Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

UDC 004:351.746:007 DOI: https://doi.org/10.30837/0135-1710.2026.188.005

Ramil Akhundov, Elshan Hashimov

MODELING INFORMATION PROCESSES AND DERIVING MEASURABLE REQUIREMENTS IN PHYSICAL PROTECTION SYSTEM DESIGN

The study examines information processes in the conceptual design of physical protection systems and their role in transforming sensor outputs, operator inputs, and communication flows into timely protective action. Attention is focused on the fact that design sufficiency is constrained not only by sensors, barriers, and response forces, but also by delays and uncertainty arising between detection, decision, and dispatch. The purpose of the study is to formalize information processes as explicit design objects and to develop an approach for deriving measurable information requirements that can be justified and verified at the conceptual design stage. The objectives are to define a reference workflow from event generation to response activation, to decompose the total information-to-action time into operational stages, to incorporate uncertainty related to false alarms, ambiguity, workload, and degraded communications, and to link requirement statements with acceptance evidence. The research uses a conceptual and methodological approach based on systems analysis, scenario decomposition, latency structuring, and traceability mapping between threat scenarios, bottlenecks, requirement targets, and verification evidence. The study develops a structured information-to-action model that makes explicit the stages of sensing, validation, fusion, decision-making, communication, and dispatch. On this basis, a method is proposed for translating scenario-specific bottlenecks into verifiable requirements for timeliness, accuracy, completeness, and resilience. The study also identifies practical forms of acceptance evidence, including timed drills, log-based measurements, stress testing, and simulation-supported assessment. The results show that conceptual design becomes more defensible when information processes are modeled explicitly rather than treated as implicit assumptions. The proposed approach enables designers to justify measurable requirements, reveal critical latency sources, and support revalidation of design sufficiency under changing operational conditions.

Keywords: *physical protection system; conceptual design; information processes; alarm validation; data fusion; command and control; communications resilience; acceptance evidence.*

1. Introduction

Physical protection systems are typically described in terms of tangible components: sensors, barriers, access control devices, and response forces [1–3]. While these elements are necessary, they are not sufficient to explain why a system succeeds or fails under real adversarial conditions. In practice, operational outcomes are often determined by information processes that connect detection to action. The same sensor coverage can produce radically different security performance depending on how signals are validated, how information is fused across sources, how quickly decisions are made, how reliably communications propagate directives, and how response resources are dispatched under uncertainty and workload [4, 5].

A persistent methodological weakness in conceptual design is the implicit assumption of near-perfect information [6]. Early design stages frequently treat detection as an instantaneous event, decision-making as a negligible delay, and communications as a transparent channel. This assumption is convenient for describing system architecture, but it is risky for requirement justification because it masks the dominant sources of failure. False alarms can saturate operators and erode trust in alerts. Ambiguous signals can trigger prolonged validation cycles. Degraded communications can disrupt escalation and dispatch. Insider-enabled actions can bypass traditional detection cues. Under such conditions, the bottleneck is not the physical layer but the information-to-action loop that governs the timing and correctness of intervention [6, 7].

The problem addressed in this paper is that information processes are often not treated as first-class design objects at the conceptual stage. As a result, information requirements are either absent or expressed as generic aspirations rather than measurable thresholds. This gap weakens review defensibility. A design may be compliant on paper and still be operationally insufficient because the information chain cannot deliver timely and reliable decision support for the detection–decision–response sequence. Without a structured model of information flows and latencies, it is difficult to justify why particular sensor configurations, staffing levels,

© Ramil Akhundov, Elshan Hashimov, 2026
This is an Open Access article under the CC BY-NC-SA 4.0 license https://creativecommons.org/licenses/by-nc-sa/4.0/deed.uk

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

alarm-management policies, or command-and-control procedures are sufficient for representative scenarios.

This study argues that conceptual design must explicitly model information processes, including their latency and uncertainty, and must translate them into verifiable requirements. The core idea is straightforward: sufficiency is time-conditioned, and information delays consume the time margin needed to interrupt an adversary before the critical element is reached. Therefore, conceptual design should specify not only what is installed, but how information is generated, transformed, transmitted, interpreted, and acted upon, with explicit acceptance targets for timeliness, reliability, completeness, and resilience under degraded conditions.

The aim of this paper is to formalize information processes within conceptual physical protection design and to provide a reproducible method for deriving measurable information requirements that support system-level sufficiency. The objectives are to define a reference information workflow from sensing to decision to response, decompose the information-to-action timeline into measurable components, represent key uncertainty sources such as false alarms and degraded communications, and establish a traceability structure that links information requirements to scenario needs and verification evidence.

The remainder of the paper is organized as follows. The next section reviews related approaches in physical protection, command-and-control, and alarm management and clarifies where information processes are under-modeled. The methods section presents the information-process model, latency decomposition, and requirement derivation logic. The results section provides measurable requirement templates and practical artifacts for verification and monitoring. The paper concludes with discussion of implications, limitations, and directions for future work.

2. Background And Related Approaches

Conceptual design of physical protection systems has traditionally been dominated by prescriptive and component-oriented approaches. Normative frameworks provide minimum requirements for barriers, access control, detection devices, and response arrangements, enabling consistency and auditability across portfolios of facilities [8, 9]. This baseline remains essential, particularly for high-consequence settings, because it prevents omission of critical protective functions. However, normative specifications frequently treat information as an implicit enabler rather than as an explicit design object. Requirements tend to describe what hardware must exist and what procedures must be documented, while the operational performance of the information-to-action loop, how quickly and reliably an alarm becomes a validated decision and an executed response, is under-specified [10–12].

The classical detection–delay–response doctrine provides an operational logic that highlights why information processes matter [13, 14]. Detection must occur early enough to initiate the defender chain, delay must create the time reserve needed for response, and response must be executed before the adversary reaches the target. In this chain, information is not merely a front-end sensor output. It is the continuous input to decision-making and coordination: the defender cannot exploit delay if alarms are not validated promptly, and response effectiveness degrades if communications are unreliable or if command-and-control introduces friction. Yet, in much of the applied practice, information processes are treated as a background assumption, with decision latency and communications reliability either neglected or treated as fixed constants.

Research on situation awareness and decision-making in military and security operations provides a more explicit treatment of information processing, particularly through the concepts of perception, comprehension, and projection as prerequisites for action [15, 16]. Within this literature, performance is strongly influenced by information quality, cognitive workload, ambiguity management, and the design of human–machine interfaces. Alarm fatigue and operator overload are well-known phenomena that can substantially increase validation and decision time, even when sensors technically function as specified. These insights are directly relevant to physical protection design, but they are often not integrated into the conceptual requirement-setting process, which still privileges hardware-centric measures [17, 18].

A related body of work addresses sensor data fusion, alarm management, and security operations center workflows. Multi-sensor fusion can reduce uncertainty and improve classification, but it can also introduce additional processing steps and latency, especially when signals are inconsistent or when the system is configured conservatively to reduce false positives. Alert management policies, such as escalation rules, acknowledgement procedures, and prioritization, largely determine the effective time to take action [19]. The literature also emphasizes that communications and command-and-

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

control are not transparent pipes: network congestion, degraded links, and procedural bottlenecks can delay dispatch and reduce coordination quality, particularly during multi-event situations or intentional diversion.

Across these approaches [20–22], recurring failure modes can be traced to information processes rather than to physical components alone. False alarms can saturate operators and cause delays in acknowledging genuine events. Ambiguous detections can trigger prolonged verification cycles [23, 24]. Degraded communications can fragment the operational picture and slow or misdirect response. Insider-assisted actions can bypass expected signatures, forcing reliance on procedural checks and internal monitoring. These failure modes are consistent with "compliant but insufficient" outcomes: a facility may meet prescriptive equipment and staffing requirements, yet still fail operationally because the information loop cannot deliver timely, reliable decision support under representative conditions.

Scenario-based and risk-informed design approaches partially address these issues by emphasizing operational context [23]. They encourage designers to consider how different threat mechanisms stress different subsystems, including decision-making. Nevertheless, many scenario-based treatments still stop short of defining measurable information requirements. Scenarios are used to justify security measures, but the information processes that link information discovery to action are not formalized in a way that allows for the establishment of acceptance criteria, such as the maximum allowable verification time for a given alarm load, the minimum communication availability under degraded conditions, or the required classification accuracy for a given threat class [25–27]. The gap addressed by this paper is therefore specific: existing approaches recognize that information matters, but they lack a unified conceptual model that treats information processes as first-class design objects and converts them into verifiable requirements tied to system-level sufficiency. The contribution pursued here is to formalize the information workflow from sensing to decision to response, decompose its latency and uncertainty components, and provide a traceable method to derive measurable information requirements and evidence pathways that can be integrated with physical protection design from the earliest stages.

3. Material and Methods

This study develops a conceptual and methodological framework that treats information processes as explicit design objects in the conceptual design of physical protection systems. Two analytical layers are distinguished. First, a reference information-process model is introduced to describe how information moves from sensing to response activation in a protected facility. Second, a Scenario-Driven Information Requirement Derivation Method is defined to translate the modeled information process into measurable, verifiable, and traceable requirement statements. The scope is methodological rather than facility-specific: the purpose is not to calibrate a single site, but to provide a reproducible structure that can later be instantiated with site data, operating assumptions, and threat scenarios.

The protected facility is represented as a socio-technical system comprising sensing assets, human operators, procedures, command-and-control functions, communications channels, and response forces. In this study, command-and-control (C2) denotes the set of functions responsible for decision-making, authorization, coordination, and dispatch based on validated security information. Information is modeled as a bounded forward process that links observation to action through a sequence of operational stages. These stages include event generation and sensing, alarm validation, multi-source fusion, threat classification, decision and authorization, communication of directives, dispatch and mobilization, and response activation. A feedback loop is also acknowledged conceptually because logs, after-action review, and parameter updates are necessary for lifecycle revalidation, but the formal part of the framework focuses on the forward information-to-action path.

A reference information-process model used in conceptual physical protection design is presented in Figure 1. The figure describes only the forward information-to-action path and the lifecycle feedback loop; the derivation of measurable requirements is introduced separately below.

Figure 1 shows how information moves from heterogeneous sources to response activation through detection, validation, fusion, decision, communication, and dispatch stages. In this representation, C2 denotes the command-and-control functions responsible for decision-making, authorization, coordination, and dispatch.

Let S denote the set of information sources, including intrusion sensors, access-control events, video analytics, operator reports, and system-health telemetry. Let $m \in M$ denote information messages generated by these sources and transmitted through communications channels under a given operating context. The operating

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

context includes visibility, weather, staffing posture, communications status, operator workload, and the presence of concurrent incidents. Within this representation, the reference model serves a descriptive role: it makes explicit where information is created, transformed, delayed, degraded, or lost before a protective action is activated.

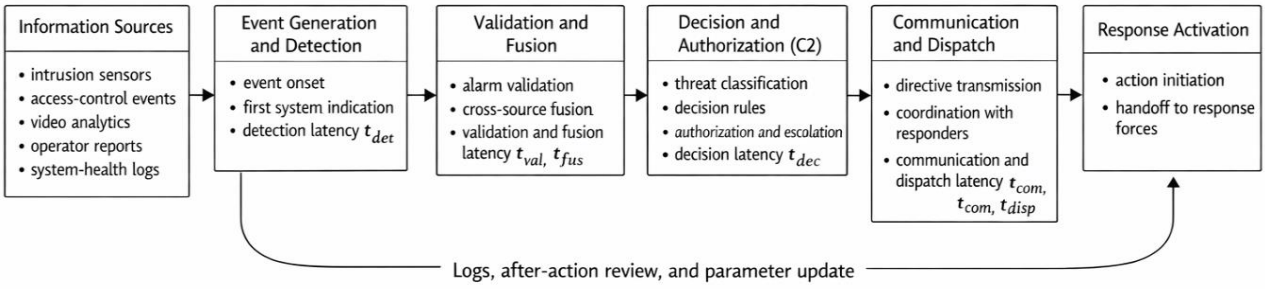

Fig. 1. Reference information-process model for conceptual physical protection system design

To avoid ambiguity, the principal symbols and operational metrics are defined before formal derivation. For a scenario s, let $T_{info,s}$ denote the total information-to-action time. Let $t_{det,s}$ denote detection latency from event onset to first system indication; $t_{val,s}$, alarm validation time from first indication to confirmed event status; $t_{fus,s}$, multi-source fusion time; $t_{dec,s}$, decision and authorization latency; $t_{com,s}$, communications latency for disseminating directives and situational context; and $t_{disp,s}$, dispatch and mobilization time from decision to response activation. In addition, let $P_{D,s}$ denote the probability of timely detection within a specified time window, $P_{C,s}$ the probability of correct classification, FAR_s the false alarm rate, $A_{com,s}$ communications availability, $L_{loss,s}$ message loss rate, and W_s an operator-workload indicator expressed, for example, through alert arrival rate or queue length. The symbol $Pr(\cdot)$ denotes probability.

Information quality is represented through a minimal set of dimensions that are both operationally meaningful and measurable at the conceptual design stage: timeliness, accuracy, completeness, integrity, and availability. Timeliness is captured through the latency structure of the information-to-action chain. Accuracy is represented through timely-detection and correct-classification probabilities. Completeness characterizes whether the decision-maker receives sufficient context to choose and authorize an action without excessive additional verification. Integrity addresses the trustworthiness of information and resistance to corruption or misleading inputs. Availability reflects whether information and communications remain usable under degraded or adversarial conditions. These dimensions are treated as design constraints rather than as qualitative aspirations because the objective is to justify measurable requirement targets at an early design stage.

The reference model is made operational through an explicit decomposition of the information-to-action time into stage-specific latency components. For scenario s, the total information-to-action time is represented as

$$T_{info,s} = t_{det,s} + t_{val,s} + t_{fus,s} + t_{dec,s} + t_{com,s} + t_{disp,s}. \quad (1)$$

Equation (1) states that the total delay between event onset and response activation is the sum of the detection, validation, fusion, decision, communications, and dispatch latencies. This decomposition is aligned with sufficiency-oriented defender timelines because information delays directly consume the time margin available for interruption. At the conceptual design stage, the key implication is that information processes must not be treated as negligible constants. Their duration is scenario-dependent and may become dominant under ambiguity, high workload, multi-event concurrency, or degraded communications.

Uncertainty is represented in two complementary ways depending on the available evidence base. When historical logs, controlled tests, or validated simulations support probabilistic characterization, latency terms and performance measures are treated as random variables and requirement statements are expressed through chance constraints. A generic probabilistic acceptance form is

$$Pr\left(T_{info,s} T_{info,s}^{max}\right) \geq 1 - \varepsilon_s, \quad (2)$$

where $T_{info,s}^{max}$ is the maximum admissible information-to-action time for scenario s, and ε_s is a scenario-specific tolerance for non-compliance that reflects consequence severity and operational risk posture. When only selected

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

stages are dominant for a given scenario, the requirement may be stated in stage-specific form, for example,

$$Pr\left(t_{val,s}+t_{dec,s}+t_{com,s}\le T_{proc,s}^{max}\right)\ge 1-\varepsilon_s, \qquad (3)$$

where $T_{proc,s}^{max}$ is the maximum admissible time allocated to the validation, decision, and communication stages under the scenario considered.

Table 1. *Information metrics catalogue for conceptual PPS design*

Metric / variable	Definition	Measurement source	Typical acceptance target form
t_{det}	Detection latency from event onset to first system indication	Sensor timestamps; event logs	$t_{\text{det}} \le \overline{t_{\text{det}}}(s)$
t_{val}	Alarm validation time from first indication to confirmed event status	SOC logs; operator acknowledgement records	$t_{val} \le \overline{t_{val}}(s)$
t_{fus}	Multi-source fusion time to consolidate signals into a coherent event	Fusion engine logs; analytics pipeline logs	$t_{fus} \le \overline{t_{fus}}(s)$
t_{dec}	Decision and authorization latency to select and approve an action	C2 system logs; dispatch approvals	$t_{dec} \le \overline{t_{dec}}(s)$
t_{com}	Communications latency for disseminating directives and situational context	Network telemetry; message delivery logs	$t_{com} \le \overline{t_{com}}(s)$
t_{disp}	Dispatch and mobilization time from decision to response activation	Dispatch logs; radio logs; unit status logs	$t_{disp} \le \overline{t_{disp}}(s)$
T_{info}	Total information-to-action time $t_{\text{det}}+t_{val}+t_{fus}+t_{dec}+t_{com}+t_{disp}$	Integrated logs across SOC and C2	$T_{info} \le \overline{T_{info}}(s)$ or $Pr(\cdot)\ge 1-\varepsilon_s$
P_D	Probability of timely detection within specified window	Test campaigns; labeled data; simulation	$P_D \ge \underline{P_D}(s)$
P_C	Probability of correct classification (threat vs nuisance, class label)	Labeled data; red-team drills; analytics QA	$P_C \ge \underline{P_C}(s)$
FAR	False alarm rate per sensor or per zone per time unit	SOC alarm logs; analytics output	$FAR \le \overline{FAR}(s)$
A_{com}	Communications availability (successful delivery ratio)	Network monitoring; message receipts	$A_{com} \ge \underline{A_{com}}(s)$
L_{loss}	Message loss rate under nominal/degraded conditions	Network telemetry; stress tests	$L_{loss} \le \bar{L}_{loss}(s)$
W	Operator workload indicator (alerts per unit time, queue length)	SOC dashboards; ticketing system	$W \le \bar{W}(s)$ or queue stability criterion
ε_s	Risk tolerance for probabilistic acceptance	Governance parameter	$Pr\left(T_{info} \le \overline{T_{info}}\right)\ge 1-\varepsilon_s$

When probabilistic estimation is not sufficiently supported by data, uncertainty is handled through conservative bounding rather than by unsupported precision. In such cases, design targets are assigned explicit margins so that the worst plausible latency values under the defined operating context remain within acceptance limits. This approach avoids conceptually fragile designs that are sufficient only under nominal assumptions and provides a practical bridge between early-stage design and later empirical refinement.

The reference information-process model is descriptive. Requirement derivation is performed by a separate procedure, here termed the Scenario-Driven Information Requirement Derivation Method. Its purpose is to convert scenario-specific information bottlenecks into measurable, verifiable, and traceable requirement statements. The method proceeds through five steps.

First, a bounded set of representative scenario classes is defined. These classes are not intended to exhaust all possible attacks, but to capture the dominant operational stressors that shape the information process. Typical classes include covert intrusion, forced entry, insider-assisted action, diversion plus main attack, coordinated multi-point attack, communications degradation, false alarm surge, and sensor degradation or partial failure. Second, for each scenario class, the dominant information bottleneck is identified. This bottleneck may arise from ambiguity-driven validation delay, false alarm saturation, classification difficulty, decision congestion, communications instability, message loss, or prioritization conflict during concurrent events.

Third, the dominant bottleneck is mapped to one or more measurable metrics. For example, ambiguity-driven scenarios primarily map to $t_{val,s}$, $t_{fus,s}$, and $P_{C,s}$; false

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

alarm surge maps to FAR_s, W_s, and validation delay under load; degraded communications map to $t_{com,s}$, $A_{com,s}$, and $L_{loss,s}$. Fourth, acceptance thresholds are assigned to the selected metrics in a form compatible with design review and later verification. The resulting scenario-specific requirement set may be expressed as

$$R_s = \left\{T_{info,s}^{max}, P_{D,s}^{min}, P_{C,s}^{min}, FAR_s^{max}, A_{com,s}^{min}, L_{loss,s}^{max}, W_s^{max}\right\},$$

where R_s is the requirement set for scenario s; $P_{D,s}^{min}$ is the minimum acceptable timely-detection probability; $P_{C,s}^{min}$ the minimum acceptable correct-classification probability; FAR_s^{max} the maximum acceptable false alarm rate; $A_{com,s}^{min}$ the minimum acceptable communications availability; $L_{loss,s}^{max}$ the maximum acceptable message loss rate; and W_s^{max} the maximum acceptable operator-workload level. The specific content of R_s may vary by scenario, but the principle remains constant: every requirement must be tied to an identified bottleneck and stated in measurable form.

Fifth, each requirement is paired with an evidence pathway that makes later acceptance testing or operational monitoring possible. This step converts requirement statements from abstract design intentions into review-defensible claims. The method therefore links each scenario not only to a bottleneck and a metric, but also to a verification route that can be exercised during testing, commissioning, or lifecycle revalidation.

The final element of the methodology is a traceability structure that connects scenario classes, information bottlenecks, measurable requirements, and acceptance evidence. Time-bound requirements are primarily associated with instrumented timed drills, synchronized event logs, and dispatch records. Accuracy-related requirements are associated with labeled datasets, controlled red-team exercises, and validated classification tests. Resilience requirements under concurrency, false alarm load, or degraded communications are associated with stress testing, injected-alarm campaigns, network degradation exercises, and simulation-supported assessment when repeated empirical trials are impractical.

This traceability structure has two functions. Methodologically, it ensures that every requirement introduced at the conceptual stage has an identifiable operational motivation and an evidentiary pathway. Practically, it supports lifecycle revalidation because the same metrics that justify the requirement during design can later be monitored through logs, tests, and after-action review. In this way, information-process requirements become explicit, testable, and revisable components of conceptual physical protection design rather than implicit assumptions embedded in hardware-oriented descriptions.

4. Results

This study yields three methodologically connected outputs for conceptual physical protection system design:

1) a reference information-process model that makes the information-to-action chain explicit;

2) a scenario-specific set of measurable information requirements derived from that model;

3) a traceability structure linking each requirement to a preferred acceptance evidence pathway.

Reference information-process model as a design object

The first result is a reference information-process model that represents information not as a background assumption, but as an explicit part of conceptual design. In this representation, the information chain is structured as a bounded sequence of operational stages extending from event generation and detection to validation, fusion, decision, communication, dispatch, and response activation. As described in Section 3.1, this model captures the forward information-to-action path and the associated lifecycle feedback through logs, after-action review, and parameter update.

The practical value of the model lies in its ability to make time consumption and degradation points visible at the conceptual stage. Instead of treating detection as a single instantaneous event, the model distinguishes between the time required to generate an indication, the time needed to validate and interpret that indication, and the additional time consumed by decision-making, authorization, communication, and dispatch. This separation is important because, in representative operational settings, dominant delays frequently occur after the first alarm indication rather than at the point of sensing itself.

When used as a design object, the reference model supports structured reasoning about where information may be delayed, degraded, or lost. It therefore provides a common analytical basis for identifying bottlenecks associated with alarm ambiguity, false alarm load,

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

concurrent incidents, communication degradation, and operator workload. In this sense, the model is descriptive rather than prescriptive: it defines the information path that must be analyzed before measurable requirements can be assigned.

Scenario-specific measurable information requirements

The second result is a scenario-specific requirement set that expresses information performance in measurable rather than declarative terms. Using the latency decomposition introduced in Eq. (1), the total information-to-action time is treated as a structured sum of stage-specific delays. The probabilistic acceptance forms in Eqs. (2) and (3) then allow these delays to be bounded either at the total-process level or at the level of dominant processing stages, depending on the operational character of the scenario.

On this basis, measurable requirements can be written as explicit performance targets for timeliness, accuracy, and resilience. In practical terms, the requirement set includes bounded total information-to-action time, bounded validation and decision intervals, minimum timely-detection probability, minimum correct-classification probability, maximum false alarm rate, minimum communications availability, and maximum tolerable message loss and workload level, as formalized by Eq. (4). The advantage of this structure is that it transforms conceptual design statements into reviewable and testable claims.

The requirements are scenario-sensitive rather than universal. Different scenario classes stress different parts of the information process and therefore generate different requirement priorities. In ambiguity-dominated scenarios, the primary design concern is not only prompt detection, but also rapid validation and sufficiently accurate classification. In communication-degraded scenarios, communications latency, availability, and message loss become dominant. In scenarios characterized by false alarm surges or concurrent events, operator workload and sustained validation performance under load become central requirement categories. The method therefore does not impose a single fixed target set for all cases. Instead, it produces a structured requirement profile whose content depends on the dominant information bottleneck of the scenario under consideration.

A further result is that these requirements can be stated without collapsing conceptual design into unsupported numerical precision. Where validated logs, controlled trials, or simulation-supported evidence are available, the requirement set can be expressed probabilistically in the form introduced in Eqs. (2) and (3). Where such support is limited, the same structure remains usable through conservative bounding and explicit safety margins. This makes the framework applicable both in early-stage design and in later refinement phases.

Traceability from scenario class to evidence pathway

The third result is a traceability structure that connects scenario classes, dominant information stressors, measurable requirements, and acceptance evidence. This result is important because conceptual requirements are not credible unless they can be linked both to an operational need and to a feasible verification route. In the proposed framework, each requirement is justified by a scenario-defined bottleneck, quantified through one or more metrics, and paired with a corresponding evidence pathway.

This traceability logic allows requirement statements to remain operationally meaningful. A bounded validation time is linked to ambiguity management and can be assessed through instrumented timed drills or synchronized event logs. A classification requirement is linked to interpretation quality and can be supported by labelled test events, controlled exercises, or validated analytics assessment. A communications availability target is linked to degraded-network scenarios and is supported by telemetry, stress testing, or injected degradation exercises. In this way, the requirement object is not limited to a threshold value, but includes the rationale for the threshold and the means by which later acceptance can be demonstrated.

To make the traceability structure operational, Table 2 maps representative scenario classes to dominant information stressors, corresponding requirement priorities, and preferred acceptance evidence.

Table 2 summarizes this traceability structure in operational form. It shows that scenario classes differ not only by external threat mechanism, but also by the type of information stress they impose on the protection process. This mapping provides a disciplined basis for selecting requirement priorities and matching them with appropriate evidence pathways at the conceptual design stage.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

Table 2. *Scenario class to information-requirement mapping and preferred evidence*

Scenario class	Dominant information stressor	Primary information requirements (examples)	Preferred acceptance evidence
Covert intrusion	Weak signatures, ambiguity, delayed confirmation	Tight bounds on t_{det} and t_{val}; minimum P_D; improved P_C for low-signature events	Instrumented detection tests; labeled video/radar datasets; simulation on stealth paths
Forced entry	Clear signatures but short time window; rapid escalation	Bound t_{det}; constrain $t_{dec} + t_{disp}$ to preserve time margin; reliable communications A_{com}	Timed drills; dispatch logs; communications delivery tests
Insider-assisted	Boundary collapse, atypical signatures, access-event dominance	Strong P_C for credential misuse patterns; low t_{val} for access anomalies; integrity/availability of logs	Access-control audit; red-team drills; log forensics and anomaly testing
Diversion plus main attack	Concurrent alarms, saturation, prioritization conflict	Queue stability ($(workload(W))$; bound $t_{val} + t_{dec}$ under load; probabilistic acceptance $Pr\left(T_{\text{inf}\,o} \le \overline{T_{\text{inf}\,o}}\right) \ge 1 - \varepsilon_s$	Multi-event exercises; stress tests with injected alarms; simulation or hybrid evidence
Coordinated multi-point attack	C2 overload, ambiguity, competing priorities	Bound t_{dec} and t_{com} under concurrency; resilience of dissemination A_{com}	Coordinated drills; C2 workload tests; simulation of simultaneous incidents
Communications degradation	Delayed/failed message delivery, fragmented picture	Availability A_{com} and loss L_{loss} targets; tighter bounds on t_{com}; conservative margins in T_{info}	Network stress tests; degraded-mode exercises; telemetry-based validation
False-alarm surge	Operator fatigue, trust erosion, long validation	FAR limit; bound t_{val} as a function of W; improved P_C to reduce nuisance	Log-based measurement; controlled alarm-injection tests; analytics QA
Sensor degradation / partial failure	Increased miss probability, delayed detection	Maintain P_D above threshold under degraded state; redundancy targets; fallback procedures reflected in t_{val} and t_{dec}	Degradation tests; redundancy checks; simulation with failure modes

Practical implications for conceptual design review

Taken together, the three outputs strengthen conceptual design in two ways. First, they make information performance reviewable at the same level of rigor as sensors, barriers, and response arrangements. Second, they provide a structured basis for lifecycle revalidation because the same metrics used to justify conceptual requirements can later be monitored through logs, drills, and stress testing.

As a result, the proposed framework supports a shift from hardware-centered sufficiency claims to evidence-oriented information-process justification. Conceptual design is thereby strengthened not through the addition of complexity for its own sake, but through explicit recognition that information delay, ambiguity, and degradation are often decisive determinants of protective performance.

5. Discussion

The findings of this study indicate that information processes should be treated as a primary design concern in conceptual physical protection system design rather than as a secondary implementation detail. The proposed reference information-process model shows that operational sufficiency depends not only on the presence of sensors, barriers, and response forces, but also on the ability of the protection system to transform heterogeneous observations into timely and reliable action. This point is important because conceptual designs often assume that once an event is detected, the remaining information chain will function with negligible delay or uncertainty. The present results show that this assumption is methodologically weak, since validation, fusion, decision, communication, and dispatch may consume a substantial share of the available interruption margin.

A central implication of the study is that conceptual design should explicitly connect information performance to the broader detection-delay-response logic. Delay resources create practical protective value only if information is processed quickly enough to support timely authorization and mobilization. In this sense, the reference model contributes more than descriptive clarity: it provides a structured basis for identifying where information bottlenecks arise and how they affect protective sufficiency. The model therefore strengthens

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

conceptual review by making information latency and degradation visible at the same analytical level as physical barriers and response arrangements.

The results also support the view that information requirements should be differentiated by scenario rather than stated as universal design aspirations. Different scenario classes stress different parts of the information process and therefore produce different requirement priorities. Covert intrusion and ambiguity-dominated situations place greater emphasis on rapid validation and correct classification, whereas communications-degraded scenarios make transmission delay, availability, and message loss more critical. Similarly, false alarm surges and concurrent events highlight the importance of workload tolerance and sustained validation performance under operational load. The scenario-driven requirement derivation method is therefore valuable because it converts these differences into measurable and reviewable requirement profiles rather than leaving them at the level of general design judgment.

Another important implication is that requirement credibility depends on traceability to evidence. Conceptual requirements are stronger when they are not limited to threshold statements, but are explicitly linked to a scenario rationale, a measurable metric, and a feasible acceptance pathway. In this respect, the proposed traceability structure addresses a common weakness of early-stage design, namely the tendency to formulate information-related expectations without specifying how they will later be tested, monitored, or revalidated. By linking requirement categories to instrumented drills, synchronized logs, stress testing, or simulation-supported assessment, the framework improves the defensibility of conceptual design claims and supports later lifecycle governance.

From a practical design perspective, the study highlights several areas that deserve more deliberate treatment in conceptual review. Alarm validation logic, operator decision support, communications robustness, and dispatch coordination should be regarded as measurable engineering objects rather than as procedural background assumptions. This does not mean that all information variables must be estimated with high numerical precision at the conceptual stage. Rather, it means that information performance should be framed in a disciplined way, with explicit targets, justified margins, and a clear pathway for later refinement when richer empirical evidence becomes available. Such an approach is especially useful in environments where operating conditions, adversary behavior, or communication reliability may change over time.

At the same time, the proposed framework should not be interpreted as a substitute for facility-specific calibration or empirical validation. Its contribution is methodological: it offers a structured way to represent the information-to-action chain, derive scenario-sensitive requirement sets, and connect those requirements to evidence. The framework is therefore most useful as a conceptual design instrument that improves transparency, traceability, and review discipline before detailed site-specific modeling is performed.

Overall, the discussion confirms the main argument of the paper: conceptual physical protection design is strengthened when information processes are modeled explicitly, translated into measurable requirements, and tied to evidence-based acceptance logic. By separating the descriptive role of the reference model from the procedural role of the requirement derivation method, the study provides a clearer basis for integrating information performance into conceptual protection design and for defending those design choices during expert review, testing, and subsequent revalidation

The proposed framework should also be interpreted within its scope. Its contribution is methodological rather than site-specific, and the requirement structures introduced here still require calibration against facility conditions, operating procedures, and validated empirical evidence. In particular, probabilistic formulations depend on the availability of sufficiently reliable logs, controlled trials, or simulation-supported datasets. These limitations do not reduce the conceptual value of the framework, but indicate the need for future work on site-level instantiation and empirical validation.

6. Conclusion

This study has shown that information processes should be treated as explicit design objects in the conceptual design of physical protection systems. The proposed framework demonstrates that protective sufficiency depends not only on sensing, barriers, and response resources, but also on the timely and reliable transformation of observations into authorized action. By representing the information-to-action chain as a structured process, the study makes visible the operational delays and degradation mechanisms that may otherwise remain implicit in hardware-centered design descriptions.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

The main contribution of the study is threefold. First, a reference information-process model was developed to describe the forward path from event generation and detection to response activation. Second, a scenario-driven method was proposed for deriving measurable information requirements from dominant information bottlenecks. Third, a traceability structure was introduced to connect scenario classes, requirement priorities, and preferred acceptance evidence. Taken together, these elements provide a more transparent and reviewable basis for conceptual design decisions.

The results indicate that information requirements should not be formulated as generic aspirations, but as scenario-sensitive and measurable design statements. Depending on the operational character of the scenario, priority may shift toward rapid validation, correct classification, communications robustness, workload tolerance, or bounded end-to-end information latency. This makes conceptual design more defensible because requirement targets are linked not only to abstract performance expectations, but also to identifiable operational stressors and feasible evidence pathways.

At the same time, the framework should be interpreted within its intended scope. Its contribution is methodological rather than site-specific, and the proposed requirement structures still require calibration against facility conditions, operating procedures, and validated empirical evidence. In particular, probabilistic formulations depend on the availability of reliable logs, controlled trials, or simulation-supported datasets. Future research should therefore focus on site-level instantiation, empirical validation, and comparative assessment across different classes of protected facilities.

Overall, the study supports the conclusion that conceptual physical protection design is strengthened when information processes are modeled explicitly, translated into measurable requirements, and linked to evidence-based acceptance logic. This approach improves transparency, supports expert review, and creates a more rigorous foundation for later testing, commissioning, and lifecycle revalidation.

Conflict of Interest

The authors declares that there is no conflict of interest, particularly of a financial, personal, authorial, or any other nature, that could influence the research or the results published in this article.

Funding

The study was conducted without financial support.

Data Availability

The manuscript has no associated data.

Use of Artificial Intelligence

The authors confirms that they did not use artificial intelligence technologies to write this work.

References

1. Akhundov, R., Hashimov, E. (2025), Enhancing the efficiency of the military environmental security system through the implementation of advanced technical means", *Proceedings of International scientific and practical conference: Modeling, Control and Information Technologies*, No. 8, pp. 348–352. DOI: https://doi.org/10.31713/MCIT.2025.108

2. Akhundov, R., Hashimov, E. G., Islamov, I. (2026), "Methodological limitations of normative design of physical protection systems for critical and military facilities in a dynamic threat environment", *International scientific journal* "*Grail of Science*", No.62, pp. 873–889. DOI: https://doi.org/10.36074/grail-of-science.20.02.2026.096

3. Cozens, P., Love, T. (2015), "A Review and Current Status of Crime Prevention through Environmental Design (CPTED)", *Journal of Planning Literature*, No. 30(4), pp. 393–412. DOI: https://doi.org/10.1177/0885412215595440

4. El Wely, I. C., Chetaine. A. (2020), "Analysis of physical protection system effectiveness of nuclear power plants based on performance approach", *Annals of Nuclear Energy*, No. 153, pp. 108051. DOI: https://doi.org/10.1016/j.anucene.2020.107980

5. Garcia, M. L. (2008), Design and Evaluation of Physical Protection Systems. 2nd ed. Elsevier. DOI: https://doi.org/10.1016/C2009-0-25612-1

6. Genserik, L. L. Reniers, A. A. (2014), "Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects", *Process Safety and Environmental Protection*, No. 92(6), pp. 583–589. DOI: https://doi.org/10.1016/j.psep.2013.04.002

8. Akhundov, R., Hashimov, E. G. (2025), Quantitative categorization of facilities and modeling of potential adversaries", *Grail of Science*, No. 60, pp. 469–482.

9. Hashimov, E. et al. (2026), "Research of the efficıency multıservıce networks usıng MIMO technology", *Advanced Information Systems*, No. 10(1), pp. 66-71. DOI: https://doi.org/10.20998/2522-9052.2026.1.08

10. Hashimov, E., Akhundov, R. G., Talibov, A. M., Islamov, I. (2026), "Constrained optimization of an integral security indicator for adaptive management of hazardous facilities", *Grail of Science*, No. (62), pp. 1003–1014.

11. Islamov, I. et al. (2025), "Big data analytics and machine learning for predicting radiation and chemical threats in the military sphere", *Theory and practice of modern science: Collection of scientific papers "SCIENTIA" with proceedings of the X International Scientific and Theoretical Conference*, pp. 30–38. DOI: https://doi.org/10.36074/scientia-26.09.2025

12. Akhundov, R., Islamov, I. (2025), "Military Environmental Security under Radiation and Chemical Threats", *Control and Information Technologies: Proceedings of International scientific and practical conference*, No. 8, pp. 414-419. DOI: https://doi.org/10.31713/MCIT.2025.129

13. Islamov, I. et al. (2025), "Controller-level scalability problems in software-defined networks", *Proceedings of the 13th International Scientific and Technical Conferenc*e, Vol. 1, pp. 70–71. DOI: https://doi.org/10.13140/RG.2.2.31197.88801

14. Islamov, I. et al. (2025), "Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization", *Scientific guidelines: Theory and practice of research – Proceedings of the VI International Scientific Conference*, pp. 185–195. https://doi.org/10.62731/mcnd-03.10.2025

15. Islamov, I. et al. (2025), "Innovative approaches to environmental recovery in conflict-affected areas", *Proceedings of the VII International Scientific Conference*, pp. 180–190. DOI: https://doi.org/10.62731/mcnd-24.10.2025

16. Islamov, I. et al. (2025), "The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology", *Proceedings of the VII International Scientific Conference*, pp. 183–192. DOI: https://doi.org/10.62731/mcnd-10.10.2025

17. Kampova, K., Lovecek, T., Řehák, D. (2020), "Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic", *International Journal of Critical Infrastructure Protection*, No. 30, pp. 100376. DOI: https://doi.org/10.1016/j.ijcip.2020.100376

18. Akhundov, R., Hashimov, E. G., Islamov, I. (2026), "Scenario oriented sufficiency criteria for physical protection systems provide a traceable path from threat classes to design requirements", *Grail of Science*, No. 63. DOI: https://doi.org/10.36074/grail-of-science.06.03.2026.074

19. Kaplan, S., Garrick, B. J. (1981), "On the quantitative definition of risk", *Risk Analysis*, Vol. 1, No. 1, pp. 11–27. DOI: https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

20. Lovecek, T., Ristvej, J., Simak, L. (2010), "Critical Infrastructure Protection Systems Effectiveness Evaluation", *Journal of Homeland Security and Emergency Management*, Vol. 7, No. 1. DOI: https://doi.org/10.2202/1547-7355.1613

21. Mondal, S., Adak, B., Mukhopadhyay, S. (2023), "Functional and smart textiles for military and defence applications", *Smart and functional textiles*, pp. 397–468. DOI: https://doi.org/10.1515/9783110759747-011

22. Řehák, D., Senovsky, P., Hromada, M., Lovecek, T. (2019), "Complex approach to assessing resilience of critical infrastructure elements", *International Journal of Critical Infrastructure Protection*, No. 25, pp. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2019.03.003

23. Rehak, D., Slivkova, S., Janeckova, H., Stuberova, D., Hromada, M. (2022), "Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview", *Energies*, Vol. 15, No. 14, pp. 5276. DOI: https://doi.org/10.3390/en15145276

24. Shoop, B., et al. (2006), "Mobile detection assessment and response systems (MDARS): A force protection physical security operational success", *Unmanned Systems Technology*, Vol. 6230, pp. 668–678. DOI: https://doi.org/10.1117/12.665939

25. Talibov, A. M., Hashimov, E. G., Akhundov, R. G. (2025), "Modeling and forecasting radiological and chemical threats in the military sphere", *Proceedings of the 15th International Scientific and Technical Conference*, Vol. 1, pp. 120–121.

26. Yang, J., Huang, L., Ma, H., Xu, Z., Yang, M., Guo, S. (2022), "A 2D-graph model-based heuristic approach to visual backtracking security vulnerabilities in physical protection systems", *International Journal of Critical Infrastructure Protection*, No 38, pp. 100554. DOI: https://doi.org/10.1016/j.ijcip.2022.100554

27. Zou, B., Yang, M., Zhang, Y., Benjamin, E.-R., Tan, K., Wu, W., Yoshikawa, H. (2018), "Evaluation of vulnerable path: Using heuristic path-finding algorithm in physical protection system of nuclear power plant", *International Journal of Critical Infrastructure Protection*, No. 23, pp. 90–99. DOI: https://doi.org/10.1016/j.ijcip.2018.08.006

Received (Надійшла) 08.02.2026
Accepted for publication (Прийнята до друку) 01.03.2026
Publication date (Дата публікації) 12.03.2026

ISSN 3083-7715 (online) *Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)*
ISSN 3083-7650 (0135-1710)(print) *Management Information System and Devices. 2026. No. 1 (188)*

About the Author / Відомості про автора

Ахундов Раміль Гурбаналі – доктор філософії з національної безпеки та військових наук, професор, Національний університет оборони; Баку, Азербайджан;
Ramil Akhundov – PhD in National Security and Military Sciences, Professor, National Defense University; Baku, Azerbaijan;
e-mail: mr.axundov1@gmail.com
ORCID ID: https://orcid.org/0009-0001-8798-8044

Гашимов Ельшан Гіяс – доктор національної безпеки та військових наук, професор, Азербайджанський технічний університет; професор, Національний університет оборони; Баку, Азербайджан;
Elshan Hashimov – Doctor in National Security and Military Sciences, Professor, Azerbaijan Technical University; Professor, National Defense University; Baku, Azerbaijan;
e-mail: hasimovel@gmail.com
ORCID ID: http://orcid.org/0000-0001-8783-1277

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ ТА ВИЗНАЧЕННЯ ВИМІРЮВАНИХ ВИМОГ ПРИ ПРОЕКТУВАННІ СИСТЕМ ФІЗИЧНОГО ЗАХИСТУ

У дослідженні розглядаються інформаційні процеси на етапі концептуального проектування систем фізичного захисту та їхня роль у перетворенні даних, отриманих від датчиків, вхідних даних оператора та потоків комунікації на своєчасні захисні дії. Особлива увага приділяється тому, що ефективність проекту обмежується не лише датчиками, бар'єрами та силами реагування, а й затримками та невизначеністю, що виникають між виявленням, прийняттям рішення та відправленням сил реагування. ***Метою*** *дослідження є формалізація інформаційних процесів як явних об'єктів проектування та розробка підходу до визначення вимірюваних інформаційних вимог, які можна обґрунтувати та перевірити на етапі концептуального проектування.* ***Завдання*** *полягають у визначенні еталонного робочого процесу від генерації події до активації реагування, розбитті загального часу від інформації до дії на оперативні етапи, врахуванні невизначеності, пов'язаної з помилковими тривогами, неоднозначністю, навантаженням та погіршеним зв'язком, а також ув'язуванні формулювань вимог із доказами прийнятності. У дослідженні використовується* ***концептуальний та методологічний підхід****, заснований на системному аналізі, розбитті сценаріїв, структуруванні затримок та відображенні простежуваності між сценаріями загроз, вузькими місцями, цільовими вимогами та доказами перевірки. У дослідженні* ***розроблено*** *структуровану модель «від інформації до дії», яка чітко визначає етапи зондування, валідації, злиття, прийняття рішень, комунікації та диспетчеризації. На цій основі запропоновано* ***метод*** *перетворення вузьких місць, характерних для конкретних сценаріїв, на перевірювані вимоги щодо своєчасності, точності, повноти та стійкості. Дослідження також визначає практичні форми доказів прийнятності, включаючи навчання з обмеженим часом, вимірювання на основі журналів, стрес-тестування та оцінку з використанням моделювання.* ***Результати*** *показують, що концептуальне проектування стає більш обґрунтованим, коли інформаційні процеси моделюються явно, а не розглядаються як неявні припущення. Запропонований підхід дозволяє проектувальникам обґрунтувати вимірювані вимоги, виявити критичні джерела затримки та підтримати повторну перевірку достатності проекту в умовах мінливих експлуатаційних умов.*

Ключові слова: *система фізичного захисту; концептуальне проектування; інформаційні процеси; перевірка сигналів тривоги; об'єднання даних; управління та контроль; стійкість комунікацій; докази прийнятності.*

Бібліографічні описи / Bibliographic descriptions

Ахундов Р. Г., Гашимов Е. Г. Моделювання інформаційних процесів та визначення вимірюваних вимог при проектуванні систем фізичного захисту. *Автоматизовані системи управління та прилади автоматики*. 2026. № 1 (188). С. 5–16. DOI: https://doi.org/10.30837/0135-1710.2026.188.005

Akhundov, R., Hashimov, E. (2026), "Modeling Information Processes and Deriving Measurable Requirements in Physical Protection System Design", *Management Information System and Devices*, No. 1 (188), P. 5–16. DOI: https://doi.org/10.30837/0135-1710.2026.188.005