Model of intelligent protection for temperature-based transmitting channels in laboratory sensor networks with embedded information processing

Yaroslav Tarasenko[1,†], Serhii Orlov[1,†], Oleh Chervotoka[1,†], Oleh Dmitriiev[1,*,†], Nataliia Lada[1,†] and Serhii Osadchyi[2,†]

[1] *State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Vyacheslava Chornovola 164 18000, Cherkasy, Ukraine*

[2] *Central Ukrainian National Technical University, pr. University, 8 25006, Kropivnitsky, Ukraine*

Abstract

The paper is devoted to solving the relevant problem of protecting information from leakage through thermal channels in systems with built-in information processing means. In the work it is presented a hierarchical modular model of intelligent protection against information leakage through temperature-based transmission channels in IoT-oriented laboratory sensor networks with embedded information processing increase the reliability of information protection during laboratory tests against leakage through thermal channels by means of intelligent control of active protection processes. The results have proved the increase in the reliability of information protection during laboratory tests against leakage through thermal channels up to 20% in comparison with analogue protection systems. The means of intelligent control of active protection processes made it possible to develop an adaptive model of thermal covert channel protection. The proposed model of intelligent protection for temperature-based transmitting channels in laboratory sensor networks is based on intelligent management decision-making by a cyber-physical protection system through parametric linking of input data and physical changes in active protection. The proposed approach integrates three key components of input data: input physical, analytical and predictive parameters. It takes into account the influence of input physical parameters on output physical parameters as well as on the input predictive and analytical parameters. The protection system operates autonomously, adapting to input parameters, while ensuring the safety of laboratory equipment. The NIST statistical tests are used for detecting anomalies in thermal channel during the active protection is used. The contribution of this work lies in advancing intelligent active protection of IoT-based laboratory systems, ensuring reliable operation under security threats.

Keywords

thermal-side channel, sensor networks, cyber-physical systems, adaptive security, active defense systems, total laboratory automation, IoT oriented laboratory systems, information leakage prevention

1. Introduction

The current pace of technical development, production volumes and diversity of high-tech equipment require the development of highly effective procedures and means of confirming the quality of such products. Technologies for confirming quality and conducting technical examinations by research laboratories need significant improvement in terms of automation and intellectualization of processes. The paper [1] defines the prospects for the development of so-called total laboratory automation (TLA) technologies. It notes the important advantages of using these technologies, which include high efficiency and accuracy, reduced cost and time of laboratory testing, and the ability to manage data. The use of TLA is an important component of the

AISSLE-2025: International Workshop on Applied Intelligent Security Systems in Law Enforcement, October, 30–31, 2025, Vinnytsia, Ukraine

[1,*] Corresponding author.

[†] These authors contributed equally.

yaroslav.tarasenko93@gmail.com (Y. Tarasenko); w7nner@gmail.com (S. Orlov); ron1978@ukr.net (O. Chervotoka); dmitriievoleh@gmail.com (O. Dmitriiev); ladanatali256@gmail.com (N. Lada); srg2005@ukr.net (S. Osadchyi)

0000-0002-5902-8628 (Y. Tarasenko); 0000-0003-3840-4089 (S. Orlov); 0000-0002-1083-4178 (O. Chervotoka); 0000-0003-1079-9744 (O. Dmitriiev); 0000-0002-7682-2970 (N. Lada); 0000-0002-1811-3594 (S. Osadchyi)

competitiveness of research laboratories. The fact that TLA operates at three stages of data processing during laboratory testing (pre-analytical, analytical and post-analytical) explains the extreme relevance of information security measures during processing.

TLA procedures are inextricably linked to the use of cyber-physical systems that operate in laboratories and are controlled by corresponding information systems. These latest systems are based on IoT technology and include built-in information processing systems. As noted in [1], it is IoT integration that is a priority area for unifying the laboratory environment. Embedded information processing systems are necessary for real-time test process management and are the basic hardware for the application of artificial intelligence in the implementation of TLA approaches.

Along with the advantages of using IoT-oriented sensor networks, there is a threat of information leakage through a number of channels. Work [2] provides a classification of information leakage channels: network-based, host-based and physical. Since a cyber-physical system is used for TLA application, network channels are associated with physical devices. Physical channels include electromagnetic, power, thermal, acoustic, and optical channels. The thermal channel is one of the least common but most vulnerable in the context of the system under consideration. The architecture of a cyber-physical system with built-in information processing means involves placing various sensor nodes and test devices at a short distance from each other. The laboratory management system involves the use of video surveillance and, in some cases, thermal imaging. This situation is highly conducive to information leakage via thermal channels. Work [2] explains possible information leakage procedures, according to which the presence of a built-in laboratory data processing processor and temperature sensors as components of devices that are nodes of a sensor network fully satisfies the necessary and sufficient conditions for a full-fledged attack.

An analysis of the most modern trends in the development of the material base of research laboratories and challenges to the implementation of TLA technologies allows us to substantiate the problem of developing technologies for protecting IoT-oriented laboratory sensor networks with built-in information processing systems from leakage through thermal channels.

2. Background and related work

The problem of protecting information from leakage through thermal channels in systems with built-in information processing means is relevant and is being addressed by the scientific community. Among the works describing approaches to solving this problem is [3]. The authors propose protecting the thermal channel of potential leakage of sensitive information for embedded systems through improved thermal management using digital twin technology. The main disadvantage of using such protection in the operation of equipment with embedded information processing systems is the increase in data processing time. The speed of management decisions and response to environmental factors during laboratory tests is a critical parameter. In this case, the use of technologies based solely on detecting interference in the system is impractical. It is important to use active protection measures that do not reduce the speed of operations performed by the processor embedded in the laboratory equipment.

In [2], a number of active protection approaches are proposed, among which two are worth considering in the context of information leakage through thermal channels. The approaches of interest are known as shielding and jamming. The advantages of these approaches make it possible to develop an active protection system. Such an active protection system must function on an appropriate basis, which is an intelligent system for detecting incidents and managing active protection processes. Modern developments in active protection systems do not take into account the need for adaptability. Thus, in [4], one of these approaches, jamming, is used. An important drawback of the authors' proposed development when applied to the task of laboratory testing with an IoT-oriented sensor network is reliability. The paper also notes that the bandwidth of thermal data transmission channels can reach more than 45 bits/s. The iterative nature of the described approach, which consists of initial analysis and subsequent channel jamming, allows a significant amount of information to be transmitted. The lack of noise adaptability and the ability to control it opens up vulnerabilities in the selection and overcoming of thermal noise frequency. Such characteristics of the system require its

significant improvement in the direction of intelligent control and increased adaptability to input parameters, which will increase its reliability. There is a need for self-diagnosis of the system with the possibility of further intelligent control of protection processes, which necessitates both the detection of incidents and the execution of actions with the data transmission channel. In [5], machine learning approaches are used for adaptive protection control, but its focus is on energy efficiency rather than equipment reliability. Work [6], like [4], is based on the jamming approach, but has the same shortcomings for solving the task at hand, where it is important for the autonomous adaptive protection control system to make management decisions.

A significant number of works are devoted to incident detection procedures. Work [7] is devoted to risk assessment in IoT-oriented systems, taking into account various types of threats, including physical and remote access threats. The assessment approach proposed in the work is based on modelling behavior and determining the possibility of threats being realized, which is similar in principle to the modelling of a digital twin in work [3]. Promising areas for threat detection in IoT-oriented systems in [8] include automated incident detection and the use of machine learning algorithms. Work [9] evaluates the characteristics of modelling so-called honeypots, which can be used in the process of forming the analytical apparatus of a neural network when assessing risks to the system by evaluating influencing factors.

Work [10] is devoted to improving the efficiency of continuous transmission of multidimensional signals. Taking into account the thermal signal and its possible improved transmission is important for increasing the reliability of active protection and improving operating conditions [4].

A study of current sources revealed a lack of works dedicated to protecting information from leakage through thermal channels in IoT-oriented systems with built-in information processing capabilities. An insufficiently studied issue of intelligent response to detected incidents through the use of an active adaptive protection system in laboratory testing tasks using an IoT-oriented sensor network and embedded information processing systems has been identified.

The contradiction that needs to be resolved lies in the need to ensure maximum reliability of protection while maintaining the safety of equipment operation.

The aim of the work is to increase the reliability of information protection during laboratory tests against leakage through thermal channels by means of intelligent control of active protection processes. To achieve this goal, the following scientific tasks were formulated:

- To develop a parametric model for controlling the physical component of an IoT-oriented device's active protection system with built-in information processing capabilities.
- To develop a model for intelligent measurement of input physical parameters.
- To describe the procedure for making management decisions.
- To propose a forecasting model for the application of active protection.

3. Formation of an intelligent protection model

The protection system for the thermal data transmission channel in IoT-oriented sensor systems is characterized by three components: an active physical countermeasure system, an intelligent countermeasure process management system, and an intelligent analytics system. The management system controls the physical protection elements in real time.

Protection can be applied to IoT-oriented equipment with built-in information processing capabilities – a built-in specialized microprocessor (system in package or SiP). Such a processor heats the cover panel of IoT-oriented equipment. The transmission of information bits occurs due to the fact of heating or cooling of the panel (0 or 1), as well as due to the speed of heating and cooling.

Intelligent protection involves responding to external factors and adjusting the system accordingly by analyzing data using neural network technologies. The fundamental difference of the proposed development lies in the ability to automatically adapt the physical protection of the

thermal data transmission channel from embedded computing systems in real time. The general model of intelligent protection is modular and is represented by the formula:

$$D=f(F,K,P), \tag{1}$$

where F is the analytics model for threat detection, K is a model for intelligent management decision-making regarding system protection, P is a model for predicting the behavior of an IoT-oriented sensor network, f is the integration function based on a parametric control model that takes physical parameters into account.

Since the sensor network is a cyber-physical system, data leakage can occur through neighboring devices equipped with thermal sensors or through surveillance devices, including thermal imaging equipment. To prevent this, it is necessary to consider the physical component of protection (Fig. 1), which is controlled by the intelligent component.

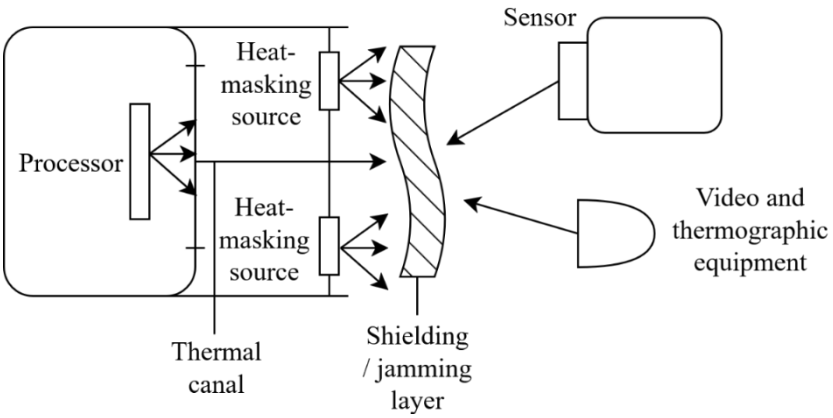


Figure 1: Graphical representation of the physical component of the protection model.

The intelligent system requires physical management and analytical components. The physical component is responsible for preventing information leakage at the physical level, the management component analyses the input parameters and makes the appropriate decision, and the analytical component conducts research on the bit stream. The general diagram of the proposed intelligent protection of the thermal information transmission channel is shown in Figure 2.

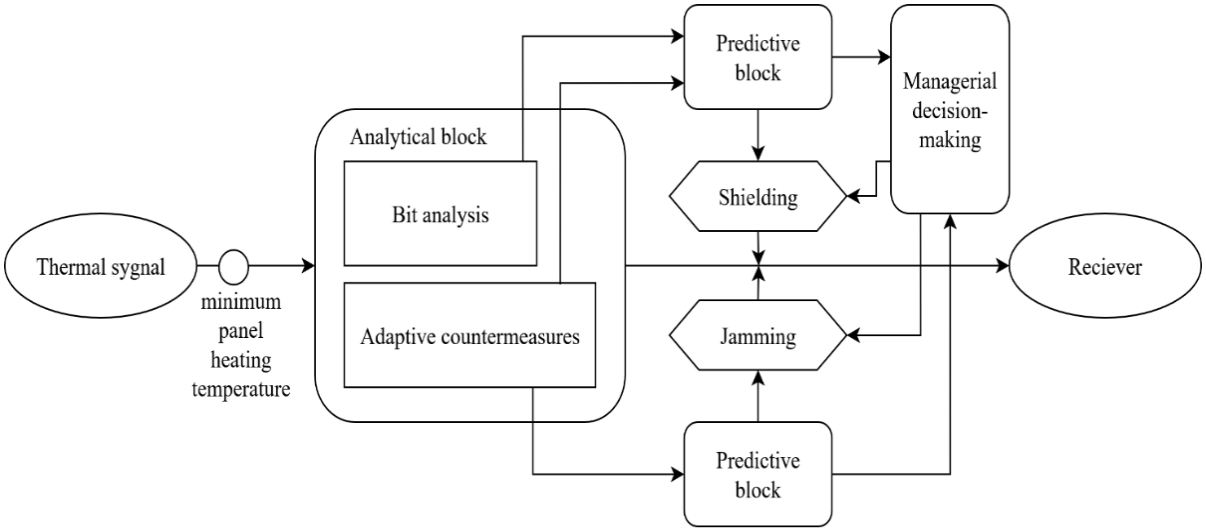


Figure 2: Structural-logical diagram of the thermal channel protection process.

The protection system must be autonomous and not connected to an IoT-oriented sensor system in order to prevent its compromise. Such requirements necessitate the intellectualization of the protection system.

An important aspect is adaptation to the type of processor, channel bandwidth, and data transmission method through the analysis of input parameters, which are then converted into physical variable parameters of the adaptive physical countermeasure system.

3.1. Parametric model for controlling the physical component

The protection system is activated after an event occurs in which the temperature of the case panel may differ from the temperature of the built-in information processing device. Such an event is one of the input parameters of the parametric model. When the panel's minimum heating temperature is exceeded, the analytical system is activated. The time required to perform analytical actions can reach 5 hours, since, according to [3], the information transfer threshold can be 20 bits/hour. The analytical system requires at least 100 bits of information to form conclusions. During this time, certain information can be transmitted, so the protection system must be enabled. A permanently enabled system can damage the components of the test laboratory equipment and therefore must respond adaptively to changes in input parameters.

The moment of activation of the protection system is determined using a numerical temperature model that describes the thermal regime of the surface of the laboratory equipment housing panel, the temperature of which rises under the influence of temperature fluctuations caused by the heating of the processor (built-in information processing system).

The heat flow of the case panel under the action of an internal heat source is calculated using the differential equation of unsteady heat conduction for a flat plate:

$$\frac{\partial T}{\partial \tau} = \alpha \frac{\partial^2 T}{\partial x^2}, \tag{2}$$

where T is the temperature, τ is time, x is the thickness of the case panel, α is the thermal conductivity coefficient.

Equation (2) is solved using the numerical method of finite differences with an implicit calculation scheme using a non-uniform grid. The result of the solution is the dynamics of the temperature change of the case panel surface under the action of the built-in information processing device over time (Fig. 2). This determines the minimum heating temperature of the case panel for the protection system to start.

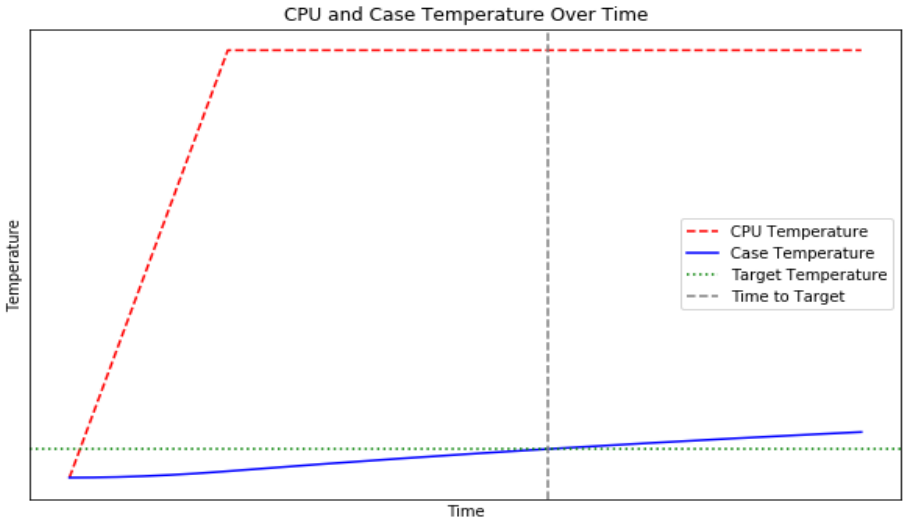


Figure 3: Dynamics of changes in the temperature of the case panel surface under the influence of a built-in information processing device over time to determine the minimum heating temperature of the panel.

The increase in temperature on the surface of the case panel is recorded by temperature sensors, and when it reaches a certain value (Target Temperature) at a certain point in time (Time to Target), active protection is activated.

The intelligent control approach requires consideration of the correlations between the input physical parameters and the resulting adaptive changes in the protection system. For automated control, it is necessary to form a set of parameters that affect the resulting states of the system. Input parameters are divided into three classes: physical parameters, analytical parameters, and predictive parameters (Table 1).

Table 1
Input and output parameters of the model

Designation	Name
	Input physical parameters (F)
f_1	Panel heating temperature
f_2	Panel heating intensity
f_3	Temperature change frequency
f_4	Transition through the minimum panel heating temperature
	Input analytical parameters (K)
k_1	Result of the current NIST statistical test
k_2	Results of previous NIST statistical tests
	Input predictive parameters (P)
p_1	Channel noise level
p_2	Channel shielding level
p_3	Potential damage to equipment from additional heat sources
p_4	Processor temperature increase
p_5	Frequency of panel temperature fluctuations
p_6	Air layer temperature increase
	Output physical parameters (L)
l_1	Distance from the panel to an additional heat source
l_2	Power of additional heat sources
l_3	Number of simultaneously activated heat sources
l_4	Distance between heat sources
l_5	Duration of operation of additional heat sources
l_6	Frequency of switching on additional heat sources

A graphical representation of the relationship between the elements of the intelligent protection model, taking into account the input and output parameters, is shown in Figure 4.

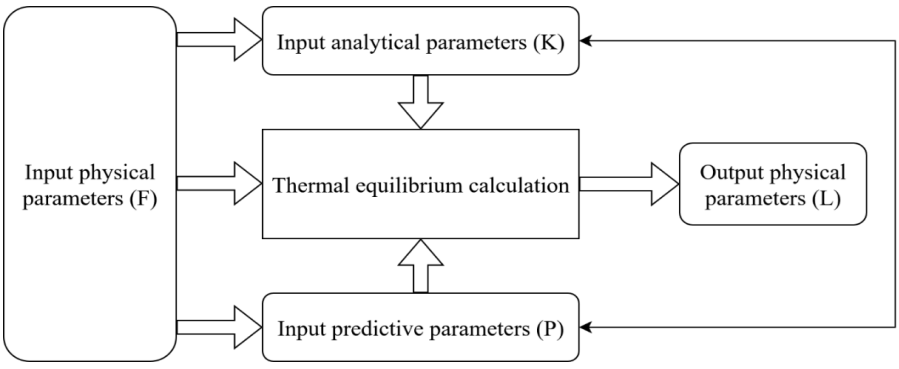


Figure 4: Connection between elements of the intelligent protection model, taking into account input and output parameters.

The main task of the model is to maintain thermal equilibrium in the shielding/jamming layer space zone. To accomplish this task, it was considered the non-stationary thermal conductivity from the panel, which is heated according to the formula:

$$\frac{\partial T}{\partial \tau} = \alpha \frac{\partial^2 T}{\partial x^2} + \frac{f_2}{pc}, \tag{3}$$

where p is the density of the material, c is the heat capacity, f_2 is the heating intensity of the panel.

If the system investigates thermal equilibrium at a point on the shielding/jamming layer, air density is used.

In addition to panel heating, the influence of additional heat sources from the active protection system must be taken into account. The influence of additional heat sources is modelled using the following formula:

$$Q(x,t)=\sum_{i=1}^{N} l_{2i}(t)\cdot\delta(x-x_i), \tag{4}$$

where x_i is the coordinate point of the additional source, $\delta(x-x_i)$ is function that models the additional source, l_2 is the power of additional heat sources.

Additional heat sources are integrated into the heat conduction equation as follows:

$$\frac{\partial T}{\partial \tau}=\alpha\frac{\partial^2 T}{\partial x^2}+\frac{1}{pc}\left(f_2(t)+\sum_{i=1}^{N} l_{2i}(t)\cdot\delta(x-x_i)\right). \tag{5}$$

The boundary conditions for equations (2-5) are conditions of the III kind: on the inner surface ($x=0$) – convective heat exchange with embedded information processing device; on the outer surface ($x=L$) – convective heat exchange with the ambient air.

The general form of the parametric model is presented as follows:

$$T(x,t)=f(x,t;F,L), \tag{6}$$

where F – input physical parameters of the system, L – output physical parameters of the system.

Both classes of parameters are described in detail in Table 1.

The detailed view of the parametric model for controlling the physical component of the active protection system is presented as follows:

$$T(x,t)=f(x,t;f_1,f_2,f_3,f_4,l_1,l_2,l_3,l_4,l_5,l_6). \tag{7}$$

The presented parametric model describes the dependencies of physical input and physical output parameters.

As shown in Figure 4, physical input parameters affect input analytical and input predictive parameters. All three categories of parameters are involved in the system's management decision-making process. When making a management decision, physical input parameters are taken into account and, in addition to positioning the active protection elements in space, the duration and frequency of switching on additional heat sources are determined. The physical output parameters affected by intelligent protection, which is a physical interpretation of active protection, are shown in Figure 5.

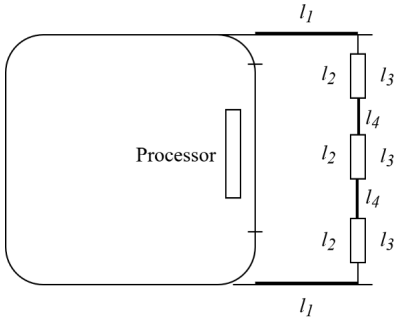


Figure 5: Graphical representation of the adaptive physical output parameters of the protection model.

An essential component of the system is the analytical component, which includes both incident detection and the automatic decision-making procedure.

3.2. Model of intelligent measurement of input physical parameters

The analytical component accepts two streams of input parameters: initial and post-processing parameters. Initial parameters include input physical parameters, the intelligent measurement of which affects the duration and frequency of the protection system activation. At the same time, the thermal channel is analyzed for the presence of information transfer. The results of this analysis can be considered post-processing parameters.

Intelligent measurement involves interpreting the results of measuring input physical parameters. The process of intelligent measurement is based on a procedure for determining the weighting coefficients of the influence of input physical parameters on the output physical parameters of the protection system. In accordance with the provisions set forth in [11], the determination of the influence of indicators on output parameters is carried out using multivariate regression. In this case, it is necessary to calculate the weight coefficients of the input parameters for each output parameter using a multiplicative model:

$$E^{l_i}=B_0 f_1^{b_1}\cdot f_2^{b_2}\cdot f_3^{b_3}\cdot l_4^{b_4}, \tag{8}$$

where B_0 is the constant coefficient of the regression equation, b_1 is weight coefficient.

Logarithmic transformation is used to convert the multiplicative model into a linear model. The formula for the linear model takes the form:

$$y^{l_j}=\omega_0+\sum_{i=1}^{n}\omega_i f_i^{l_j}+\varepsilon_j, \tag{9}$$

where ω_i is weight coefficient.

The least squares method is used to determine the coefficients. The formula for determining the coefficients takes the form:

$$\omega=\left(F^T F\right)^{-1}F^T y. \tag{10}$$

In intelligent measurement tasks, the dependence formed by regression analysis is converted into a neuron, which is described by the formula:

$$A=\sigma\left(\sum_{k=1}^{k}\omega_k f_k+\varepsilon\right). \tag{11}$$

It is also important to take into account the results of post-processing. One of the NIST tests is used to analyze bits. The system selects the necessary test based on the frequency of bit transmission through the thermal channel. Statistical properties are studied based on one of the approaches described in [12]. Entropy analysis is performed, statistical dependencies and bit pair correlations are studied. When the statistical coefficient is denoted as S, then the formula describing the analytical neuron takes the form:

$$\widehat{A}=\sigma\left(\sum_{k=1}^{k}\omega_k f_k+\omega_{k+1}f'_{k+1}+\varepsilon\right), \tag{12}$$

where f'_{k+1} is an additional input parameter obtained as a result of post-processing, ω_{k+1} is the weight coefficient of the additional input parameter.

Work [13] describes a model that takes into account sets of initial processes with sets of goal scenarios in the process of managing complex organizational and technological objects in the context of cyber threats. This model can be adapted for the current task of managing an adaptive active protection system, taking into account the intelligent measurement of input physical parameters. The model of intelligent measurement of input physical parameters is described as follows:

$$R=\left\langle F, L, A, \widehat{A}\right\rangle. \tag{13}$$

This model allows to describe the analytical component of the protection system. In order to describe the process of management decision-making, it is necessary to take into account input

physical as well as input analytical and prognostic parameters. As can be seen from Figure 3, the input analytical and prognostic parameters are indirectly influenced by the input physical parameters. This situation requires the formation of a formalized procedure for management decision-making.

3.3. Management decision-making procedure

A management decision is made on the basis of intellectual processing of physical prognostic and analytical input parameters, taking into account the hierarchical influence of physical parameters on analytical and prognostic ones. The hierarchical structure is represented as follows:

$$\begin{cases} \widehat{k_c} = \sum_{n=1}^{i} \alpha_{ci} f_i + \omega_c + 1 f_c^{'} + 1 + \varepsilon_c^{(k)} \\ p_m = \sum_{n=1}^{i} \beta_{mi} f_i + \varepsilon_m^{(p)} \\ y = \gamma_0 + \sum_{n=1}^{i} \gamma_i f_i + \sum_{c=1}^{j} \theta_c k_c + \sum_{m=1}^{l} \vartheta_m p_m + \varepsilon \end{cases}, \quad (14)$$

where α_{ci}, β_{mi} are the coefficients of influence of physical parameters on analytical and prognostic parameters, respectively, γ_0 is the coefficient of direct influence of physical inputs on physical output parameters, ϑ_m, θ_c are the coefficients of indirect influence of input analytical and prognostic parameters on physical output parameters.

Taking into account the indirect influence, the equation for the linear model y takes the form:

$$y = \gamma_0 + \sum_{n=1}^{i} \gamma_i f_i + \sum_{c=1}^{j} \Theta_c \left(\sum_{n=1}^{i} \alpha_{ci} f_i + \omega_{(c+1)} f_{(c+1)}^{'} + \varepsilon_c^{(k)} \right) + \sum_{m=1}^{l} \vartheta_m \sum_{n=1}^{i} \beta_{mi} f_i + \varepsilon_m^{(p)} + \varepsilon. \quad (15)$$

This takes into account both the direct influence on output parameters as well as indirect influence of physical input parameters on analytical and predictive inputs, which ultimately causes a change in physical output parameters.

Management decisions are based on the approach described in [11]. Management decision situations take into account the level of influence q of the input parameter on the output physical parameter. The set of influence parameters is divided into three categories: the influence of physical parameters on analytical and prognostic input parameters; the direct influence of physical inputs on physical output parameters; the indirect influence of input analytical and prognostic parameters on physical output parameters. The following formula is used to make a management decision and reflect situation S:

$$S = \bigcup_{r=1}^{c} S_{\alpha}^{q} \cup \bigcup_{l=1}^{m} S_{\beta}^{q} \cup \bigcup_{z=1}^{i} S_{\gamma}^{q} \cup \bigcup_{v=1}^{c} S_{\theta}^{q} \cup \bigcup_{b=1}^{m} S_{\vartheta}^{q}. \quad (16)$$

The formed analytical component is related to the predictive component of the protection model. The task is to form a predictive model.

3.4. Forecasting model in the application of active protection

According to [14], it is proposed to use the ARIMAX model to form a forecast, taking into account the regression analysis and lags of the predicted parameters. This model, unlike other forecasting models, allows considering external (exogenous) variables, that is important for taking into account the influence of additional factors, while maintaining acceptable computational requirements. For each predicted variant, the following formula is used:

$$y_t = c + \sum_{k=1}^{p} \phi_k y_{t-k} + \sum_{q=1}^{Q} \theta_q \varepsilon_{t-q} + \sum_{n=1}^{i} \beta_n f_{n,t} + \varepsilon_t, \quad (17)$$

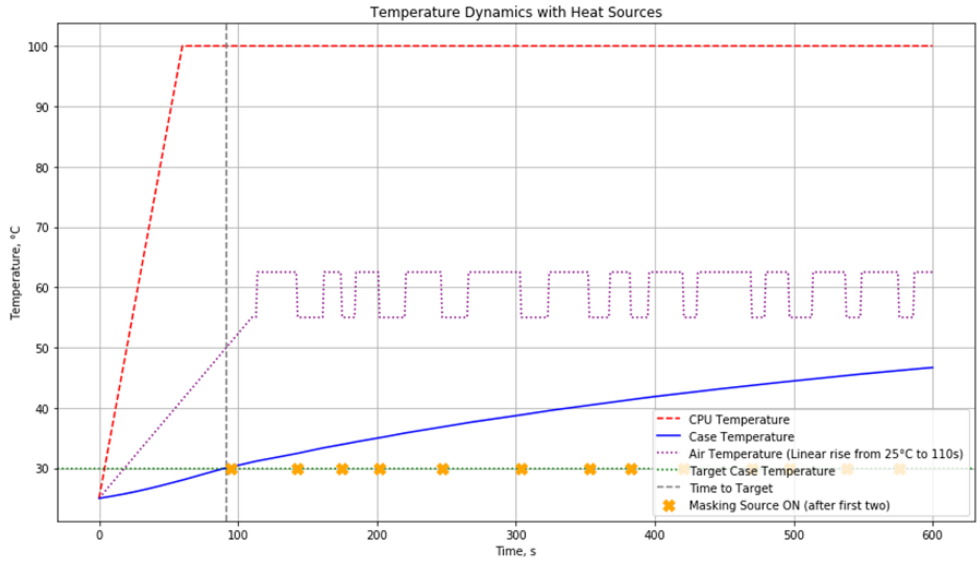
where y_t is the predicted indicator at time t, c is a constant, ε_t is a random error, ϕ_k is the autoregression coefficient, y_{t-k} – previous values of the forecast series, θ_q are moving average coefficients, ε_{t-q} – previous forecast residuals, β_n is an impact coefficient, $f_{n,t}$ is a value of the exogenous factor at time t.

This formula describes the forecasting model.

3.5. The results' evaluation and discussion

To evaluate the effectiveness of the intelligent protection proposed in this work, a software tool was developed for modelling and analyzing the temperature dynamics of the thermal data transmission channel. Using the model, the influence of changes in the initial parameters of the adaptive active protection system on the possibility of data transmission through the thermal channel was investigated. The simulation results are shown in Figure 6.

Figure 6:



Temperature change dynamics during the operation of the active protection system.

The following conditions were specified for the simulation: CPU temperature – 100 degrees Celsius after 60 seconds of its usage, case temperature from 25 to 47 over a period of 600 seconds. When the minimum panel heating temperature of 30 degrees was reached, the protection system was activated at time intervals determined by the control system based on the input data. The simulation considered the use of an embedded information processing device Siemens SIMATIC S7-1200 and an aluminum case panel with thickness of 2 mm. The selection of hardware and materials is not limited to those presented but is intended to demonstrate the behavioral patterns of the system.

To evaluate the effectiveness, metrics similar to those defined in a similar work [4] were used, namely bit error rate (BER) and energy efficiency. Characteristics typical of the proposed development were added, which qualitatively distinguish it from analogues – equipment safety and protection adaptability.

As a result of modelling, it was established that BER is 97%, which is 3% higher than the analogue, and energy efficiency is 23.47 W, which is lower than the analogue. For an objective and comprehensive assessment of efficiency, the method described in [9] was used. Four criteria were used: BER (Br), energy efficiency (Ef), equipment safety (Es), and adaptability (Ad). Integral efficiency is determined by the formula:

$$E = \frac{Br + Ef + Es + Ad}{4}. . \quad (18)$$

The summary linguistic assessment is presented in Table 2.

Table 2
Comparative table of the proposed and analogue defense model assessment

Criterion	Proposed defense		Analogue defense	
	Linguistic assessment	**Numerical equivalent**	**Linguistic assessment**	**Numerical equivalent**
Br	Very High	1.00	High	0.75
Ef	Medium	0.50	High	0.75
Es	High	0.75	High	0.75
Ad	High	0.75	Low	0.25

The efficiency of the development was denoted as Er, and the efficiency of the analogue as Ea. According to the calculations of integral efficiency, Er = 0,75, and Ea = 0,625. The analysis proved an increase in efficiency by 0,125, or 20%.

4. Conclusions

The paper developed a hierarchical modular model of intelligent protection for temperature-based transmitting channels in laboratory sensor networks with embedded information processing based on intelligent management decision-making by a cyber-physical protection system through parametric linking of input data and physical changes in active protection, which made it possible to ensure the reliability of protection while maintaining the safety of equipment operation thanks to the formed adaptive active protection system. Software was developed that allowed the presented models to be verified. The effectiveness of the protection system has been increased by 20% compared to the existing similar approach. The following scientific results were obtained in the work:

1. A parametric model for controlling the physical component of the active protection system of IoT-oriented laboratory equipment, combined into a sensor network, was developed based on the determination of non-stationary thermal conductivity by studying the thermal equilibrium at the point on the shielding/jamming layer, which made it possible to form the dependence of the input and output physical parameters.
2. A model for the intelligent measurement of input physical parameters was developed based on regression analysis by determining weight coefficients using the least squares method, which made it possible to describe the analytical component of the protection model, taking into account the statistical analysis of bits passing through the thermal communication channel.
3. A procedure for making management decisions based on situational management was developed by intelligently processing physical prognostic and analytical input parameters, taking into account the hierarchical influence of physical parameters on analytical and prognostic ones, which made it possible for the active protection system to respond adaptively to changes in physical input parameters.
4. A forecasting model for the application of active protection based on the ARIMAX model has been developed by taking into account the regression analysis performed, which made it possible to form probable event scenarios based on the input physical parameters and previous results.

The practical significance lies in the possibility of implementing intelligent active protection for IoT-oriented equipment in research laboratories, combined into a sensor network and equipped with built-in information processing capabilities during laboratory testing.

The prospect for further research is to expand the protected channels of information leakage and to search for optimal ways to integrate the protection of thermal channels of information leakage into a multi-channel intelligent protection system.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Y. Nam, H.-D. Park, Revolutionizing laboratory practices: pioneering trends in total laboratory automation, Annals of Laboratory Medicine (2025). https://doi.org/10.3343/alm.2024.0581

[2] I. Miketic, K. Dhananjay, E. Salman, Covert channel communication as an emerging security threat in 2.5D/3D integrated systems, Sensors 23 (2023) 2081. https://doi.org/10.3390/s23042081

[3] A. Z. Benelhaouare, I. Mellal, M. Oumlaz, A. Lakhssassi, Mitigating thermal side-channel vulnerabilities in FPGA-based SiP systems using thermal digital twin technology, Electronics 13 (2024) 4176. https://doi.org/10.3390/electronics13214176

[4] P. Rahimi, A. K. Singh, X. Wang, Selective noise-based countermeasure against thermal covert channel attacks in multi-core systems, Journal of Low Power Electronics and Applications 12 (2022) 25. https://doi.org/10.3390/jlpea12020025

[5] J. Gonzalez-Gomez, M. B. Sikal, H. Khdr, L. Bauer, J. Henkel, Balancing security and efficiency: mitigation of power-based covert channels, IEEE Trans. CAD Integrated Circuits Syst. 43 (2024) 3395–3406. https://doi.org/10.1109/tcad.2024.3438999

[6] J. Wang, X. Wang, Y. Jiang, A. K. Singh, L. Huang, M. Yang, Mitigation of enhanced thermal covert channel in many-core systems, IEEE Trans. CAD Integrated Circuits Syst. 39 (2020) 3276–3287. https://doi.org/10.1109/tcad.2020.3012642

[7] I. Rozlomii, A. Yarmilko, S. Naumenko, Vulnerability modeling in cybersecurity of intelligent infrastructure networks, in: Lecture Notes in Networks and Systems, Springer, 2025, 234–348. DOI:10.1007/978-3-031-90735-7_19

[8] K. T. Chui, B. B. Gupta, J. Liu, V. Arya, N. Nedjah, A. Almomani, P. Chaurasia, Survey of IoT and cyber-physical systems: standards, security, challenges, Information 14 (2023) 388. https://doi.org/10.3390/info14070388

[9] A. Korchenko, V. Breslavskyi, S. Yevseiev, N. Zhumangalieva, A. Zvarych, S. Kazmirchuk, Linguistic standards construction for honeypot efficiency assessment, Eastern-European Journal of Enterprise Technologies 1 (2021) 14–23. DOI: 10.15587/1729-4061.2021.225346

[10] L. Berkman, O. Turovsky, L. Kyrpach, O. Varfolomeeva, V. Dmytrenko, O. Pokotylo, Code structure analysis for multidimensional signal transmission channels, Eastern-European Journal of Enterprise Technologies 5 (2021) 70–81. DOI: 10.15587/1729-4061.2021.242357

[11] T. Prokopenko, Y. Lanskykh, V. Prokopenko, O. Pidkuiko, Y. Tarasenko, Ontological SCRUM-based project situation management under risk, Eastern-European Journal of Enterprise Technologies 6 (2023) 47–54. https://doi.org/10.15587/1729-4061.2023.292526

[12] C. Foreman, R. Yeung, F. J. Curchod, Statistical testing and randomness extraction for RNG improvement, Entropy 26 (2024) 1053. https://doi.org/10.3390/e26121053

[13] T. Prokopenko, Y. Tarasenko, O. Lavdanska, S. Rudnytskyi, Y. Rudnytska, Technology for alternative management of organizational objects under cyber threats, CEUR Workshop Proceedings 3187 (2021) 170–181. https://doi.org/10.5281/zenodo.11119888

[14] H. A. Selmy, H. K. Mohamed, W. Medhat, Predictive analytics framework for sensor data with deep learning, Neural Computing and Applications (2024). DOI: 10.1007/s00521-023-09398-9