs}), each Re_i sends to RS the test signal δt of a duration smaller than Δt, placing δt in the center of Δt_i. Note that each Re_i does this alternately on i within its interval Δt_i.

Step 2. Since all Re_i know the value Δt, they will send their Δt_i in one common message SC of duration $n\Delta t$, where n is the number of receivers.

Step 3. The signals δt of the message SC arrive at RS. Here, they are converted to ${}^*\delta t$ and then returned to receivers. Receiver Re_i determines the new value T_i by the shift δt within Δt_i.

The method is effective under two conditions. First, the signal δt must not leave Δt_i for any displacement of Re_i. Second, the duration $n\Delta t$ must be smaller than that of the previous method for determining T_i (with a group of individual messages). Let us demonstrate that both conditions hold.

For stationary Re_i without any external impacts, the signal δt is in the center of Δt for any T_i. Otherwise, δt is shifted.

Let L be the maximum distance between RS and any Re_i, and v be the maximum speed of Re_i. Then during the measurement time T_i, the receiver will move at the distance ${}^*L = T_i v$. The signal δt will shift within Δt by no more than the time interval ${}^*\Delta t = {}^*L/c = T_i\, v/c$. The interval Δt must be at least $2{}^*\Delta t$ for δt not to move to the adjacent interval Δt. The entire measurement cycle for n receivers will be done in the time $2n\mathrm{T}_i\, v/c << nT_i$. Allocating a separate frequency channel for each Re_i will eliminate the dependence on n and reduce the admissible time of measuring the distance to RS for the entire group Re.

The solutions described above ensure minimum delay when executing the command sent to the receivers. Indeed, RS (if exists) acts as the only source of the command. The receiver measures the distance to RS before getting the command, and there is no delay at the beginning of its execution. Next, each receiver has to start executing the command only when all receivers get it, delaying the execution due to its distance to RS. As shown in this section, the receivers have all the necessary information for this in advance; upon getting the command, the receiver starts its execution with the corresponding time shift. Thus, the presence of RS eliminates command execution delays. Delays inevitably occur without RS.

If a group of sources forms a common command without RS, then their simultaneous actions are achieved only by replacing RS with one of the sources (the leader). The leader will act as RS. Such a process takes unacceptably much time.

In Section 4, sources send messages to receivers only via RS, adjusting the message arrival at RS depending on their distance to RS. Acting like receivers, the sources determine the distance to RS and then send messages so that they reach RS at the same time or in a given order. The sources determine the distance to the RS in advance, and a common command will be formed without delay, e.g., using the solutions of Section 6.

The method for measuring signal transfer (PTP, WR) without changing the paper's solutions can be replaced by another known method. Thus, in all cases, the presence of RS minimizes the delay when executing a common action of all receivers.

We have described the synchronized execution of commands in the case of a single RS sending signals to all receivers. Section 5 considers a more general problem. But first, in Section 4, we discuss the joint synchronous actions of a group of sources.

4. SYNCHRONOUS ACTIONS IN A GROUP OF SOURCES

The synchronous actions of a group of sources were considered in [6]. They are used repeatedly in this paper. A summary of such actions that corresponds to Section 3 is given below.

Similar to the actions of receivers, in Section 3 the sources organize their actions as follows. Sources So_j from the group So, ordered by j, send the signal S to RS. In response, RS sends the signal S_{rs} and the signal ${}^*S_{rs}$ (the sign of completing S). Then sources So_j alternately determine the distance to RS and calculate the delays $D_j = C - t_j + a_j$, by analogy with d_i, C, T_i, and a_i from Section 3. Now the sources can synchronously send messages to RS (and commands to receivers) without any control center.

To describe further actions of the sources, we introduce a logic scale LS, i.e., a sequence of bits equal to the number of sources in So. Let source So_j need to transmit a message to RS. This source enters one into the jth bit of the scale LS and transmits it to RS using the signal f_1. The other bits of LS may not contain binary values, or So_j enters zero into them and transmits it using the signal f_0. In the second case, several signals f_1 and f_0 arrive at RS (and further at Re_i) simultaneously from different sources. They are perceived as a pair of signals in some operations of Re_i but as the signal f_1 in most operations.

To start interacting with RS, the sources send to RS the signal S and gent the signals S_{rs} and ${}^*S_{rs}$ in response. After that, the sources send their scales LS to RS with the delays D_j and get a combined scale ${}^*LS$, with the same-name bits of all scales received by RS. Now So_j can send their messages to RS in a given order without delays on the sources not requesting message transmission.

Thus, we have obtained a useful result. The sources order their messages by sending them to RS. Now RS acts as a single source, sending messages-commands from RS to receivers. At the same time, sources can be receivers to coordinate joint actions. In particular, So_j can acknowledge the agreement of the entire group So to execute a command sent to Re. As shown in Section 6, besides signal repeat, RS can also execute several operations distributed among the members of *So* without logical elements.

In contrast to the synchronous actions of objects, there is no possibility to specify the occupation time of *RS* for the asynchronous actions of objects. In this case, we apply barrier synchronization [7]. When executing a common operation, one or more objects send a signal *B* that is accessible to all objects and differs from all other signals. When some object completes its work within the common operation, it stops transmitting the signal *B*. When all objects do so, the transmission of the signal *B* stops. In the absence of this signal, other objects can start the next operation. Without these actions, the value *C* will be chosen unreasonably large for the asynchronous operations of objects. The operations of sources (Section 4) are used in the next section for the multilayer synchronization of actions in *Re*.

5. MULTILAYER SYNCHRONIZATION FOR GROUPS OF RECEIVERS

In contrast to Section 3, here the group of objects is divided into subgroups (layers) Le_1, Le_2, ..., Le_n (Fig. 3). Within a layer, objects act as discussed in the previous sections. The signals they exchange are inaccessible to the objects of other layers. But the repeaters *RS* of the layer controlled by layer objects can merge with the repeaters *RS* of the next layer. The first layer of receivers gets source commands directly from *So* of the layer (Section 3). Then the group *Re* of first-layer receivers through its repeater acts as a group of sources for second-layer receivers, coordinating their actions as described in Section 4. For this purpose, the repeaters *RS* of these layers act jointly: the second-layer repeater transmits first-layer signals to second-layer objects and sends second-layer signals to the first layer. Next-layer receivers act in the same way. In the simplest case, last-layer receivers need to act synchronously with respect to external objects. In the more complex case, the computers of receivers and computers of sources in a layer exchange messages through their *RS*s, which are simultaneously accessible to all these objects and should be used to correct their actions. Hence, additional time is required. Let us start with the simplest process (process 1).

Process 1. The objects are divided into *k* layers, $k = 0, ..., n$. The receivers of layer *k* interact with the receivers of layer $k + 1$ by switching to the source mode. The new sources of layer *k* act as described in Section 3, synchronizing the receivers of layer $k + 1$.

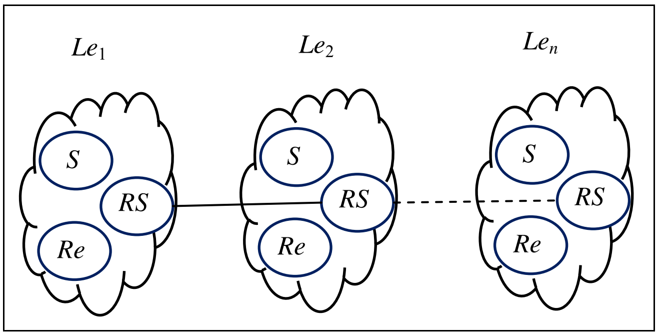

Fig. 3. Multilayer synchronization of groups of receivers.

Moving from layer to layer, this process reaches the layer whose receivers are to be synchronized. The synchronization will be done. The intermediate layers are forbidden to perform any external actions.

If the receivers of all layers are required to perform external actions simultaneously without *RS* with the same time *C* for all layers, then we use process 2. (It complements the actions of process 1.)

Process 2. Upon getting a command, the receivers of arbitrary layer $k \leq n$ repeatedly calculate the value $F = n – k$, increasing *k* by one. In each iteration, the value *F* is calculated with the delay *C*.

If $F = 0$, the receivers of the layer will perform an external action. In the first iteration (for layer $k = 0$), we obtain $F = n$; for layer $k = 1$, $F = n – 1$, and so on. As a result, the receivers in all layers will get $F = 0$ when the last layer receives the command. They will simultaneously perform the external action.

Besides external actions, the computers of layer *k* objects may need data and command exchange as well as distributed computations. For this purpose, they use the common resource RS_k. Suppose that an upper bound $^*C$ can be specified for the occupation time of this RS_k by layer objects. Then the occupation time is considered by replacing *C* with $^*C$ if the layers work alternately.

In the presence of asynchronously acting objects, the following two-phase synchronization process yields the best result.

The synchronization preparation phase. In this phase, the data are asynchronously prepared for transmission to the receivers by first-layer sources. All actions are performed using barrier synchronization (Section 4). If necessary, first-layer receivers also asynchronously form additional data to prepare actions as second-layer sources. The transition to second-layer actions is performed by the barrier synchronization signal. All layers perform their work alternately. All layers do not need to perform external actions simultaneously. (This is the aim of the next phase.)

The synchronization phase. The process is similar to process 2, but all layers are renumbered in the reverse (the last layer n has number 0). The objects of the layer with the new number $k = 0$ act as sources and start synchronizing the receivers of all layers. Upon getting the command, the objects repeatedly calculate the value* $F = n - k$, increasing k by one, with the delay $^{**}C$. When $F = 0$, the receivers in all layers simultaneously perform the external action.

The synchronization phase is faster: the objects just pass the command to the previous layer. Therefore, $^{**}C < C$. In the synchronization phase, a feedback link is additionally introduced to pass the results of computations of the next layers to the previous ones.

Thus, we have obtained the following result. The objects synchronize their actions and perform them simultaneously in all layers of the multilayer structure without any control center.

6. A SUMMARY OF THE GROUP OPERATIONS PERFORMED ON THE NETWORK

We summarize the group operations considered in the paper as a means of group interaction of objects. Several operations were developed for this paper; others were introduced by the author earlier and adapted for the purposes of this paper. The operations listed below were developed at different times at Trapeznikov Institute of Control Sciences, the Russian Academy of Sciences (ICS RAS). The following text thoroughly describes the basic principles of group operations without addressing the primary sources.

The main properties of operations are as follows. Input data for an operation come simultaneously from a group of distributed objects (data storage devices). These data are processed simultaneously during their transmission without increasing the data transfer time. Operations are performed in network facilities of the object system without using computers and other computing devices. The time to obtain the result does not depend on the amount of data processed.

These results are a consequence of coordinating object actions through message synchronization processes. Regardless of the current arrangement and location of objects, their actions are synchronized by allocating a special object (signal repeater *RS*) for the groups. A group of messages is synchronously delivered to one object *RS* and subsequently forwarded to a group of receivers as a single common message for all sources. This is performed quite simply and quickly. But this message arrives at a group of randomly located receivers at different times. Using *RS*, the receivers introduce appropriate delays and simultaneously perform the required group action. According to the previous sections of the paper, the above properties hold for all **object action control operations**: the synchronization of sources, the synchronization of receivers, multilayer synchronization, the elimination of access conflicts, and barrier synchronization.

In addition, we list distributed **computational operations**: search for maximum and minimum, the bitwise logical AND and OR operations, and the analog-digital operations of counting, addition, and subtraction. These operations are not used here, but they accelerate system control when searching for objects with given properties and estimating the system state. They were described, e.g., in the paper [7]. Let us outline their operating principle.

To determine the maximum, objects send numbers in the binary representation, transmitting the highest digit at the first step. The next digit is transmitted only by the objects that transmitted one before, and so on. Hence, the maximum of the transmitted numbers remains. Replacing ones with zeros determines the minimum. It is possible to switch from the binary representation to other number systems if the digits of a number are represented by a scale in which all digits contain zeros, except for the digit corresponding to the digit value.

The bitwise AND and OR operations allow quickly estimating the state of all system objects. For this purpose, the object state is described by a scale, i.e., a sequence of binary digits equal to one if the corresponding attribute is present and zero otherwise. Ones and zeros are transmitted on the signal frequencies f_1 and f_0, respectively. The state of all objects is estimated with the simultaneous transmission of the scales to *RS* and combining same-name digits of object sequences in *RS*. When the AND operation is performed, the presence of f_0 in the scale digit of *RS* means that at least one object does not have the corresponding feature. Otherwise, the feature is inherent in all objects. For the OR operation under the same conditions, the presence of f_1 means that at least one object has the corresponding feature. Otherwise, the feature is absent in all objects.

To perform analog-to-digital operations, *RS* contains an analog-to-digital converter (ADC). Let the objects characterize their state with a scale (a sequence of attributes represented by zeros and ones). If objects send their scales to *RS* with combining same-name digits, then ADC will estimate the total energy of received signals and yield a value reflecting the presence of an attribute for all objects. This value will be received simultaneously by all objects. Combining such operations with the bitwise AND and OR operations allows estimating the state of the object system more accurately. The addition and subtraction of numbers in a non-binary number system were described in [7]. In these operations, the digits of numbers are represented by scales with one only in the digit of the scale corresponding to the digit value. The result also does not depend on the number of objects participating in the operation.

ADC operations require optical signal sources with stable energy. Modern technology allows obtaining an accurate digital value at the simultaneous summation of several thousands of signals. In [8], a simple LED source with an output power stability below 50 ppm/ºC was presented.

7. THE SOLUTIONS PROPOSED IN THIS PAPER: GENERAL ANALYSIS

The main results of this paper have been obtained with distributed group operations not used in known network systems. Their counterpart is associative operations proposed in the 1960s for concentrated associative computers. The associative operations are performed according to the following enlarged scheme.

In associate computers, the control center simultaneously sends a common command to a group of associative computer nodes with associative memory. The nodes perform the required actions. Their result is accessible to other nodes. It simultaneously comes to the center, which forms the next command based on the received results, and so on. The main application of associative computers was hard real-time control systems. An example is the STARAN associative supercomputer, which controlled aircraft movements at the J.F. Kennedy International Airport (New York, the USA). The group operations described in the paper can be considered a variant of associative operations with the following peculiarities. The operations are distributed and are executed directly in a simple network facility (a repeater). The repeater has no computing facilities; nevertheless, it executes all these group operations and serves for managing object interaction and simultaneously estimating the state of all objects. All types of object interaction described above are performed in a decentralized way without any control center. Thus, the structures proposed in the paper have both network and associative capabilities.

Note that at present, many researchers study networks executing message transfer and other functions (data transport management and distributed computing [9–12]). However, these important R&D works differ from those carried out in ICS RAS: new functions are performed by computers of network facilities, whereas group operations are not used.

CONCLUSIONS

This paper has proposed a decentralized control method for the simultaneous start of actions in a distributed group of stationary or mobile automatic objects. With this method, the objects start their actions with the minimum delay at an a priori unknown action instant.

The simultaneous start of actions in a group of objects with an a priori known action instant is successfully implemented in the IEEE 1588-2019 standard. Thus, the scope of this standard has been extended to real-time control systems by adding to the capabilities to start actions at an a priori unknown instant.

Due to network group operations, the proposed method has a fast response to emerging events.

REFERENCES

1. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, *IEEE Std 1588-2008* (*Revision of IEEE Std 1588-2002*), 2008, pp. 1–269. DOI: 10.1109/IEEESTD.2008.4579760.
2. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, *IEEE Std 1588-2019* (*Revision of IEEE Std 1588-2008*), 2020, pp. 1–499. DOI: 10.1109/IEEESTD.2020.9120376.
3. Girela-López, F., López-Jiménez, J., Jiménez-López, M., et al., IEEE 1588 High Accuracy Default Profile: Applications and Challenges, *IEEE Access*, 2020, vol. 8, pp. 45211–45220.
4. Sliwczynski, Ł., Krehlik, P., Buczek, Ł., and Schnatz, H., Picoseconds-Accurate Fiber-Optic Time Transfer with Relative Stabilization of Lasers Wavelengths, *Journal of Lightwave Technology*, 2020, vol. 38, no. 18, pp. 5056–5063.
5. Moreira, P., Timing Signals and Radio Frequency Distribution Using Ethernet Networks for High Energy Physics Applications, *PhD Thesis*, University College of London, 2014. https://discovery.ucl.ac.uk/id/eprint/1461109/1/PMmoreira_PhD_Final-signed[1].pdf.
6. Stetsyura, G.G., Decentralized Autonomic Synchronization of Interaction Processes of Mobile Objects, *Control Sciences*, 2020, no. 6, pp. 47–56. (In Russian.)
7. Stetsyura, G.G., Network Information-Computing Support of Automatic Mobile Objects Interaction, *Automation and Remote Control*, 2019, vol. 80, no. 6, pp. 1134–1147. DOI: 10.1134/S0005117919060110.
8. Bosiljevac, M., Babić, D., and Sipus, Z., Temperature-Stable LED-Based Light Source without Temperature Control, *Proceedings of SPIE OPTO*, San Francisco, USA, 2016, vol. 9754, pp. 1–6. DOI: 10.1117/12.2211576.
9. Tennenhouse, D.L., Towards an Active Network Architecture, *SIGCOMM Comput. Commun. Rev.*, 1996, vol. 26, no. 2. http://ccr.sigcomm.org/archive/1996/apr96/ccr-9604-tennenhouse.pdf.
10. Zilberman, N., Watts, P.M., Rotsos, C., and Moore, A.W., Reconfigurable Network Systems and Software-Defined Networking, *Proc. of the IEEE*, 2015, vol. 103, no. 7, pp. 1102–1124.
11. In-Network Computing, ACM SIGARCH, 2019. https://www.sigarch.org/in-network-computing-draft/

12. Kim, D., Towards Elastic and Resilient In-Network Computing, *PhD Thesis*, Carnegie Mellon University, 2021. http://reports-archive.adm.cs.cmu.edu/anon/2021/CMU-CS-21-143.pdf.

*This paper was recommended for publication
by V.G. Lebedev, a member of the Editorial Board.*

*Received November 28, 2021,
and revised May 5, 2022.
Accepted May 19, 2022*

Author information

Stetsyura, Gennady Georgievich. Dr. Sci. (Eng.), Chief Researcher, Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ gstetsura@mail.ru

Cite this paper

Stetsyura, G.G. The Simultaneous Start of Actions in a Distributed Group of Automatic Devices: A Decentralized Control Method with a Signal Repeater, *Control Sciences* **3,** 46–54 (2022). http://doi.org/10.25728/cs.2022.3.5

Original Russian Text © Stetsyura, G.G., 2022, published in Problemy Upravleniya, 2022, no. 3, pp. 55–64.

Translated into English by *Alexander Yu. Mazurov*,
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com