Development of a Methodology for Building a Multi-Contour Information Resource Protection System in Cyber-Physical Systems*

Serhii Yevseiev[1†], Serhii Pohasii[1†*], Vladyslav Sokol[1†], Yevhen Melenti[2†] and Stanislav Milevskyi[1†]

[1] National Technical University "Kharkiv Polytechnic Institute", Kyrpychova 2 61002 Kharkiv, Ukraine
[2] National Academy of Security Service of Ukraine, Maksymovycha 22 03022 Kyiv, Ukraine

Abstract

This paper presents a methodology for constructing a multi-layered information security system for cyber-physical systems (CPS), addressing modern challenges related to hybrid and post-quantum threats. The concept is based on five stages: threat probability assessment, preventive modeling, game-theoretical analysis, implementation of post-quantum cryptographic mechanisms (LDPC-based CCS), and multi-contour security architecture development.

The effectiveness of protection is evaluated using KPI(eff), KPIeffinv, and KPInorm indicators, particularly in the context of mobile wireless technologies (LoRa, Sigfox, LTE-M, NB-CPS). A modification of the Go-Back-N protocol is proposed to enhance functional efficiency in wireless memory channels. The proposed models can be applied in the development of secure CPS for critical infrastructure and industrial IoT systems.

Keywords

cyber-physical systems, multi-layered security, post-quantum cryptography, LDPC codes, LPWAN

1. Introduction

In the modern digital society, cyber-physical systems (CPS) play a critically important role in ensuring the functioning of infrastructure facilities, industrial complexes, healthcare institutions, smart cities, and other complex technical systems. These systems integrate computational resources, network infrastructure, and physical entities that interact in real time. Consequently, the security of information resources circulating within CPS has acquired strategic importance, as any violation of data integrity or authenticity can lead to severe consequences — both economic and social.

The threats faced by CPS are complex and multifaceted. They encompass traditional cyber threats (such as malware injection, unauthorized access, data theft or tampering) as well as emerging ones, related to the advancement of quantum computing, targeted attacks on network infrastructure, and hybrid methods involving social engineering. Of particular concern is the vulnerability of mobile wireless communication channels, which are increasingly used in CPS for remote monitoring, control, and automation.

Under these circumstances, there is a growing need for the development of new information security systems capable of ensuring reliable protection of data transmitted within CPS. One promising approach is the construction of multi-contour security architectures that consider both internal and external threats, allow for modeling of adversarial behavior, and support the adaptive formation of preventive measures. When combined with mathematical models and post-quantum

Proceedings of the Workshop on Scientific and Practical Issues of Cybersecurity and Information Technology at the V international scientific and practical conference Information security and information technology (ISecIT 2025), June 09–11, 2025, Lutsk, Ukraine
* Corresponding author.
† These authors contributed equally.
Serhii.Yevseiev@gmail.com (S. Yevseiev); spogasiy1978@gmail.com (S. Pohasii); vladyslav.sokol@gmail.com (V. Sokol); melenty@ukr.net (Y. Melenti); milevskiysv@gmail.com (S. Milevskyi)
0000-0003-1647-6444 (S. Yevseiev); 0000-0002-4540-3693 (S. Pohasii); 0009-0009-9446-2049 (V. Sokol); 0000-0003-2955-2469 (Y. Melenti); 0000-0001-5087-7036 (S. Milevskyi)

cryptographic algorithms, this approach offers a robust foundation for the creation of resilient and effective cybersecurity systems.

Specifically, the study proposes a five-stage methodology for constructing a multi-contour security system for CPS, which includes: assessing the probability of threat realization; forming preventive models based on the Lotka-Volterra equations; evaluating system effectiveness using game-theoretical models; constructing integrated mechanisms for ensuring confidentiality, integrity, and authenticity of information; and developing security strategies based on attacker resources. This structured process enables a systematic and adaptive approach to securing information circulating in CPS.

A central component of the proposed methodology is the use of post-quantum cryptographic systems — in particular, code-based cryptosystems (CCS) utilizing LDPC (low-density parity-check) codes, which enable cryptographic transformations with high performance and moderate energy consumption. This is especially relevant for wireless mobile technologies used in resource-constrained environments, such as LoRa, Sigfox, LTE-M, and NB-CPS, which are widely adopted in low-power wide-area networks (LPWAN). The research demonstrates that implementing cryptosystems based on LDPC codes significantly increases the overall effectiveness of security systems while maintaining acceptable levels of latency and energy consumption.

Special attention is given to modeling the interaction between the adversary and the CPS defense system. To this end, mathematical tools such as game theory are applied, enabling analysis of conflict scenarios and determination of optimal behavioral strategies under constrained resources. The Lotka-Volterra "predator-prey" model has been adapted to cybersecurity tasks, incorporating the hybrid nature and synergy of threats, as well as the financial and computational capabilities of the adversaries.

The study also presents a methodology for calculating the functional efficiency of CPS, considering the probability of packet delivery, packet size, delivery time, system resilience, and more. This methodology forms the basis for KPI-based security analysis, supporting economic justification for the implementation of security technologies and ensuring the reliable operation of CPS in high-threat environments.

Thus, the conceptual framework presented in this work combines advanced techniques in mathematical modeling, post-quantum cryptography, and intelligent risk assessment. It provides the foundation for implementing an effective, flexible, and resilient information protection system for CPS in a time of rapid technological progress and increasingly sophisticated cyber threats. The relevance of this topic is confirmed by the growing number of cyber incidents affecting critical infrastructure, the need to adapt to novel threats (including those emerging with the development of quantum technologies), and the high demands for reliability, energy efficiency, and uninterrupted operation of CPS across various domains of human activity.

2. Materials and methods

The creation of large critical infrastructure systems and the intensification of research into the dynamics of CPS require constant improvement and updating of the current apparatus for modeling and controlling dynamic systems [1, 2; 3; 4, 5, 6]. Recently, the center of gravity of research has shifted towards the development of a methodology for dynamic systems with changing parameters. The use of methods for analyzing such systems allows us to dramatically expand the range of tasks to be solved.

Based on research [7, 8, 9, 10, 11, 12, 13], a new methodology for building an information resource security system is proposed based on methods and models for building multi-circuit security systems,

as well as mechanisms for providing basic security services based on post-quantum algorithms - CCS with LDPC codes, which are characterized by speed and are used in mobile "Internet technologies". Fig. 1–2 shows its structural and logical diagram [5, 6].

It includes five stages [5, 6]:

1) determining the probability of impact of threats on CPS;

2) forming models of preventive measures based on the Lotka-Volterra model;

3) assessing effectiveness based on game-theoretic approach models;

4) building integrated mechanisms to ensure confidentiality, integrity, authenticity and reliability of CPS information resources;

5) determining the state and forming strategies for building multi-circuit protection systems.

Stage 1. Determining the likelihood of threats to the CPS

To determine the probability of the impact of threats on CPS, we use an expert approach to forming a threat classifier. To form an expert assessment, we use a modification of the threat classifier, which is implemented programmatically at the link https://skl.sspu.sumy.ua/threat.

To obtain an assessment of the current state of information security based on the proposed concept of a two-circuit information protection system CPS, let us assume that “1” corresponds to the maximum level of security provided by the security system as a whole, and “0” corresponds to the absence of the required level of information protection.

To determine the probability of a threat being realized with the limiting capabilities of protection A and the limiting capabilities of attack B, we will use the probability density function of the random variable x – F(x). The specified probability is determined by the difference F(B)–F(A), where A is the limiting level of capabilities of the defense side, B is the limiting level of capabilities of the attack side.

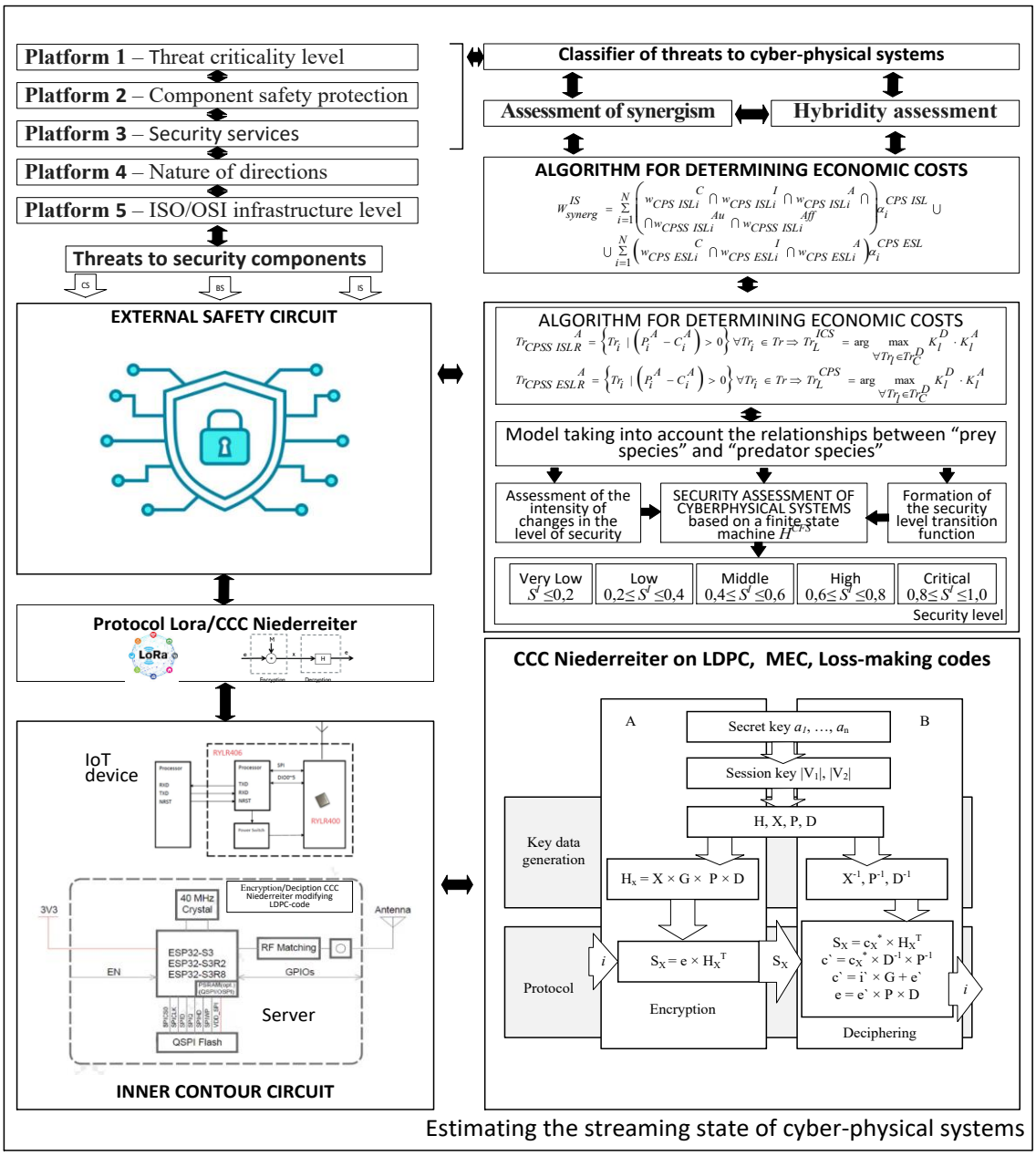

Figure 1: CPS Flow State Assessment

The level of security is defined as the share of those resources protected from cyberattacks as follows:

$$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt. \quad (1)$$

To ensure the security of the entire protection system, we take into account the threats of the internal and external contour:

– threats of the internal contour taking into account hybridity and synergy [5, 6, 13]:

$$W^{CPS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg} = W^{CPS\ ISLC}_{synerg} \bigcap W^{CPS\ \ ISLI}_{synerg} \bigcap W^{CPS\ \ ISLA}_{synerg} \bigcap W^{CPS\ ISLAu}_{synerg} \bigcap W^{CPS\ \ ISLInv}_{synerg}, \quad (2)$$

– threats to the external contour, taking into account hybridity and synergy [13]:

$$W^{SCP\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg} = W^{CPS\ ESLC}_{synerg} \bigcap W^{CPS\ \ ESLI}_{synerg} \bigcap \bigcap W^{CPS\ \ ESLA}_{synerg} \bigcap W^{CPSS\ \ ESLAu}_{synerg} \bigcap W^{CPS\ \ ESLInv}_{synerg}, \quad (3)$$

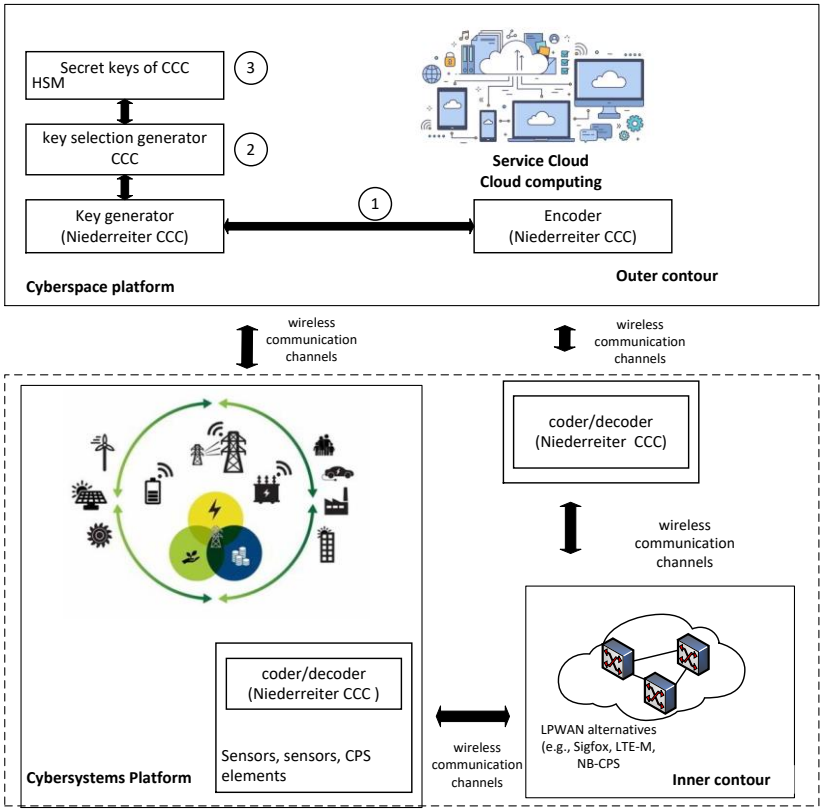

Figure 2: CPS multi-circuit protection system

Analysis of the classification of attackers allows us to form the set {Hj} CPS ISL, which determines the levels of influence on the CPS of the internal circuit, as well as the set {Hj} CPS ESL, which determines the levels of influence on the CPS of the external circuit. We determine the weight coefficient of the attacker's "danger" by the formula [, 5, 6,12]:

$$\gamma^{CPS}_{ICS} = \frac{1}{N}\sum_{i=1}^{N}\gamma^{CPS}_{ICS\ i}, \quad (4)$$

where: $\gamma^{CPS}_{ICS\ i} = \left(\beta^{ICS}_{i} \cup \beta^{CPS}_{i}\right) \times p_{rj} \times r_{motiv}$, – opportunity weights

$\beta^{CPSS\ ISL}_{i} = W^{CPSS\ ISL}_{cp} \bigcap W^{CPSS\ ISL}_{cash} \bigcap T^{CPSS\ ISL}$, offender for CPS ISL and

$\beta^{CPSS\ ESL}_{i} = W^{CPSS\ ESL}_{cp} \bigcap W^{CPSS\ ESL}_{cash} \bigcap T^{CPSS\ ESL}$ CPS ESL (in accordance);

$W^{CPSS\ ISL}_{cp}\left(W^{CPSS\ ESL}_{cp}\right)$ – the offender's computing resources

$W_{cash}^{CPSS\ ISL}\left(W_{cash}^{CPSS\ ESL}\right)$ – economic opportunities of attackers.

The data on the criteria and indicators of expert assessment of its detection are given in the works [5, 6], allowing us to take into account that the attack is determined by a complex criterion that takes into account the cost of implementation and the computational capabilities available to the attacker.

Stage 2. Formation of models of preventive measures based on the Lotka-Volterra model [5, 6]

Based on the proposed approach, the coefficients of the Lotka-Voltera model α=0.39, β=0.32, γ=0.29, φ=0.27 were obtained, which take into account the synergy and hybridity of modern threats, funding for the formation and improvement of the protection system, and also allows determining the financial and computational capabilities of the attacker based on the identified threats.

Development of evolving CPS security models, taking into account the computational capabilities and the direction of targeted cyberattacks.

The number of objects representing attack targets, taking into account their hybridity, can be represented as follows:

$$\tilde{N}_1 = \sum_{i=1}^{Q}\begin{pmatrix} N_{1_i}^{C} \times A_i^{C} + N_{1_i}^{I} \times A_i^{I} + N_{1_i}^{A} \times A_i^{A} + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix}, \quad (5)$$

When implementing the algorithm, it is assumed that the parties to the conflict determine the criticality of cyber threats, which are economically feasible to carry out and/or which need to protect information resources (CPS), first of all. The birth rate of "victims" α is proposed to be used from [6]. To assess the impact of modern threats on protection means β, we will use the expression in [5, 6,7]. To determine the coefficient of computational capabilities of the attacker φ, we will use the classification of attackers, as presented in [5, 6,7],

Table 1 shows the initial data of the criteria and indicators of expert assessment of its location [5, 6].

Table 1

Initial data of criteria and indicators of expert assessment of the weight coefficient of the attacker's computing capabilities

Category	Weighting coefficient evaluation indicators				
	w_{cp}^{CPS}	$\beta_i^{CPS} \in \{\beta_i^{CPS}\}$ TCPS	w_{cash}^{CPS}	prj	rmotiv
Critical	1	1	1	1	1
High	0,75	0,75	0,75	0,75	0,75
Average	0,5	0,5	0,5	0,5	0,5
Low	0,25	0,25	0,25	0,25	0,25
Very low	0,001	0,001	0,001	0,001	0,001

The coefficient of possibility of preventive measures is represented as:

$$\gamma^j = \frac{1}{K \times B}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^{j} \times w_{kg}^{j}\right), \quad (6)$$

Based on the proposed models, a method for assessing the security of CPS based on the Lotka-Volterra predator-prey model is proposed.

Stage 3. Evaluating effectiveness based on game-theoretic models

In [5, 6, 11], models of interaction of antagonistic agents in security systems were proposed. They allowed to obtain solutions for two main problems in the field of cybersecurity: the interaction of a system administrator and an attacker during the organization of the protection of information resources. These problems are considered for two conditions: when the game matrix contains cost estimates of resources and when the matrix reflects the probabilities of threat realization. Pure and mixed strategies are defined for different initial conditions, which allows to exclude irrelevant strategies.

These elements form the basis of a taxonomy of games and their models. Models built on game theory help to identify a number of relevant tasks for ensuring key aspects of security: confidentiality, integrity, availability and authenticity.

Stage 4. Building integrated mechanisms to ensure confidentiality, integrity, authenticity and reliability of CPS information resources [5, 6]

To provide basic services, it is proposed to use Niederreiter CCS, which are discussed in detail in [5, 6, 8, 10, 12].

The formation of the public key for the Niederreiter CCS is carried out by multiplying the masking matrices by the generating or verification matrices:

$$H_{X_{a_i}}^{LDPCu} = X^u \times H^{LDPCu} \times P^u, u \in \{1, 2, ..., r\}. \quad (7)$$

The syndromic sequence is transmitted to the communication channel:

$$S^* = \left(e_n\right) \times H_{X_{a_i}}^{LDPC^T}. \quad (8)$$

where is an additional session key for each information packet. A specific algorithm is used for Niederreiter CCS.

On the receiver side, the authorized user, knowing the masking matrices, applies a fast soft decoding algorithm for decryption.

The use of post-quantum asymmetric cryptosystems allows achieving the required level of security in providing security services. The use of LDPC codes allows for easy integration of mobile wireless technologies based on IEEE802.XX standards.

At stage 5, the state is determined and strategies are formed for building multi-circuit protection systems.

It is proposed to divide the CPS into two subsystems: security and infrastructure. The inner loop of the CPS provides the necessary set of services and functionality, while the outer loop is a management system (MS) built on the basis of a synthesis of wireless networks and cloud technologies.

This approach facilitates the synthesis of internal and external circuits, taking into account the operational efficiency, energy efficiency and relative security of each of them. In addition, it allows you to objectively assess the threats of each circuit, taking into account the computing resources and financial capabilities of attackers. Fig. 1–2 presents a structural diagram of the concept of two-circuit security CPS.

Based on the research conducted, a comprehensive indicator of CPS functional efficiency has been proposed, which allows assessing the overall performance and reliability of the system, taking into account security, confidentiality, economic costs, and quality of service.

To build a model of a complex indicator of CPS functional efficiency taking into account the proposed factors, it is necessary to determine how each of them affects the overall efficiency of the system and combine them into a formula.

The methodology for assessing the functional efficiency of data transmission based on a complex indicator allows you to obtain emergent properties, taking into account the synthesis of a complex indicator of the effectiveness of investments in the security of CPS information resources, the results of the assessment of modern threats in CPS, their hybridity and synergy, as well as the results of an express assessment of the stability and efficiency of the software (or software-hardware) implementation of cryptographic algorithms.

Calculating the efficiency indicator KPI(eff) and taking into account the parameters, the calculation for each technology requires normalization of the parameters.

$$KPI\,(_{eff}) = \frac{R-T}{R} \times B \times P \times KPI_{effin} \times KPI_{norm}, \tag{9}$$

where:

P – probability of package delivery (in fractions of 1).

R – package size.

T – package delivery time (seconds).

B – security system stability for the chosen strategy

To calculate the comprehensive indicator of the effectiveness of investments in ensuring the security of information resources in LPWAN, KPI_{effinv}, a normalized multifactor approach can be used. The calculation uses parameters such as energy efficiency, power consumption, and security system stability, which can affect the security of information resources.

The coefficient of the comprehensive indicator of the effectiveness of security investments KPI_{effinv} (LPWAN) can be represented as a weighted sum of normalized factors:

$$KPI_{effinv} = w_1 \frac{P}{P_{\max}} + w_2 \frac{Ef}{Ef_{\max}} + w_3 (1 - \frac{Ed}{Ed_{\max}}) + w_4 \frac{Bi}{Bi_{\max}} + \ldots + w_m \frac{Bn}{Bn_{\max}}, \tag{10}$$

where:

$$w \in \{1, \ldots m\}, B \in \{i, \ldots n\},$$

Ef – energy efficiency.

Ed – energy consumption.

B_i – stability of the security system.

w_i – weighting factors (determine the importance of each factor).

Parameters marked max are the maximum possible values for normalization. All weighting factors are equal to 0.25.

To calculate the efficiency indicators KPI(eff), it is necessary to use the changed degree of information secrecy when applying crypto-code constructions on the proposed LDPC codes, allowing to provide an integrated increase in the level of reliability (due to error correction properties), efficiency (compatible with symmetric cryptography algorithms in terms of cryptographic conversion speed) and the required level of energy consumption, the results of comparative studies on the criteria of efficiency, energy consumption. Synthesis with the proposed technologies based on CCS (NSCC) will allow not only to provide the required level of the main criteria of modern wireless networks, but also to fundamentally change the methodological foundations of building security systems.

Table 2 shows the results of the analysis of data indicators on KPI_{norm}, KPI_{effinv} and $KPI_{(eff)}$.

Table 2
Performance indicators of low-power wide-range wireless technologies

Technology	Normalized efficiency ratio KPI_{norm}	Investment efficiency ratio KPI_{effinv}	Efficiency ratio $KPI(eff)$
LoRa	0,21	0,794	0,04218
Sigfox	0,14	0,735	0,00050
LTE-M	0,68	0,378	0,00423
NB-CPS	0,56	0,753	0,00691
EC-GSM-CPS	0,35	0,875	0,36610
LoRa HCCC with LDPC codes	0,21	0,919	0,58586
LoRa CCC with LDPC codes	0,21	0,981	0,83385

Thus, Lora technologies with post-quantum protection algorithms - crypto-code constructions with LDPC codes, which allow building asymmetric and/or hybrid cryptosystems (LoRa HSCC and LoRa CCC) allow ensuring the necessary level of efficiency in the post-quantum period. This takes into account not only the possibility of counteracting targeted (mixed) attacks with signs of hybridity and synergy (the possibility of integration with social engineering methods), but also increasing the level of reliability and the possibility of their use in smart technologies with limited energy-intensive requirements. To increase the functional efficiency indicator KPI(eff) CPS, it is proposed to use data exchange management protocols that will ensure the necessary indicators: data transmission efficiency, noise immunity and security.

One such protocol is the Go-Back-N loopback data exchange control protocol, which allows for the required level of functional efficiency of the CPS.

To evaluate the CPS of continuous frame feedback control, the efficiency is calculated as follows [14, 15, 16, 17] A modification of the Go-Back-N method formula involves retransmission of the packet window when an error is detected, which may affect the probability of successful delivery (P) which may slightly decrease if the error is not detected often, retransmissions may increase the delivery time T, and energy consumption increases due to retransmissions.

The generalized formula has the following form:

$$KPI\left(_{eff\_GBN}\right)=\frac{R-T}{R}\times B\times P\times(1-\mathrm{P}_{\mathrm{retry}})\times KPI_{effin}\times KPI_{norm}, \tag{11}$$

where $\mathbf{P}_{\mathrm{r}\,etry}$ factor takes into account the probability of retransmission of packets in the event of an error. This factor is critical for "Go-Back-N" because it must take into account the probability that an error could lead to a retransmission.

Fig. 3 shows the results of the investment efficiency assessment and the overall data transmission efficiency for the "Go-Back-N" method, taking into account the features of feedback and continuous frame transmission using the memoryless data transmission model.

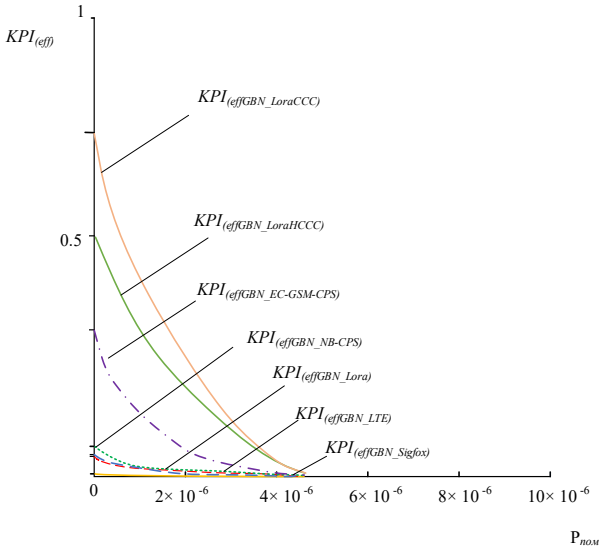

Figure 3: Evaluation of the complex performance indicator in memoryless channels

To calculate $KPI_{(eff)}$ by the Return-to-N method for channels with memory taking into account the probability of packet errors, taking into account the probability of an error within a packet, the mathematical expectation of the length of the packet errors, and the standard deviation of the values given in Table 3, we will use the following modified formula

$$\begin{aligned} KPI\left(_{eff\_GBN\_\mathrm{mem}}\right)&=\left(\frac{R-T}{R}\right)\times B\times P\times \\ &(1-\Phi(\frac{P_e-E(L)}{\sigma(L)}))\times KPI_{effin}\times KPI_{norm}, \end{aligned} \tag{12}$$

where P_e – probability of an error in the package.

$E(L)$ – mathematical expectation of the length of the error packet.

$\sigma(L)$ – standard deviation of the error packet length, which takes into account the variability in the number of packets that can be lost due to errors.

$\Phi(\frac{P_e - E(L)}{\sigma(L)})$ – cumulative distribution function of the normal distribution (Laplace function), which takes into account the probability of an error in the batch (the closer the function value is to 1, the greater the probability that errors will be detected and corrected).

Table 3 compares the efficiency ratios for LPWAN technologies, in particular for the "Go-Back-N" protocol in memoryless and memory-based channel models.

Table 3
Comparative table of efficiency coefficients of LPWAN technologies using the Go-Back-N method in channels without and with memory.

Technology	$KPI_{(eff)}$	$KPI_{(eff\_GBN)}$	$KPI_{(eff\_GBN\_mem)}$
LoRa	0,04218	0,03796	0,04639
Sigfox	0,00503	0,00452	0,00552
LTE-M	0,04234	0,03801	0,04654
NB-CPS	0,06902	0,06212	0,07591
EC-GSM-CPS	0,36609	0,32948	0,40270
LoRa CCC with LDPC codes	0,58586	0,52727	0,64444
LoRa HCCC with LDPC codes	0,83385	0,75047	0,91723

Analysis of Fig. 3 and Table 3 shows that the use of crypto-code structures with LDPC codes (LoRa CCC with LDPC codes) and hybrid crypto-code structures with LDPC codes (LoRa CCC with LDPC codes) increase the complex efficiency index by an order of magnitude by providing security services (confidentiality, integrity and authenticity of data). However, in the conditions of using a full-scale quantum computer and additional use of the damage algorithm (multi-stream cryptography), the complex efficiency index decreases by 9% (LoRa HCCC with LDPC codes KPI_{eff} is 0.7505, and LoRa CCC with LDPC codes KPI_{eff} is 0.5273), but at the same time the required level of security is ensured.

Fig. 4 shows the results of the investment efficiency assessment and the overall data transmission efficiency for the "Go-Back-N" method, taking into account the features of feedback and continuous frame transmission using the data transmission model with memory.

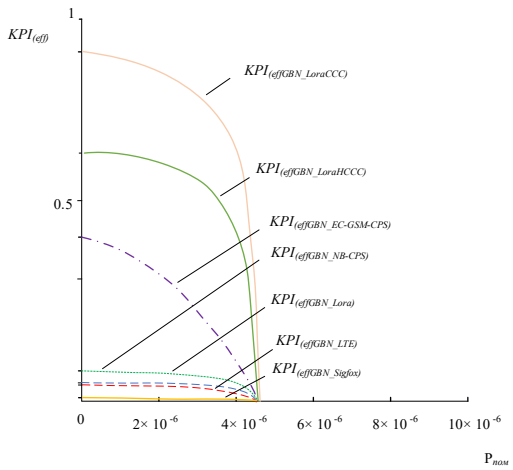

Figure 4: Evaluation of the complex performance indicator in channels with memory.

The channel model with memory provides a more "objective" model of real communication channels, as it takes into account the possibility of packetization of errors in the channel. The results shown in Fig. 4 and Table 3 confirm that the complex efficiency indicator, as well as the channel model without memory, increases by 10% (LoRa HSCC with LDPC codes KPI_{eff} is 0.917235, and LoRa CCC with LDPC codes KPI_{eff} is 0.644446). However, the necessary level of security is ensured, which in the conditions of the emergence of a full-scale quantum computer (post-quantum period) and the action of targeted (mixed) attacks with signs of hybridity and synergy provides the necessary level of security of the CPS infrastructure elements.

The proposed methodology for assessing the flow state of an automated data transmission system via wireless communication channels provides an increased level of objectivity in assessing not only targeted attacks (taking into account the financial, computational and human capabilities of the attacker). In addition, it provides an analysis of critical points (points of possible unauthorized penetration into the infrastructure), as well as the ability to counter cyberattacks based on special mechanisms, taking into account the security levels that are defined.

3. Conclusion

This study presents a comprehensive methodology for constructing a multi-contour information security system for cyber-physical systems (CPS), addressing the current challenges associated with hybrid and post-quantum threats. The proposed approach is strategically significant for the protection of infrastructure operating in a dynamic technological landscape characterized by rapid growth in wireless communication and computing technologies.

The methodology is structured around five interrelated stages: assessing the probability of threat realization, modeling preventive measures using the Lotka–Volterra equations, applying game-theoretical models to evaluate protection strategies, implementing post-quantum cryptographic mechanisms based on LDPC codes, and designing an adaptive multi-contour CPS security architecture. This transition from reactive to proactive cybersecurity management ensures both real-time threat mitigation and systemic resilience.

The first stage introduces a method for estimating the likelihood of threat implementation using a probability density function that compares the defensive and offensive capabilities. The model considers both external and internal threats and incorporates hybrid and synergistic characteristics of attacks, offering a robust and realistic assessment framework. This dual-contour perspective enables the differentiation between system-level vulnerabilities and network-level exposures.

At the second stage, preventive actions are modeled through a modified Lotka–Volterra system, traditionally used to represent "predator-prey" dynamics. This model allows the representation of economic and computational resources available to both attackers and defenders. Key coefficients (α, β, γ, φ) reflect the aggressiveness, resilience, and scalability of both threats and defensive mechanisms, providing a simulation framework for developing rational defense prioritization.

The third stage employs game theory to analyze the interactions between attackers and system administrators, allowing the definition of optimal (pure or mixed) strategies under conditions of uncertainty and limited resources. This approach is particularly useful for modeling real-time decision-making and enables the elimination of non-viable defense scenarios in complex adversarial environments.

In the fourth stage, the research focuses on designing cryptographic mechanisms that ensure confidentiality, integrity, authenticity, and trustworthiness of transmitted data. The study justifies the use of CCC Niederreiter built on LDPC codes, which demonstrate high efficiency, fault tolerance,

and low computational overhead. These cryptosystems are compatible with resource-constrained mobile and wireless devices and provide resilience to attacks from quantum computing.

The fifth and final stage proposes a dual-contour architectural model for CPS, separating the system into operational (internal) and managerial (external) subsystems. The internal contour manages service delivery and real-time control, while the external contour integrates wireless and cloud-based technologies for remote administration and communication. This division ensures layered security and allows for differentiated risk assessment and mitigation strategies for each subsystem.

In addition to the architectural framework, the paper introduces a novel method for evaluating CPS functional efficiency under adversarial conditions. The proposed KPI(eff) metric aggregates parameters such as data delivery probability, packet size, delivery time, security robustness, and energy efficiency. It was demonstrated that the integration of LDPC-based cryptographic mechanisms in LoRa wireless technologies significantly improves these performance indicators compared to other LPWAN alternatives (e.g., Sigfox, LTE-M, NB-CPS).

Furthermore, the study assesses the impact of modifying the Go-Back-N protocol for wireless channels with and without memory. It was shown that accounting for retransmission probabilities and packet error rates improves reliability and bandwidth utilization in noisy environments, thus enhancing communication stability.

The major scientific contribution of this work lies in the formalization of a layered security strategy for CPS using mathematical threat behavior models, advanced cryptographic techniques, and real-time efficiency evaluation tools. This approach provides a framework for adaptive security systems that not only defend against external intrusions but also dynamically respond to evolving threats and self-correct their operations.

The findings of this research are applicable to the design of secure CPS across a range of industries, including smart grids, industrial automation, e-health, intelligent transport systems, military technology, and smart cities. They also open new avenues for future studies in adaptive self-organizing cybersecurity mechanisms, hybrid cryptographic systems, and resistance to adversarial AI and quantum computing-based attacks.

In conclusion, the proposed methodology increases the overall efficiency of CPS security systems by 4.78% (based on KPI calculations) and lays the foundation for a paradigm shift from passive defense to emergent security governance. In an era where digital resources are strategic assets, such an approach ensures sustainable, secure, and intelligent operations of next-generation CPS.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Holovka A. (2016). Information threats in a globalized world: economics, politics, society (experience of Ukraine). Baltic Journal of Economic Studies, 2 (3), 42 – 47. doi: https://doi.org/10.30525/2256-0742/2016-2-3-42-47.

[2] DeBenedictis K.. Russian “Hybrid Warfare” and the Annexation of Crimea. Bloomsbury Publishing. 2021. doi: https://doi. org/10.5040/9780755640027.

[3] Haig Z., Hajdu V. (2017). New Ways in the Cognitive Dimension of Information Operations. Land Forces Academy Review, 22 (2), 94–102. doi: https://doi.org/10.1515/raft-2017-0013.

[4] Forrest J. Digital influence warfare in the age of social media. Praeger, 2021. 303.

[5] Pohasii S., Yevseiev S., Milov O. and others. Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies, 2020. № 4 (104). P. 15-29. (індексується базою Scopus)

[6] Pohasii S., Yevseiev S., Ryabukha Y. and others. Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies, 2021. № 6/2 (114). P. 30-43. (індексується базою Scopus)

[7] Ekshmidt V. (). Verbal Manipulation: Persuasion and Suggestion. Movni i kontseptualni kartyny svitu, 1, 2015. 275–281. URL: http://nbuv.gov.ua/UJRN/Mikks_2015_1_31.

[8] Kolmogorova A. V., Kalinin A. A., Malikova A. V. (2018). Linguistic principles and computational linguistics methods for the purposes of sentiment analysis of cyrillic texts. Current Issues in Philology and Pedagogical Linguistics, 1 (29), 139 – 148. doi: https://doi.org/10.29025/2079-6021-2018-1(29)-139-148.

[9] Lytvyn V., Vysotska V., Uhryn D., Hrendus M., Naum O. (2018). Analysis of statistical methods for stable combinations determination of keywords identification. Eastern-European Journal of Enterprise Technologies, 2 (2 (92)), 23–37. doi: https:// doi.org/10.15587/1729-4061.2018.126009.

[10] Molodetska-Hrynchuk K. (2017). Outreaches content tracing technique for social networking services. Radio Electronics, Computer Science, Control, 2 (41), 117 – 126. doi: https://doi.org/10.15588/1607-3274-2017-2-13.

[11] Savchuk V. S., Hryshchuk R. V., Hryshchuk O. M., Musienko A. P. (2018). Intelligent system for evaluating destructive nature of text content of social networks based on fuzzy logic. Science-based technologies, 38 (2). doi: https://doi.org/10.18372/2310- 5461.38.12838.

[12] Palchuk V. (2017). Methods of Content-Monitoring and Content-Analysis of Information Flows: Modern Features. Academic Papers of The Vernadsky National Library of Ukraine, 48, 506–526. doi: https://doi.org/10.15407/np.48.506.

[13] Snitsarenko P., Nakonechnyi V., Mikhieiev Y., Hrytsiuk V. (2019). The approach to automated internet monitoring system creation. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/ atit49449.2019.9030446

[14] Kuznetsov O. O., Oliinykov R. V., Horbenko Yu. I., Pushkariov A. I., Dyrda O. V., Horbenko I. D. Justification of requirements, design, and analysis of promising symmetric cryptographic transformations based on block ciphers. Bulletin of the National University "Lviv Polytechnic". Computer Systems and Networks. 2014. № 806, c. 124 – 141

[15] Sobchuk V. V., Laptev O. A., Pohasii S. S., Barabash A. O., Salanda I. P. Mathematical model for protecting an information network based on hierarchical hypernetworks. Scientific discussion. Praha, Czech Republic, 2021. Vol 1. No 61. P. 31 – 36.

[16] GOST 34.601-90. Information technology. Set of standards for automated systems. Automated systems. Stages of development. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=53626

[17] Ian F Akyildiz, Tommaso Melodia, and Kaushik R Chowdury. Wireless multimedia sensor networks: A survey. IEEE Wireless Communications, 14(6):32–39, 2007.