

Elshan Hashimov^{1,2}, Ramil Akhundov², Aziz Talibov¹, Marko Radovanović³

¹Azerbaijan Technical University, Baku, Azerbaijan

²National Defense University, Baku, Azerbaijan

³Military Academy, University of Defence in Belgrade, Belgrade, Serbia

A RISK- AND TIME-BASED MODEL FOR PROCESSING INFORMATION FLOWS IN THE PHYSICAL PROTECTION OF SPECIAL-PURPOSE AND CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The effectiveness of a physical protection system depends not only on sensor sensitivity, barrier delay, and response-force readiness, but also on the timely, complete, and undistorted delivery of heterogeneous security data to the decision-making level. This study proposes an integrated risk- and time-based model for processing information flows in the physical protection of special-purpose and critical infrastructure facilities. The information environment is represented as a directed graph. Transmission, processing, and queuing delays are combined with completeness, accuracy, consistency, reliability, and cyber-resilience indicators. A partially non-compensatory information-quality index is developed by combining a weighted geometric mean with the weakest component and a time-decay factor. Information latency is explicitly embedded in the detection, delay, and response time balance, and analytical expressions are formulated for the probability of timely intervention and residual risk. A 10,000-run Monte Carlo experiment is performed for a hypothetical three-zone facility. The distributed backup route achieved an integral information-quality score of 0.849, compared with 0.782 for the centralized primary route and 0.590 for the congested and partially compromised route. In the insider-bypass scenario, the distributed route increased the probability of satisfying the time condition from 0.442 to 0.562 and the mean integrated interruption probability from 0.246 to 0.326. The proposed approach enables weaknesses in information channels to be evaluated jointly with physical barriers and allows information routes to be selected dynamically according to event risk and the time available.

Keywords: physical protection system; information flow; information latency; data fusion, risk; time sufficiency; critical infrastructure; partially non-compensatory model.

1. Introduction

Protecting special-purpose and critical infrastructure facilities is essential to the uninterrupted operation of energy, transport, communications, water supply, industry, defense, and public administration systems. At such facilities, a physical protection system integrates the detection of an adversary, the delay of adversary movement, and the timely intervention of response forces within a single organizational and technical framework. Under the classical approach, system effectiveness is assessed using the probability of detection, the delay created by physical barriers, and the time required for response forces to reach the scene [1, 2]. The widespread deployment of digital sensors, networked cameras, biometric access-control devices, unmanned surveillance platforms, and analytical software has shown that the interaction among these three functions depends heavily on the information infrastructure. If a sensor signal is not verified in time, an event is misclassified, or a command reaches the response force too late, the time reserve created by physical barriers may lose part or all of its operational value.

Within the information environment of a physical protection system, data about the same event arrive from heterogeneous sources. A perimeter radar provides the target coordinates and speed, a thermal camera supplies a heat signature, a video surveillance system provides visual features, an access-control system reports an identification result, and a security officer contributes contextual observations. These data differ in frequency, format, accuracy, and reliability. Processing them separately

increases the operator's information load, while combining them without proper correlation may produce contradictory decisions. More data do not automatically result in better situational awareness. On the contrary, a high false-alarm rate, repeated notifications, and multiple interfaces can delay the appearance of a critical signal in the overall information stream [3, 4].

The role of information flow in physical protection is defined by two interdependent properties. The first is information quality. Data used for decision-making must be complete, authentic, consistent, traceable, and resilient to cyber effects. The second is the time value of information. Correct information may be tactically useless if it arrives after the decision window has closed. An information channel therefore cannot be evaluated solely in terms of packet loss or availability. The entire route from source data to a decision and an actionable command must be considered, together with the route's latency and reliability and the time remaining in the event scenario.

Current regulatory and methodological documents require defense in depth and a balanced combination of detection, delay, and response functions in physical protection [2, 5]. The NIST approach to operational technology security emphasizes information-security requirements such as availability, integrity, monitoring, event logging, and network segmentation [6, 7]. Nevertheless, an important methodological gap remains at the intersection of physical protection and information processing. Information quality is often studied as a separate cyber-resilience problem, whereas time sufficiency is addressed as a separate physical protection

problem. Consequently, there is no unified indicator that measures how information latency reduces the time reserve created by physical barriers and influences the choice of an optimal route.

The purpose of this study is to develop a methodological approach for modeling the generation, transmission, processing, multisource fusion, assessment, and conversion of data into management decisions in the physical protection of special-purpose and critical infrastructure facilities using risk and time criteria. To achieve this purpose, the study formalizes the information environment as a directed graph; determines route latency and reliability; proposes a partially non-compensatory information-quality indicator; incorporates information latency into the time balance of physical protection; develops a criterion for event prioritization and alternative-route selection; and verifies the approach through scenario analysis and Monte Carlo simulation.

The scientific contribution of the study consists of three main results. First, the quality of an information route is assessed not only through an average indicator, but also by considering its weakest component and the loss of information value over time. Second, information-processing time is treated not as an external parameter of the detection, delay, and response model, but as an internal variable that directly reduces the available time reserve. Third, route selection is formulated as a multicriteria optimization problem involving information quality, residual risk, violation of the time condition, and resource consumption. This approach provides a quantitative basis for demonstrating that a bottleneck in an information channel can be as dangerous as a weak link in a physical barrier.

2. Literature review

The theoretical foundation of physical protection systems lies in the functional compatibility of detection, delay, and response. Garcia relates the effectiveness of a physical protection system to the probability that an adversary will be detected and stopped by response forces before completing a critical action [1]. The IAEA recommendations identify defense in depth, a graded approach proportional to the threat, assessment of detection alarms, and the integration of response measures as core principles [2, 5]. Wadoud et al. linked detection, delay, and response functions to probabilistic and temporal indicators when evaluating the physical protection of a nuclear facility [8]. Although these studies establish the time logic of physical protection, signal transmission through a communications network, queuing at processing nodes, and conversion into decision-relevant information are generally subsumed within an aggregated detection time.

In digital physical protection systems, sensors, software, communications, and actuating elements create cyber-physical interdependencies. IAEA Nuclear Security Series No. 42-G requires the integrity and availability of computer-based systems that perform nuclear security functions to be protected [5]. NIST SP 800-82 Rev. 3 emphasizes real-time requirements, high availability, deterministic response, continuous monitoring, and risk-informed network architecture in

operational technology environments [6]. NIST SP 800-160 Vol. 2 Rev. 1 presents cyber resilience at the systems-engineering level as the ability to continue, recover, and adapt essential functions under adverse conditions [9]. These sources show that information infrastructure is inseparable from security functions, but they do not provide a calculation mechanism that directly links the current state of an information route to the time remaining in a physical attack scenario.

In the field of multisensor data fusion, Hall and Llinas systematized the basic principles of integration at the data, feature, and decision levels [10]. The refined JDL model proposed by Steinberg, Bowman, and White distinguishes among object assessment, situation assessment, impact assessment, and process refinement [11]. Khaleghi et al. provided an extensive review of uncertainty, conflict, correlation, and synchronization problems in heterogeneous data fusion [12]. Castanedo grouped data-fusion methods into data association, state estimation, and decision-fusion approaches [13]. Tsanousa et al. compared architectures for storing, indexing, and fusing sensor data in smart environments [14]. This body of research demonstrates that combining multiple sources can improve accuracy and event recognition. In many models, however, latency is treated only as a constraint or a computational cost, while its effect on the probability of timely intervention by physical response forces is not evaluated separately.

Under dynamic security conditions, situational awareness is a major determinant of operator decision quality. Endsley describes situational awareness through three levels: perception of environmental elements, comprehension of their meaning, and projection of their future status [3]. In physical protection, this sequence corresponds to receiving a sensor signal, classifying the event, assessing the adversary's intent, and selecting a response option. As the volume of information presented to the operator increases, selection and prioritization become more important. Situational awareness is improved not by the number of data items displayed on a screen, but by information that is relevant to the decision and delivered in time.

Studies of security operations centers demonstrate the practical consequences of a high notification load. Agyepong et al. established the need for systematic performance indicators to measure analyst work [15]. Forsberg and Frantti proposed a framework of technical metrics for detection, investigation, and response processes [16]. Tariq et al. identified false alarms, disconnected dashboards, staff shortages, and excessive notification volumes as key causes of alert fatigue [4]. The probabilistic cyber-alert management model developed by Chen et al. demonstrates the value of prioritization based on risk and uncertainty [17]. These findings are equally relevant to the control center of a physical protection system. The key difference is that, in a physical intervention scenario, the consequences of a delayed decision may emerge immediately in the real facility and affect people, rather than remaining confined to the information system.

Recent research has shown growing interest in the joint assessment of physical and cyber effects. Sandia

studies indicate that cyber effects on digital detection and delay measures can weaken physical protection functions, while alternative detection and response architectures can improve overall system effectiveness [18, 19]. The scenario-based assessment by Wadoud et al. further strengthens the route and time logic [8]. Nevertheless, the partially non-compensatory aggregation of information completeness, authenticity, consistency, channel reliability, and cyber resilience, together with the direct subtraction of information latency from the available time reserve, has not yet been sufficiently developed within a unified model.

A comparative review of the literature reveals three gaps. First, data-fusion models focus primarily on information content and accuracy but generally do not account for the decision deadline imposed by physical protection. Second, physical protection models assess time sufficiency but do not explicitly describe the internal delay structure of the information route. Third, cyber-resilience documents protect availability and integrity but do not formalize dynamic route selection according to the risk level of the current physical attack. The proposed methodology brings these three directions together within a unified risk-time framework.

Several English-language studies included in the reference list examine conceptual models of multilevel physical protection, the limitations of normative design under dynamic threats, justification of requirements, systems analysis of the design process, and the integration of machine learning with physical-process models [20–22]. Findings on the probabilistic formalization of risk, individual, collective, and societal risk indicators, time sufficiency, and sensitivity indicators strengthen the theoretical basis of the risk-time framework [23, 24].

The role of information processes in conceptual design, the derivation of measurable requirements, and information-to-action requirements in high-tempo operations have also been investigated [25]. Research on selecting cyber-defense architectures for critical information infrastructure, the cyber resilience of communications and command systems under hybrid attacks, the efficiency of MIMO-based multiservice networks, the probabilistic-temporal limitations of software-defined network controllers, and network indicators under dynamic threats provides a basis for defining reliability criteria for information routes [26–28].

At the sensor level, findings on advanced sensing technologies, intelligent monitoring, deep learning,

multisensor detection of ground targets, multimodal fusion, and multisensor architectures for unmanned aerial vehicles support the joint assessment of information completeness, authenticity, and consistency [29, 30].

Research on accelerating decision-making through C4ISR architecture, visual analytics in security systems, and the use of C4ISR systems in operations provides a methodological foundation for processing information flows at the decision level [31–33]. A systems approach to protecting critical infrastructure in urban environments, monitoring special-purpose information networks, analyzing information flows in technical support, and assessing the efficiency of critical communications infrastructure extends the practical scope of the model [34, 35].

3. Methodology

3.1. Research design and basic assumptions

The study combines conceptual modeling, graph theory, probabilistic assessment, multicriteria aggregation, scenario analysis, and Monte Carlo simulation. The physical protection facility is represented by three levels: an external perimeter, an internal protected zone, and a critical zone. Each zone contains detection sources, preliminary-processing devices, communication nodes, and decision-making elements. The endpoint of the information flow is not limited to the central control room, but also includes the operational command delivered to the response force. The route therefore covers every stage from signal generation to receipt of an actionable instruction.

The model is based on the following assumptions: event scenarios are assigned to predefined threat classes; the processing time and reliability of each information node can be estimated; at least one functional backup route exists; quality indicators are normalized within the interval from 0 to 1; event probability and impact severity are obtained from the risk register; and the response-force travel time is represented as a scenario-dependent random variable. In an operational system, the model can be calibrated using logs, network telemetry, sensor tests, and exercise results.

Fig. 1 traces the sequence from data generation to response action and feedback. At the sensor level, the initial signal undergoes filtering and feature extraction before being correlated with other sources (Table 1) at the multisource fusion node.

Table 1 – Information sources and assessment characteristics in physical protection

Information source	Primary data	Typical risk	Characteristic assessed in the model
Perimeter radar and vibration sensor	Coordinates, speed, boundary violation	Atmospheric effects, false alarms	Authenticity, reliability, latency
Daylight and thermal cameras	Image, object features, trajectory	Degraded visibility, loss of video stream	Completeness, consistency, cyber resilience
Access-control system	Identification, authorization, time of passage	Credential forgery, insider threat	Authenticity, traceability, integrity
Security officer	Observation, context, confirmation	Subjectivity, delayed reporting	Authenticity, processing time
OT and building automation	Status of doors, locks, power, and equipment	Cyber interference, synchronization error	Availability, consistency, cyber resilience

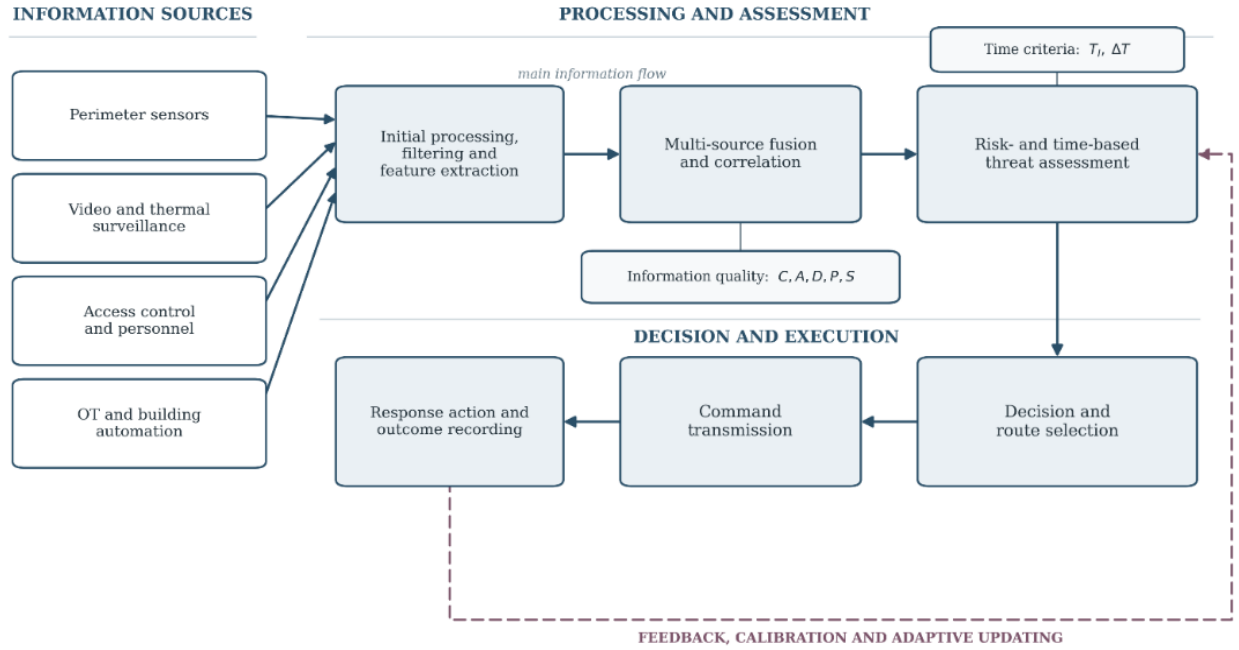


Fig. 1. Structural and functional model of information flow in a physical protection system

The threat assessment determines the event probability, target criticality, and remaining time reserve. The decision module assigns a priority and selects a route, the command is transmitted to the response force, and the outcome of the action generates feedback for updating the model parameters.

3.2. Graph model of the information environment

The information environment is represented as a directed, attributed graph:

$$G_I = (V_I, E_I, \theta_V, \theta_E), \quad r \in \mathcal{R}_s. \quad (1)$$

Here, V_I is the set of sensor, processing, fusion, decision, and execution nodes; E_I is the set of communication links between nodes; θ_V contains the node parameters; θ_E contains the channel parameters; and $\mathcal{R}_s$ is the set of feasible information routes for scenario s . Each arc (i, j) of the graph is assigned a transmission time t_{ij}^{tr} , a queuing time t_{ij}^{que} , a successful-transmission probability p_{ij} , and the current channel load u_{ij} . Each node j is characterized by a processing time t_j^{pr} , a correct-processing probability p_j^{pr} , and a computational reserve.

The total information latency along route r for event s is defined as follows:

$$T_{I,s}(r) = \sum_{(i,j) \in r} (t_{ij}^{tr} + t_{ij}^{que}) + \sum_{j \in r} t_j^{pr} + t_s^{dec} + t_s^{cmd}. \quad (2)$$

Here, t_s^{dec} is the time required to formulate the decision, while t_s^{cmd} is the time required to transmit the operational command to the response force. This decomposition makes it possible to identify the source of the delay. For example, a high t_{ij}^{que} may indicate network or server congestion, whereas a high t_s^{dec} may indicate inefficiency in the operator interface, procedure, or event-classification process.

Assuming independent components, the information reliability of a route is estimated using the following product:

$$P_{I,s}(r) = \prod_{(i,j) \in r} p_{ij,s} \prod_{j \in r} p_{j,s}^{pr}. \quad (3)$$

When common-cause failures exist among components, the product estimate may be optimistic. In operational applications, dependencies such as a shared power source, synchronization service, network switch, or software platform should be represented by separate group coefficients. For this purpose, a correction coefficient $\chi_g \in [0,1]$ for common-cause failure can be applied to the resulting value of $P_{I,s}(r)$.

3.3. Partially non-compensatory assessment of information quality

Information quality is described by five basic components: completeness $C_{s,r}$, authenticity $A_{s,r}$, consistency $D_{s,r}$, route reliability $P_{s,r}$, and cyber resilience $S_{s,r}$. Completeness represents the extent to which the attributes required to describe an event have been obtained. Authenticity expresses how accurately the information reflects the actual situation. Consistency indicates the absence of conflicts among sources. Reliability is the probability that information will be processed and transmitted without loss. Cyber resilience is the ability to preserve the critical information function under cyberattack or failure conditions.

Initial indicators measured on different scales are converted into benefit-type criteria. A benefit indicator is normalized using the following expression:

$$q_{s,r,k} = \frac{x_{s,r,k} - x_k^-}{x_k^+ - x_k^-}, \quad 0 \leq q_{s,r,k} \leq 1. \quad (4)$$

Here, x_k^+ and x_k^- are the best and worst reference values, respectively, for criterion k . Cost-type indicators, such as latency and packet loss, are normalized in the

opposite direction. The reference values should preferably be derived from acceptance-test protocols, service-level requirements, and threat scenarios rather than solely from expert judgment.

A simple weighted sum allows a weak indicator to be fully offset by other indicators with high values. Such compensation may produce an unacceptable result in physical protection. For example, high completeness should not compensate for low reliability if otherwise complete and accurate information has been altered by a cyberattack or arrives after the decision deadline. The integral information-quality score is therefore calculated using the following partially non-compensatory function:

$$Q_{I,s}(r) = \left[\prod_{k=1}^m q_{s,r,k}^{w_k} \right]^{1-\eta} [\min_{1 \leq k \leq m} q_{s,r,k}]^{\eta} \exp[-\lambda_s T_{I,s}(r)]. \quad (5)$$

Here, $w_k \geq 0$ and $\sum_{k=1}^m w_k = 1$ are the criterion weights; $\eta \in [0,1]$ is the sensitivity coefficient for the weakest link; and $\lambda_s > 0$ is the rate at which the time value of information decays. When $\eta = 0$, the model reduces to weighted geometric aggregation. As η increases, the model responds more strongly to the weakest component. The exponential factor gives preference to the route with lower latency when two routes have the same underlying quality. The value of λ_s varies with event dynamics. It should be small for a slowly developing event and larger for a rapid armed intrusion or an adversary already close to the critical zone. The criterion weights can be determined through expert pairwise comparison, the entropy method, or a combination of both. In the present calculation, the weight vector for completeness, authenticity, consistency, reliability, and cyber resilience is $\mathbf{w} = (0.20, 0.25, 0.15, 0.20, 0.20)$. Authenticity receives a relatively high weight because it directly affects decision correctness, while the minimum-component factor creates a mandatory protective threshold for all indicators. The weakest-link sensitivity is set to $\eta = 0.25$, and the information-aging parameter is set to $\lambda_s = 0.025 \text{ s}^{-1}$.

3.4. Time sufficiency, intervention probability, and residual risk

The principal decision constraint in physical protection is the time available before an adversary reaches the target and completes the critical action. Let $T_{A,s}^0$ denote the time required for the adversary's unimpeded movement and action, $T_{G,s}$ the additional delay created by physical barriers, $T_{D,s}$ the interval between the first detectable adversary action and the generation of a reliable alarm, and $T_{R,s}$ the time required for the response force to reach the intervention point after receiving the command. The time margin for scenario s and information route r is then defined as:

$$\Delta T_{s,r} = T_{A,s}^0 + T_{G,s} - T_{D,s} - [T_{I,s}(r) + T_{R,s}]. \quad (6)$$

The condition $\Delta T_{s,r} \geq 0$ indicates that the response force can intervene before the adversary completes the critical action. A negative value means that the information and response chain exceeds the time reserve created by the physical delay measures. Equation (6)

makes information latency an explicit variable in the physical-protection time balance. Under this formulation, every additional second of network or decision latency reduces the time margin by the same amount.

Because the parameters are probabilistic, a strict threshold of zero alone is insufficient. The probability of timely intervention is evaluated smoothly using a logistic function:

$$P_{T,s}(r) = \frac{1}{1 + \exp[-\kappa_s \Delta T_{s,r}]} \quad (7)$$

Here, κ_s determines the sharpness of the time threshold. When $\Delta T_{s,r}$ is strongly positive, $P_{T,s}(r)$ approaches one; when it is strongly negative, the probability approaches zero. Near the threshold, the logistic function provides a more realistic representation of measurement and execution uncertainty.

Timely and correct event detection, information-route quality, satisfaction of the time condition, and the neutralization capability of the response force jointly determine the integrated intervention probability:

$$P_{int,s}(r) = P_{D,s} Q_{I,s}(r) P_{T,s}(r) P_{N,s}. \quad (8)$$

Here, $P_{D,s}$ is the probability of detecting the event, and $P_{N,s}$ is the probability of neutralizing the adversary once a timely engagement has occurred. Multiplying the factors preserves the direct influence of any weakened function on the final result.

If π_s is the probability that scenario s will occur during the period under consideration and L_s is the impact severity of its successful realization, the residual risk is calculated as:

$$R_{res,s}(r) = \pi_s L_s [1 - P_{int,s}(r)]. \quad (9)$$

This expression shows that route selection affects not only technical quality but also the criticality of the protected asset.

The same improvement in route quality produces a greater reduction in risk for a scenario with more severe consequences.

3.5. Event prioritization and route selection

When several alerts are generated at the same time, their processing order should not be determined solely by arrival time. The following risk-time priority index is proposed for event h :

$$\Pi_h = \frac{\hat{p}_h \hat{L}_h U_h K_h}{\max(\hat{T}_{remaining,h}, \varepsilon)}. \quad (10)$$

Here, $\hat{p}_h$ is the current probability that the event represents a genuine threat; $\hat{L}_h$ is the normalized severity of the potential damage; U_h is the information-uncertainty coefficient; K_h is the criticality of the target; $\hat{T}_{remaining,h}$ is the time remaining for a decision; and ε is a small constant that prevents division by zero. A high threat probability, severe potential damage, a critical target, and little remaining time all increase the priority. Including the uncertainty coefficient prevents an unconfirmed but potentially high-consequence event from being assigned an unduly low priority.

Route selection is formulated as a multicriteria optimization problem:

$$r_s^* = \operatorname{argmin}_{r \in \mathcal{R}_s} \left\{ \alpha [1 - Q_{I,s}(r)] + \beta \frac{R_{res,s}(r)}{R_s^{\max}} + \gamma \frac{c_r}{c^{\max}} + \delta \frac{\max(0, -\Delta T_{s,r})}{T_{ref}} \right\}. \quad (11)$$

Here, c_r is the route's consumption of communication, computing, and energy resources; α , β , γ , and δ are the weights of the objective function. For critical events, β and δ may be assigned relatively high values, whereas γ may be larger during routine operation. The selection is performed subject to the following mandatory thresholds:

$$Q_{I,s}(r) \geq Q_s^{\min}, P_{I,s}(r) \geq P_s^{\min}, T_{I,s}(r) \leq T_{I,s}^{\max}. \quad (12)$$

If a route fails to meet any mandatory threshold, a favorable average value in the objective function is not sufficient for its selection. This property retains the partially non-compensatory logic at the optimization stage.

Figure 2 presents the logical sequence of the algorithm. After receiving an event, the system evaluates source reliability and information quality, then calculates latency and the time margin for the feasible routes. Routes that fail to meet the mandatory thresholds are excluded. The remaining alternatives are compared using risk, quality, time, and resource criteria. If the current route falls below a threshold, the system switches to a backup route and reassesses the outcome through feedback.

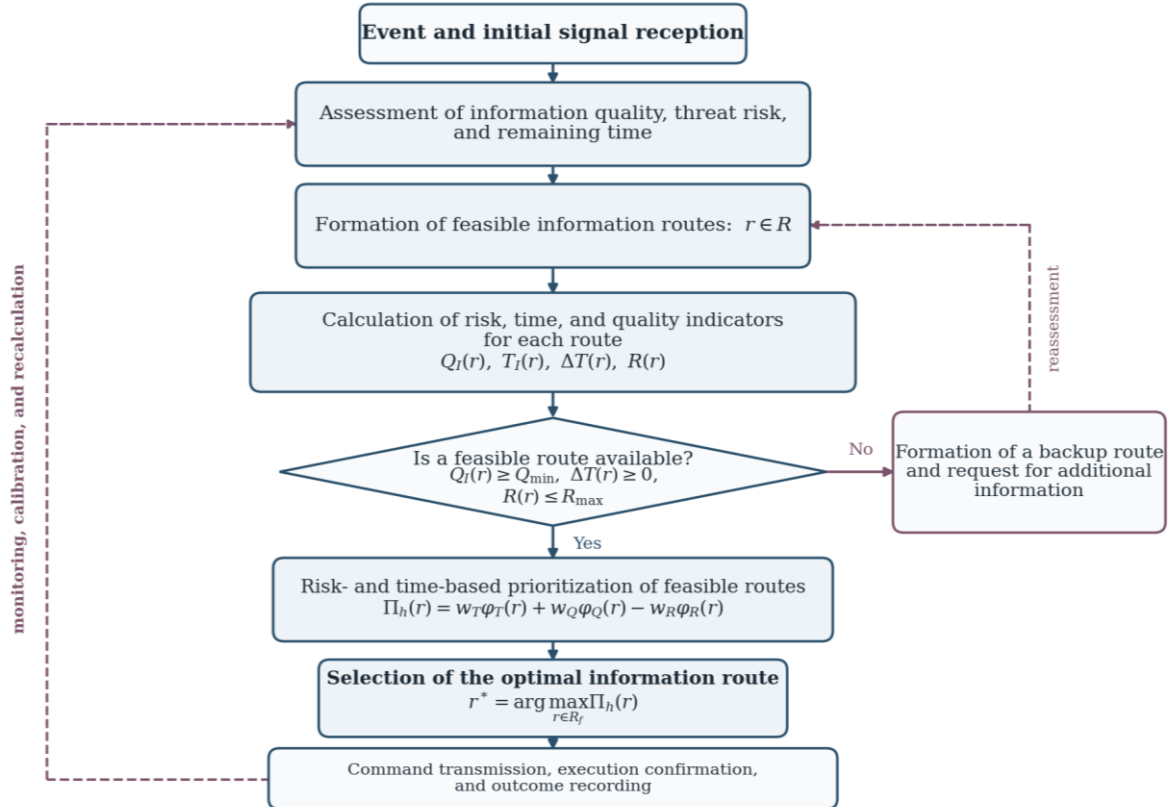


Fig. 2. Algorithm for risk-time-based prioritization and information-route selection

3.6. Computational experiment and input data

A hypothetical three-zone critical infrastructure facility is used to verify the methodology. The first zone contains perimeter radar, a vibration sensor, and daylight and thermal cameras. The second contains access control, video analytics, and a security post. The third contains critical-room sensors, an independent local controller, and the response force. Three information modes are compared: r_1 , the primary route through a central server; r_2 , a distributed backup route with local edge processing and an independent communication channel; and r_3 , a degraded route characterized by high load, packet loss, and indications of cyber interference.

As shown in Table 2, route r_1 has high completeness, but its cyber-resilience value of 0.84 lowers the minimum component. Route r_2 has slightly lower completeness at 0.89, yet its advantages in authenticity, reliability, cyber resilience, and latency

increase the integral result. For route r_3 , both the quality components and the temporal indicator deteriorate. The combined effects of exponential aging and the minimum-component penalty therefore reduce Q_I to 0.590.

Three threat scenarios are considered: s_1 , unauthorized entry through the perimeter; s_2 , a coordinated forced intrusion; and s_3 , an insider bypassing the access procedure for the critical zone (Table 3). The parameters do not reproduce classified information from an actual facility. They are engineering-realistic synthetic values selected to demonstrate the behavior of the method.

After the deterministic calculation, the effect of uncertainty is evaluated using Monte Carlo simulation (Table 4). A total of 10,000 runs is performed for each scenario and route. T_A^0 and T_R are modeled using normal distributions with standard deviations equal to 10% of their respective means. T_G and T_D are modeled using normal distributions with standard deviations equal to 15% of their means.

Table 2 – Initial and integral indicators of the information routes

Route	T_I , s	C	A	D	P	S	Q_I
r_1 , centralized primary	4.8	0.92	0.90	0.88	0.94	0.84	0.782
r_2 , distributed backup	3.1	0.89	0.93	0.91	0.97	0.93	0.849
r_3 , congested and compromised	10.6	0.86	0.81	0.77	0.83	0.70	0.590

Table 3 – Time and probability parameters of the threat scenarios

Scenario	T_A^0 , s	T_G , s	T_D , s	T_R , s	P_D	P_N
s_1 , perimeter intrusion	75	25	4	65	0.94	0.90
s_2 , forced intrusion	52	18	5	54	0.90	0.88
s_3 , insider threat	38	10	8	36	0.82	0.85

Table 4 – Monte Carlo simulation results, 10,000 runs

Scenario	Route	Mean ΔT , s	$P(\Delta T \geq 0)$	Mean P_{int}	5th percentile	95th percentile
s_1	r_1	26.21	0.993	0.654	0.650	0.662
s_1	r_2	27.99	0.995	0.713	0.712	0.718
s_1	r_3	20.49	0.969	0.479	0.383	0.499
s_2	r_1	6.32	0.786	0.472	0.026	0.619
s_2	r_2	7.87	0.836	0.545	0.058	0.672
s_2	r_3	0.46	0.525	0.244	0.001	0.467
s_3	r_1	-0.84	0.442	0.246	0.006	0.533
s_3	r_2	0.89	0.562	0.326	0.014	0.586
s_3	r_3	-6.61	0.138	0.075	0.000	0.337

To preserve positive values, T_I is modeled using a lognormal distribution. The coefficient of variation is set to 0.15 for r_1 and r_2 and to 0.25 for r_3 . The random-number generator seed is set to 20260816 to ensure reproducibility. A value of $\kappa_s = 0.45 \text{ s}^{-1}$ is used for the sharpness of the time threshold.

4. Discussion of results

The deterministic results show that changing the information route directly affects the time balance of physical protection. In scenario s_1 , a large positive time margin remains for all routes. The values are $\Delta T_{1,1} = 26.2 \text{ s}$ for the primary route, $\Delta T_{1,2} = 27.9 \text{ s}$ for the distributed route, and $\Delta T_{1,3} = 20.4 \text{ s}$ for the degraded route. Because P_T is close to one in this scenario, most of the difference in the integrated intervention probability is attributable to information quality. The corresponding P_{int} values are 0.662, 0.718, and 0.499. In the forced-intrusion scenario s_2 , the system approaches the time threshold. The time margin is 6.2 s for r_1 , 7.9 s for r_2 , and only 0.4 s for r_3 . The probability of timely intervention obtained from the logistic function is 0.942, 0.972, and 0.545, respectively. On the degraded route, the increase in mean latency to 10.6 s consumes almost the entire time reserve. Consequently, while the integrated intervention probability is 0.654 for r_2 , it falls to 0.255 for r_3 . In other words, with the detection and neutralization indicators unchanged, disruption of the information chain alone can reduce the protection outcome by 61%.

Scenario s_3 , involving an insider threat, demonstrates the greatest sensitivity to the information route. Because the insider has already bypassed part of

the perimeter barriers and detection occurs later, the decision window is narrow. The time margin is -0.8 s for r_1 , 0.9 s for r_2 , and -6.6 s for r_3 . A reduction of only 1.7 s in route latency changes the time condition from negative to positive compared with the primary route. This change increases P_T from 0.411 to 0.600 and P_{int} from 0.224 to 0.355. It follows that, in scenarios close to the time threshold, a small difference in information latency may have a greater operational effect than improvements in the individual quality components.

The Monte Carlo results reveal substantial distributions behind the deterministic values. In scenario s_1 , the time margin is large and the distribution of P_{int} is therefore relatively narrow. In scenarios s_2 and s_3 , variability in the response and attack times creates wide differences between the 5th and 95th percentiles. For example, the mean intervention probability for the combination of s_2 and r_2 is 0.545, whereas the 5th percentile is only 0.058. This result indicates that a decision based solely on the mean may be excessively optimistic. Route selection at critical facilities should therefore be evaluated using a lower percentile or a conditional risk measure in addition to the mean result.

Figure 3 shows that the distributed backup route performs best in all scenarios, although the scale of its advantage depends on the risk-time conditions. In the perimeter scenario, the improvement is limited because the time condition is almost always satisfied for every route. In the forced-intrusion and insider-threat scenarios, the faster and more resilient route affects the result through two channels: it increases Q_I and enlarges the time margin that determines P_T .

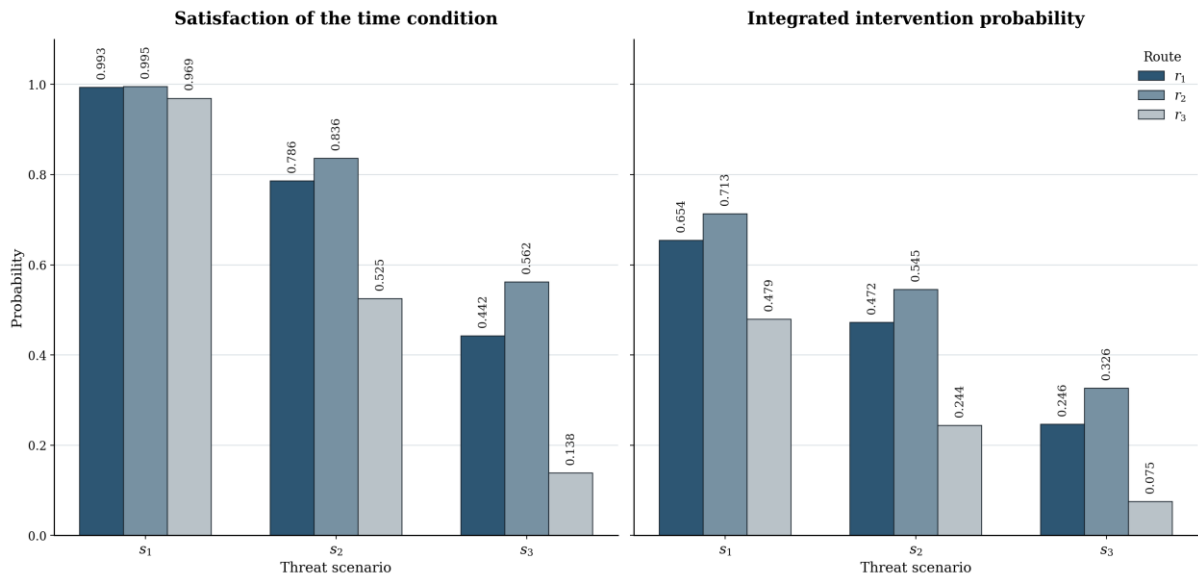


Fig. 3. Comparison of time-condition satisfaction and integrated intervention probability across scenarios

Compared with the centralized primary route, the distributed backup route increases the mean P_{int} by 8.9% for s_1 , 15.3% for s_2 , and 32.7% for s_3 . This nonlinear improvement shows that the relative importance of information latency increases as the threat approaches the critical zone.

A centralized architecture may be convenient for management and auditing, but routing all information

through the same server, switch, and analytical service introduces a common-cause failure. An edge-processing node and an independent communication channel reduce this dependency by transmitting the minimum information set required for a decision over a shorter route.

The sensitivity analysis identifies response time T_R as the most influential parameter (Table 5).

Table 5 – One-way sensitivity analysis for the main parameters

Parameter varied for s_2 and r_2	Change in P_{int} at lower value	Change in P_{int} at higher value	Interpretation
T_I , -20% and +20%	+2.25%	-2.41%	Increased latency affects the result through both Q_I and P_T
T_R , -10% and +10%	+2.60%	-22.35%	The nonlinear effect near the time threshold is strongest
λ , -20% and +20%	+1.56%	-1.54%	The information-aging rate has an approximately symmetric effect
η , 0.10 and 0.40	+0.61%	-0.60%	The weakest-link penalty is limited when the quality components are balanced
A , -0.05 and +0.05	-1.31%	+0.99%	The quality result changes because authenticity has a high weight
S , -0.05 and +0.05	-1.11%	+0.79%	Cyber resilience preserves the advantage of the backup route

A 10% increase in T_R reduces P_{int} by 22.35% for the combination of s_2 and r_2 . The fact that the decrease is much larger than the corresponding increase is explained by the nonlinear nature of the logistic function. When the system is close to the time threshold, a negative change produces a sharp loss, whereas the benefit of a positive change is limited as the probability approaches one. This finding indicates that information-route optimization should be coordinated with response-force deployment and readiness.

The relatively low sensitivity to η is attributable to the balanced quality components of the selected route r_2 . If one component, such as cyber resilience, fell to 0.50, the influence of the minimum-component factor would increase considerably. The parameter η is therefore not merely a mathematical hardening factor. It expresses the facility's risk attitude toward a weak link. At high-consequence facilities, a higher value of η and separate minimum thresholds for each component are appropriate.

A three-level management structure is proposed for practical application of the methodology. At the strategic level, acceptable risk, minimum Q_I , minimum P_I , and maximum information-latency thresholds are established. At the operational level, the state of routes, server and network loads, sensor failures, time synchronization, and cyber incidents are monitored. At the tactical level, the priority of a specific event is calculated, a route is selected, and a response command is generated. This division links technical indicators to management decisions.

The proposed model also offers a different way of addressing false alarms. Simply filtering out false alarms may increase the risk of losing a genuine event. In addition to threat probability, the priority index considers potential damage, target criticality, uncertainty, and the remaining time. Consequently, a low-confidence signal associated with a critical target and a narrow decision window is not rejected outright. Instead, it is sent for urgent verification

through an additional sensor request or a more reliable route. This approach establishes a functional balance between automation and operator oversight.

From a scientific perspective, the model connects data-fusion theory with the time sufficiency of physical protection. In the data-fusion literature, the principal objective is to improve the accuracy of a unified situation picture [10–14]. In the physical protection literature, the main objective is to enable response forces to intervene before the adversary completes the critical action [1, 2, 8]. Equation (5) integrates the quality and time value of information, while Equation (6) links that value to the physical time margin. Information-architecture improvements can therefore be assessed not merely as IT performance measures, but as investments in physical security.

The study also has several limitations. First, the computational experiment uses synthetic data and cannot be treated as a direct normative result for a specific facility. Second, Equation (3) assumes conditional independence among components, although operational systems contain power, software, and communication dependencies. Third, P_D and P_N are treated as constants, although they may correlate with weather, adversary tactics, personnel readiness, and information quality. Fourth, the parameter κ_s of the logistic function must be calibrated using exercise and incident data. Future studies could address these limitations through Bayesian networks, common-cause failure models, and adaptive weight updating based on real-time telemetry.

5. Conclusions

This study develops a model that integrates risk and time criteria for processing information flows in the physical protection of special-purpose and critical infrastructure facilities. From generation of the sensor signal to delivery of the operational command to the response force, the model separately accounts for transmission, queuing, processing, decision, and command delays. Representing the information environment as a directed graph makes it possible to identify alternative routes, bottlenecks in nodes and channels, and common-cause dependencies.

Combining completeness, authenticity, consistency, reliability, and cyber resilience through a weighted geometric mean, a minimum-component factor, and an exponential time penalty limits full compensation for a weak indicator. This property is essential for critical protection systems because distorted, unreliable, or delayed information cannot be considered safe merely because other quality indicators are strong. The proposed Q_I indicator reflects not only the technical correctness of information, but also its operational usefulness for the specific event.

Including information latency in the time-sufficiency equation shows that each unit of time lost in the communication and processing chain reduces by the same amount the reserve created by physical barriers. Near the time threshold, this effect is nonlinear. In the insider-threat scenario, switching from the primary route to the distributed backup route changes the deterministic time margin from -0.8 s to 0.9 s. In the Monte Carlo experiment, it increases the probability of satisfying the time condition from 0.442 to 0.562. The mean integrated intervention probability rises from 0.246 to 0.326, corresponding to a relative improvement of 32.7%.

The results confirm that route selection should not be treated as a static network rule. It should be implemented as a dynamic decision based on event probability, impact severity, target criticality, information uncertainty, and the remaining time. Distributed processing and an independent backup channel not only increase availability, but also widen the decision window. The design of a physical protection system should therefore specify mandatory thresholds for the latency, reliability, and cyber resilience of information routes alongside sensor and barrier performance requirements.

For practical implementation, the model parameters should be calibrated using the facility's risk register, acceptance tests, communication logs, operator-activity records, and tactical exercise results. The strategic level should define acceptable risk and minimum quality thresholds; the operational level should monitor route and node status; and the tactical level should provide real-time prioritization and route switching. Future research may validate the model using data from an operational facility, represent correlated failures through Bayesian networks, detect adversarial data manipulation, and update weight parameters adaptively.

Conflict of interest

The authors declare that they have no conflict of interest regarding this research, including financial, personal, authorship-related, or any other type of conflict that could affect the research and its results presented in this article.

Фінансування

Дослідження проводилося без фінансової підтримки.

Data availability

The manuscript has no associated data.

Use of artificial intelligence tools

The authors confirm that artificial intelligence technologies were not used in the preparation of this work.

REFERENCES

1. Garcia, M. L. (2008), *Design and Evaluation of Physical Protection Systems*, 2nd ed., Butterworth-Heinemann, Burlington, doi: <https://doi.org/10.1016/B978-0-08-055428-0.50005-1>
2. (2011), *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, IAEA Nuclear Sec. Ser. No. 13. Vienna: IAEA, 57 p., doi: <https://doi.org/10.61092/iaea.ko2c-dc4q>
3. Endsley, M. R. (1995), "Toward a theory of situation awareness in dynamic systems", *Human Factors*, vol. 37(1), pp. 32–64, doi: <https://doi.org/10.1518/001872095779049543>

4. Tariq, S., Chhetri, M. B., and Paris, C. (2025), "Alert fatigue in security operations centres: Research challenges and opportunities", *ACM Computing Surveys*, doi: <https://doi.org/10.1145/3723158>
5. (2021), *Computer Security for Nuclear Security*, IAEA Nuclear Security Series No. 42-G., IAEA, Vienna 2021, 86 p., available at: <https://www.iaea.org/publications/13629/computer-security-for-nuclear-security>
6. Stouffer, K., Pease, M., Tang, C. Y., Zimmerman, T., Pillitteri, V. Y., Lightman, S., Hahn, A., Saravia, S., Sherule, A., and Thompson, M. (2023), *Guide to Operational Technology Security*. NIST SP 800-82 Rev. 3., National Institute of Standards and Technology, Gaithersburg, doi: <https://doi.org/10.6028/NIST.SP.800-82r3>
7. (2020), *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5, National Institute of Standards and Technology, Gaithersburg, Joint Task Force, doi: <https://doi.org/10.6028/NIST.SP.800-53r5>
8. Wadoud, A. A., Adail, A. S., and Saleh, A. A. (2018), "Physical protection evaluation process for nuclear facility via sabotage scenarios", *Alexandria Engineering Journal*, vol. 57(2), pp. 831–839, doi: <https://doi.org/10.1016/j.aej.2017.01.045>
9. Ross, R., Pillitteri, V. Y., Graubart, R., Bodeau, D., and McQuaid, R. (2021), *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST SP 800-160 Vol. 2 Rev. 1, National Institute of Standards and Technology, Gaithersburg, doi: <https://doi.org/10.6028/NIST.SP.800-160v2r1>
10. Hall, D. L., and Llinas, J. (1997), "An introduction to multisensor data fusion", *Proceedings of the IEEE*, vol. 85(1), pp. 6–23, doi: <https://doi.org/10.1109/5.554205>
11. Steinberg, A. N., Bowman, C. L., and White, F. E. (1999), "Revisions to the JDL data fusion model", *Proceedings of SPIE*, vol. 3719, pp. 430–441, doi: <https://doi.org/10.1117/12.341367>
12. Khaleghi, B., Khamis, A., Karray, F. O., and Razavi, S. N. (2013), "Multisensor data fusion: A review of the state-of-the-art", *Information Fusion*, vol. 14(1), pp. 28–44, doi: <https://doi.org/10.1016/j.inffus.2011.08.001>
13. Castanedo, F. (2013), "A review of data fusion techniques", *The Scientific World Journal*, doi: <https://doi.org/10.1155/2013/704504>
14. Tsanousa, A., et al. (2022), "A review of multisensor data fusion solutions in smart manufacturing: systems and trends", *Sensors*, vol. 22(5), 1734, doi: <https://doi.org/10.3390/s22051734>
15. Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2023), "A systematic method for measuring the performance of a cyber security operations centre analyst", *Computers & Security*, vol. 124, article 102959, doi: <https://doi.org/10.1016/j.cose.2022.102959>
16. Forsberg, J., and Frantti, T. (2023), "Technical performance metrics of a security operations center", *Computers & Security*, vol. 135, 103529, doi: <https://doi.org/10.1016/j.cose.2023.103529>
17. Chen, H., Dunklee, A., Jajodia, S., Liu, R., McNamara, S., and Subrahmanian, V. S. (2022), "PCAM: A data-driven probabilistic cyber-alert management framework", *ACM Transactions on Internet Technology*, vol. 22(3), article 67, pp. 1–24, doi: <https://doi.org/10.1145/3511101>
18. Johnson, J. (2020), "Physical security and cybersecurity of energy storage systems", *Energy Storage Handbook*, Sandia National Laboratories, available at: https://www.researchgate.net/publication/348785890_Chapter_18
19. Evans, A., Russell, J. L., and Cipiti, B. B. (2023), "New security concepts for advanced reactors", *Nuclear Science and Engineering*, vol. 197(S1), pp. S70–S79, doi: <https://doi.org/10.1080/00295639.2022.2112134>
20. Akhundov, R.G., Hashimov, E.G., and Islamov, I.J. (2026), "Conceptual models of multi-level physical protection systems for special-purpose and critical infrastructure facilities", *Grail of Science*, no. 61, pp. 591–608, doi: <https://doi.org/10.36074/grail-of-science.23.01.2026.066>
21. Akhundov, R.G., Hashimov, E.G., and Islamov, I. (2026), "Methodological limitations of normative design of physical protection systems for critical and military facilities in a dynamic threat environment", *Grail of Science*, no. 62, pp. 873–889, doi: <https://doi.org/10.36074/grail-of-science.20.02.2026.096>
22. Akhundov, R.G. (2026), "Enhancing the physical protection of critical facilities through the integration of physical process models and machine learning", *Grail of Science*, no. 61, pp. 722–731, doi: <https://doi.org/10.36074/grail-of-science.23.01.2026.083>
23. Akhundov, R.G., Talibov, A.M., and Hashimov, E.G. (2026), "Temporal sufficiency of physical protection systems for critical and military facilities", *Grail of Science*, no. 68, pp. 913–930, doi: <https://doi.org/10.36074/grail-of-science.15.05.2026.102>
24. Talibov, A.M., Akhundov, R.G., and Hashimov E.G. (2026), "Integral sensitivity indicator based on multilayer indicators for critical infrastructure and special-purpose facilities and the selection of measures", *Grail of Science*, no. 65, pp. 563–579, doi: <https://doi.org/10.36074/grail-of-science.03.04.2026.063>
25. Akhundov, R.G. and Hashimov, E.G. (2026), "Modeling information processes and deriving measurable requirements in physical protection system design", *Management Information System and Devices*, no. 1(188), pp. 5–16, doi: <https://doi.org/10.30837/0135-1710.2026.188.005>
26. Gasimov, V., Mammadov, J., Islamov, I., and Hashimov, E. (2026), "Evaluation of alternative solutions for the effective structure of the cyber security system in critical information infrastructures by the hierarchical analysis method", *Advanced Information Systems*, vol. 10(2), pp. 87–99, doi: <https://doi.org/10.20998/2522-9052.2026.2.10>
27. Hashimov, E.G., Ibrahimov, B.G., Islamov, I.J., Talibov, A.M., and Akhundov, R.G. (2026), "Research of the efficiency multiservice networks using MIMO technology", *Advanced Information Systems*, vol. 10(1), pp. 66–71, doi: <https://doi.org/10.20998/2522-9052.2026.1.08>
28. Ibrahimov, B.G., Akhundov, R.G., and Hashimov E.G. (2025), "Research of multi-service communication networks taking into account dynamically emerging security threats", *Problems of Informatization*. Proc. of the 13th International Scientific and Technical Conference, vol. 2, pp. 10–11, available at: <https://repository.kpi.kharkov.ua/handle/KhPI-Press/95974>
29. Muradova, E.E., Talibov, A.M., and Hashimov E.G. (2025), "Deep learning for critical infrastructure security in energy and transportation", *Grail of Science*, no. 56, pp. 310–323, doi: <https://doi.org/10.36074/grail-of-science.19.09.2025.039>
30. Huseynov, B.S. et al. (2025), "Multisensor detection architectures on UAV platforms: methodology, indicators and implementation in Azerbaijan", *Problems of Informatization*. Proceedings of the 13th International Scientific and Technical Conference, vol. 2, pp. 132–134, available at: <https://repository.kpi.kharkov.ua/handle/KhPI-Press/96131>
31. Krikun, V.L. et al. (2025), "Accelerating decision making and operational efficiency through C4ISR architecture. *Problems of Informatization*", Proceedings of the 13th International Scientific and Technical Conference, vol. 2, pp. 120–121, available at: <https://repository.kpi.kharkov.ua/handle/KhPI-Press/96093>

32. Hazarkhanov, A.T. et al. (2025), "Visual analytics across security and systems engineering: foundations for the V-model and C4ISR", *Problems of Informatization*, Proceedings of the 13th International Scientific and Technical Conference, vol. 4, pp. 74–76, available at: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/90741da4-0b60-438f-9157-590b3b2aa6ec/content>
33. Maharramov, R.R. et al. (2025), "Application of C4ISR systems in military and security operations", *Innovative Trends in Natural Sciences, Humanities and Exact Sciences*, Proceedings of the 7th International Scientific Conference, pp. 125–134, doi: <https://doi.org/10.62731/mcnd-15.08.2025.004>
34. Talibov, A.M., and Hashimov, E.G. (2024), "Analysis of information flows in the technical support of the army", *Problems of Informatization*, Proceedings of the 12th International Scientific and Technical Conference, vol. 3, p. 6, doi: <https://doi.org/10.32620/PI.24.t3>
35. Ibrahimov, B.G., Hasanov, A.H., doi., and Hashimov, E.G. (2024), "Research and analysis of efficiency indicators of critical infrastructures in the communication system", *Advanced Information Systems*, vol. 8(2), pp. 58–64 <https://doi.org/10.20998/2522-9052.2024.2.07>

Received (Надійшла) 15.06.2026

Accepted for publication (Прийнята до друку) 26.08.2026

Publication date (Дата публікації) 25.09.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Гашимов Елшан Гіяс – доктор наук з національної безпеки та військових наук, професор, професор Азербайджанського технічного університету, професор Університету національної оборони, Баку, Азербайджан;

Elşan Hashimov – Doctor in national security and military sciences, professor, professor of Azerbaijan Technical University, professor of National Defense University, Baku, Azerbaijan;

e-mail: hasimovel@gmail.com; ORCID Author ID: <http://orcid.org/0000-0001-8783-1277>;

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57195631270>.

Ахундов Раміль Гурбаналі – доктор філософії з національної безпеки та військових наук, професор Національного університету оборони, Баку, Азербайджан;

Ramil Akhundov – PhD in National Security and Military Sciences, Professor of National Defense University, Baku, Azerbaijan;

e-mail: mr.axundov1@gmail.com; ORCID Author ID: <https://orcid.org/0009-0001-8798-8044>;

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=59968793800>.

Талібов Азіз Машалла – доктор наук з національної безпеки та військових наук, професор, професор Інституту систем управління, Баку, Азербайджан;

Aziz Talibov – Doctor in National Security and Military Sciences, Professor, Professor of Institute of Control Systems, Baku, Azerbaijan;

e-mail: talibovaziz65@gmail.com; ORCID Author ID: <https://orcid.org/0000-0002-0572-7212>;

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=60388843600>.

Радованович Марко – Військова академія, Університет оборони, Белград, Сербія;

Marko Radovanović – Military Academy, University of Defence, Belgrade, Serbia;

e-mail: markoradovanovicgdb@yahoo.com; ORCID Author ID: <https://orcid.org/0000-0002-9866-9639>;

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57219384593>.

Модель оброблення інформаційних потоків з урахуванням ризику та часу в системах фізичного захисту об'єктів спеціального призначення та критичної інфраструктури

Е. Г. Гашимов, Р. Г. Ахундов, А. М. Талібов, М. Р. Радованович

Анотація. Ефективність функціонування системи фізичного захисту визначається не лише характеристиками чутливості засобів виявлення, часом затримки, що забезпечується фізичними бар'єрами, та рівнем готовності сил реагування, але й своєчасністю, повнотою та цілісністю передавання неоднорідних даних у сфері безпеки до рівня прийняття рішень. У роботі запропоновано інтегровану модель оброблення інформаційних потоків з урахуванням ризику та часових характеристик для систем фізичного захисту об'єктів спеціального призначення та критичної інфраструктури. Інформаційне середовище подано у вигляді орієнтованого графа. Часові затримки передавання, оброблення та очікування інформації в чергах інтегровано з показниками її повноти, точності, узгодженості, надійності та кіберстійкості. Для комплексного оцінювання якості інформації розроблено частково некомпенсаторний індекс, що поєднує зважене геометричне середнє, значення найслабшої складової та коефіцієнт часового згасання. Затримку інформації явно враховано в балансі часу виявлення, затримки порушника та реагування. Сформульовано аналітичні вирази для визначення ймовірності своєчасного втручання та оцінювання залишкового ризику. Для гіпотетичного об'єкта з трьома функціональними зонами проведено імітаційний експеримент методом Монте-Карло, що охоплював 10 000 реалізацій. За результатами моделювання встановлено, що розподілений резервний маршрут забезпечив інтегральний показник якості інформації на рівні 0,849, тоді як для централізованого основного маршруту цей показник становив 0,782, а для переважаного та частково скомпрометованого маршруту — 0,590. У сценарії обходу системи фізичного захисту внутрішнім порушником використання розподіленого маршруту дало змогу підвищити ймовірність виконання часової умови з 0,442 до 0,562, а середню інтегральну ймовірність переривання дій порушника — з 0,246 до 0,326. Запропонований підхід забезпечує комплексне оцінювання вразливостей інформаційних каналів у взаємозв'язку з характеристиками фізичних бар'єрів та дає змогу здійснювати динамічний вибір маршрутів передавання інформації залежно від рівня ризику події й доступного часу для реагування.

Ключові слова: система фізичного захисту; інформаційний потік; затримка інформації; інтеграція даних; ризик; достатність часу; критична інфраструктура; частково некомпенсаторна модель.