INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 4, PP. 1-8
Manuscript received March 31, 2026; revised October 2026. doi: 10.24425/ijet.2026.6317

The cyberprotection method for microcontrollers with optical interface and their based devices

Vadym Malinovskyi, Leonid Kupershtein, and Leonid Maidanevych

***Abstract*—This article aims to review the current state of cybersecurity in a field of microcontrollers with optical interfaces and approaches to the method of their cyber protection, based on a complex differentiated security variable perimeter, which includes various variable protection function components. The impact of the components of cyber-attacks and information interventions on optical interfaces in specialized microcontrollers was separately analyzed and specified. Also were illustrated some experimental studies of the cyber protection method of MC's with optical interfaces. A comprehensive model of cyber protection of microcontrollers has been developed, taking into account various factors of protection against cyber threats and information influences in microcontrollers, which can be applied to both electronic microcontrollers and specialized microcontrollers with optical interfaces.**

***Keywords*—cyber defense; cyber threat; information influence; microcontroller (MC); microcontroller unit (MCU); optical interface; cyber security; Internet of Things (IoT); information system**

I. Introduction

THE modern information systems technologies based on microcontrollers have been widely presented in various devices, networks and Internet of Things (IoT) systems and devices in various fields. As noted in works [1], the main cyber security problems in MC's systems are a very strong and flexibleless architecture; the complexity and rigidity of hardware and software functions; definitive structures of microprocessors; vulnerabilities of MCU's (such as Spectre, Meltdown, Row Hammer/Rowmaster [1]); optical ports and sensors (for optical MCU's) [2] and complexity risks of intrusions in a MCU's schemes [1, 3]. Also the Zero-Day threat component of information influences cyber security risk was always presented for most microcontroller units(MCUs). This is caused by the complexity and difficulty of controlling internal information communications in the MC due to the orderliness and impossibility of full control of information communications in the MC. In various systems there are a some kinds of specialized microcontrollers with optical and optoelectronic interfaces for data communications. This types of specialized MCs may include an internal optical port or they may densely coupled with optical external sensors or optical devices (such as optical IR ports, laser/Led emitters, photo elements. There is also available wide kind of optical digital biosensor devices and digital optical sensors with internal MC[2-4]. For example, in industry are exist such special MC's as: Max DS4830, DS4830A, AD MAXM86146, MCU; fiber-optical modules MC's such as HT32F52234/HT32F52244: and special MCU based on ARM M0 Cortex 32 bit core, which has a connection with optical interfaces. It's used in various circuits and systems due to the advantages of optical radiation for information tasks: electromagnetic neutrality, contactless and invasiveness, high speed, low latency and energy index, etc. On the market there is present an specially type of MC – with an optical interface and optoelectronic sensors with a digital MC part with an open optical channel. For example, IR position sensors and MCs with IR interfaces and sensors, witch that operate in the electromagnetic wave range of 0.4-10.5μm may be compromised by the outside optical links scheme [3-4]. Those cyber threats and information interference that occur in traditional electronic MC's may not fully or partially presented themselves in MCs with an optical interface.

The specifics of cyber security in using of this MCUs witch have an optical port or interfaces are slightly different from this problem in traditional MC's based on purely electronic circuits due to optical link in interface, which may be used as an additional channel for outbound third-party connections and informational influences. The presence of an optical and/or optoelectronic part in the MC makes it specific for certain groups of interventions, in particular [3, 4]:

- contactless remote optical access, information influences, optical fault injections in optical and non optical sides [2-4];
- interventions in optical port by optical radiation in MITM (Man in The Middle) model type of attacks;
- suppression of interference and/or induction of optical signals by third-party sources by optical side[3, 4];
- interception of optical and other signals and unauthorized access in MC by optical side(including fiber-optic) [2].

Therefore, to ensure effective and efficient protection in practice, MC's with an optical interface should include and consider individual components of protection against cyber-attacks, taking into account protection over the optical interface. Classically, the problem of cyber security of the information part of the microcomputer, it's micro programs and the main functional software processes is a complex and not yet resolved problem, which will require a comprehensive assessment and review, until now it becomes even less relevant.

Vadym Malinovskyi, Leonid Kupershtein, and Leonid Maidanevych are with Vinnytsia National Technical University, Ukraine (e-mail: vad.malinovsky@gmail.com; kupershtein.lm@gmail.com, orcid 0000-0001-6737-7134; lmaidanevych@gmail.com, orcid: 0000-0002-7364-8874).

© The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/), which permits use, distribution, and reproduction in any medium, provided that the Article is properly cited.

The *goal* of the research is to improve the cyber protection level of MC's with an optical interface and based on their circuits by using a new solution and approaches in cyber protection method, based on a differential variable security perimeter.

II. APPROACHES TO DEVELOPMENT CYBER PROTECTION PRACTICES FOR MCU WITH OPTICAL INTERFACES

The assessments of cyber threats and impacts through the main and side channels in the MC considered in the works [1-2], made it possible to understand the main principles of cyber threats in MCU's and levels of developing a protection model for information processes. Cyber protection of MCUs and their based devices in the modern information environment, taking into account the complex landscape of modern cyber threats, usually is practically impossible, without the new hardware and firmware release of a new product with accrued, optimized and closed vulnerabilities (CWE, MITRE). The second part of the cyber threats consists in software firmware vulnerabilities [1]. They are fixes more easily. Therefore, most of the classical security methods for classical information systems and functional devices with OS can't be applied to microcontrollers and MC's devices directly. Known practices of microcontroller cyber protection are based on the use of such principles [1, 3]:

- isolation, filling and housing in individual MCs and their systems in complex and physical mechanical housing (including, of mirror-based covers) [5];
- separation of circuits from MCs with other information parts and use of separate software techniques [5, 6];
- quick restarting (rebooting) MCs by outbound interrupts, using flexible recovery functional with blocking malicious influence;
- use of simplified security protection micro systems and security micro function by firmware algorithm;
- use MC's integration in more high level information security systems, with monitoring and protection;
- use of flexible, redundancy and fault-tolerant algorithms and software practices in MC's firmware[7];
- use of innovation methods, based on the prediction, analysis and identification of cyber threats in MCs;
- use of innovation methods, based on multilayers defense concepts, similar and such as "Defence in Dept" in InfoSec(CyberSec) Concept [8-12] in traditional computer data systems and IoT devices, also in data computing systems based on software operation systems (OS) with some clarifications and features for the MCU's.

The problem in most of either of these methods is requiring other additional approaches. In most cases, its using are not rational and often a more expensive technique for implements to MCUs. The level of cost/technical functional criteria in MC's security system the most important factor. As described in [1], the progressive practices and principles of MC's security are:

– analysis of the processes of the MC functioning and neutralization of cyber threats and harmful effects;

– use of comprehensive approaches to MC's information protection and MC's isolation techniques;

– approaches, based on monitoring and compensative parameters in MC's reliable algorithms.

For the development of effective MCU's cyber protection method, it is necessary to take into account the specifics of the construction of its MCs, the diversity of architectures, and the diversity and anisotropy of hardware and software modules into MCU architectures. For MCs protection it is also necessary take into account the specifics of the construction of MCs with optical and other their blocks for monitoring and controlling the data processes in MC's. If observe the implementation a cyber-threat in MC with optical interface, information losses may be describes as:

$$H(IO_{out}|MCU_{out} = \sum_{i=1}^{n}\sum_{j=1}^{m}[P(IO_{int})_i \times \times Pi(MCU_{CSEC})] + H(IO_{int}|MCU_{int}) \quad (1)$$

where $H(IOout|MCUout)$– total summary entropy or data loss during transmission from the external input interface of the MC (or other MC area) with the transmission probability; $P(MCU_{intt}|IO_{in})$ – probability of reverse transmission (transmission in the opposite direction); $P_i(MCU_{CSEC}$ – probability of a cyber threat in one of the channels);– $H(IO_{int}|MCU_{int})$ – summary input data entropy. The mechanism of implementation of cyber threats by factors in MC is described by the authors in [1]. Most of $P_i(MCU_{CSEC})$ – probabilities are defined as a normal low of distribution (what is typical for MCU electronic and optoelectronic systems MCUs), as is: $P_i(MCU_{CSEC\ i})$ $Pi(MCU_{CSEC\,i}) = \frac{1}{\Delta\sqrt{2\,MCU_{CSEC\,i}}} \cdot e^{-i\frac{(MCU_{CSEC\,i}-r)^2}{2\Delta^2}}$ $[11-13]$, and in some real cases , such as MCU memory, where $MCU_{CSEC\ I}$ – is argument of security function of MCU , which characters of security level(security point). Also was present a research [18], where probabilities are defined as Weibull low of distribution function, $Pi(MCU_{CSEC\,i}) = \frac{1k}{\Delta} \cdot (\frac{MCU_{CSEC\,i}}{\Delta})^{k-1} \cdot e^{-i(\frac{MCU_{CSEC\,i}}{\Delta})^k}$ what also is typical for some MCU systems.

Data losses in (1) characterize the potential amount of data, which are lost in the MC as a result of some type of cyber-attack or harmful information influence if they are the cases. The parameters of data losses (1) in the MC can be used to estimate the amount of information data damage factor when a cyber threat is successfully implemented. For example, this could be when implementing an second side attack, such as power side attack [1].

III. CYBER PROTECTION METHOD DEVELOPMENT FOR MCU WITH OPTICAL PORTS

For cyber protection of MC's, the protection method should apply the following principles: indication and definition of a cyber threat by inside logical data sensor(s); interactive blocking of traffic and the data source of a cyber threat; the principle of isolation and use of a protective imagine variable perimeter of the MC data environment; principles of restoring previous MC's states of data values with normal parameters; the principle of determining and organizing the fixation of parameters before a cyber threat happens; principles of injection flexibility in micro firmware and in other MC's architecture blocks; the principle of obfuscation of individual indicators and information parameters of the system (for example, MCU/MK ID, MC interface addresses, protocol addresses, etc.); the principle of adaptability of the protection level; the principle of implementation and inclusion in the work of different in their essence and organization scheme of unprotected MC architectures and a scheme based on MC; the principle of flexibility and fault

tolerance to MC functionality; principles of rapid restoring previous states of the firmware and MC resources, etc. The protection method must provide adaptability to a wide number of MC architectures and be a flexible. The MC's cyber protection method development uses as the main principle - blocking of information influence with filtering and blocking harmful source data traffic in the microcontroller's interfaces. It is allows reducing the main amount of data losses (1) and should be based on a outbound isolation technique. If simplify the model, it can be shown on Fig. 1, Fig.2.

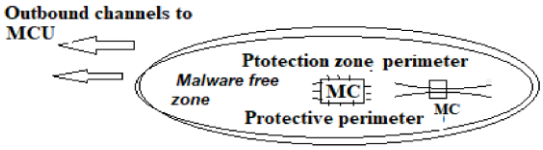
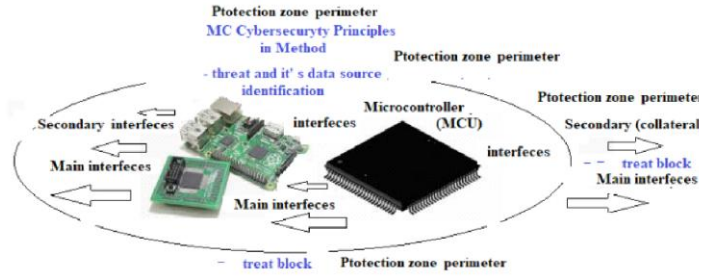
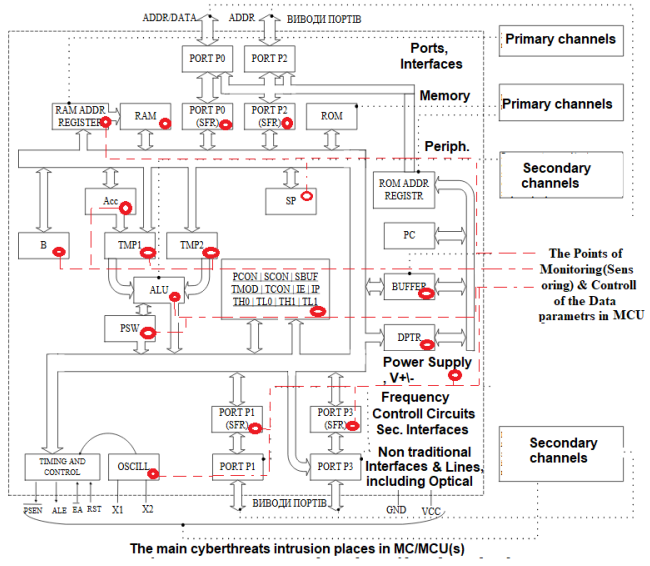


Fig. 1. Illustration of basics by the cyber protection perimeter creation in MCU systems



a)



b)

Fig. 2. Illustration of the general principle of the cyber protection method in MCU with creation and usage imaginary protective variable perimeter, which cover MC on main and side interfaces: a) general view; b) view in MC structure with data, where information parameters can be changed

The method is based on the creation of a differentiated imaginary protective perimeter, which covers MC's not only in the outbound side, but also in the inside of some MC's architecture blocks. The boundary may elapse in the middle of MC or scheme, based on them. The method includes a lot of cyber defense approaches to creating perimeter and several layers of protection in the MC.

The ensuring of proposed concept is realizing within of the Defence in Depth in InfoSec Concept [8-10], which is typical in traditional information systems. This is shown in Fig.3, precisely from the point of view of ensuring security in microcontrollers, the implementation of a differential variable imagine conditional variable security perimeter in the structure of the MC. It is implemented at several levels simultaneously: Data Security, Physical Security Layer; Perimeter Security Layer and Host Security.

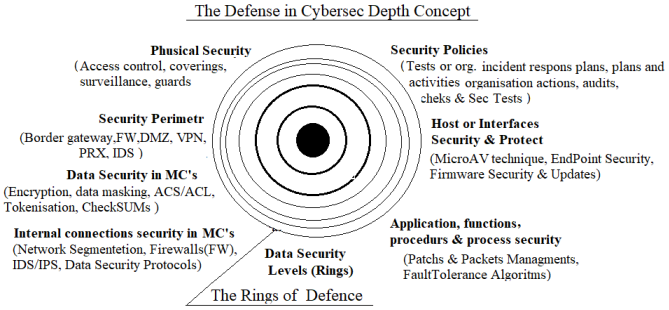


Fig. 3. Illustration of the general known Defence in Dept CyberSec Concept in MCU Data systems [8-11]

It should be noted that the creation of a conditional security perimeter is a concept that does not involve the creation of a specific isolation layer of security (unlike network shielding or local shielding of connections via interfaces and ports), but rather a set of technologies for protecting against influence and/or creating countermeasures and connections at once on several layers in microcontroller systems and microcontrollers (MC).

Several layers of protection are already known in works [8-10] as data security layers in Defence in Dept CyberSec Concept, and have proven them quite well with high efficiency.

Moreover, within the framework of the method, a variable (i.e., variable f(rx)) conditional security perimeter is created at several levels at once, which:

- changes dynamically within the framework of the spread of the cyber threat in time according to $f(t)\ \Delta t_i$;
- which creates a variable security zone of direct counteraction to the influence of the cyber threat at a specific level of contact of the IS systems of the MC with it, and localized, depending on its nature, type and dynamics;

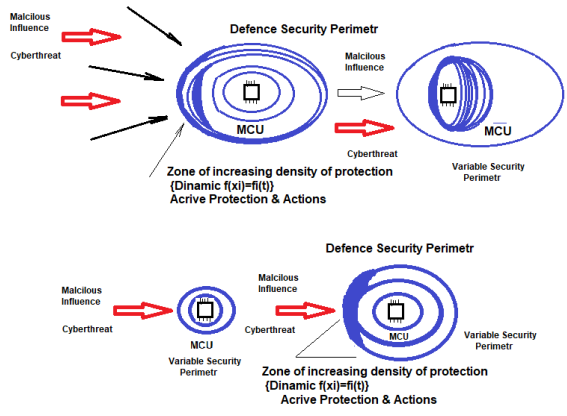


Fig. 4. The principle of variable security zone in variable perimeter creation around and inside of and in MCU with dynamic density (which changes) of active protection

- this zone is dynamic and the conditional density of its interaction changes, increases (the conditional density of counteraction and the "density" of counteraction to the cyber threat) with an increase to the surface of zone directly to cyber threat direction (as it shown in Fig.4);

- decreases, witch a decrease of the cyber threat influence

The active protection function can be described as:

$$f(p,t) = P_{por} + k \cdot A \cdot f_i(p_i, t_i). \qquad (2)$$

The active protection function, *f(p, t)* perform protection with increasing of action density, when is increasing of cyber threat intensity in the information system of MCU's in a specific direction k (vektor), depending on the intensity and probability of the cyber threat.

The active protection function $f_i(p_i, t_i)$ is dynamic and it increases with increasing intensity of cyber threat influence in information MCU system. This function is growing, taking into account the specific direction (vector parametr), which depending of intensity of probability of the cyber threat opposite to this direction.

Also, in practice, this is implemented by using a group of consolidated and managed specific cyber defense techniques(applied methods) that parallel operate at different levels of Defence in Depth Concept [8-11] in the MCU architecture(such it shown at Fig.5) with some specifics:

- micro AV protection (micro software system modules or micro AV functions in firmware) and blocking of processes and functions in the MC memory (Fig.5) by specific MC software functions and algorithm branches;

- MC recovery latest states of micro links and functions by restoring the previous data states and parameters from memory;

- MC Fault-Tolerant Algorithms (FTA) in MCU firmware;

- connection isolation and tunneling in MC interface approaches and data transfer processes in MC interfaces and ports;

- external protection, blocking and isolation mechanisms (at the external level of the MC system) via various channels (including) via side and power channels;

- Physically isolates and isolates the MC crystal from influences and attacks of the injection and optical fault injection type of attack, for example, a physical screen. with a layer of electrically conductive and ferromagnetic materials and optically reflective materials (similarly studied in [5-7, 20]). Also, for effective shielding, it is possible to use promising new materials with new shielding properties that will provide protection against physical and other types of interference in the MC system and will be able to counteract physical and other influences on the microprocessor system.

- Introduction of other mechanisms for interactive MC shielding - for example, effective changes and introduction of artificial failures into the information processes of the cyber threats themselves: for example, effective and rapid changes in the main information parameters of cyber threats (for example, individual possible malicious process), which will lead to the failure of the malicious process.

The method itself is conditional and theoretical, but has practical functionality when using complex management of practical security technologies in MC.

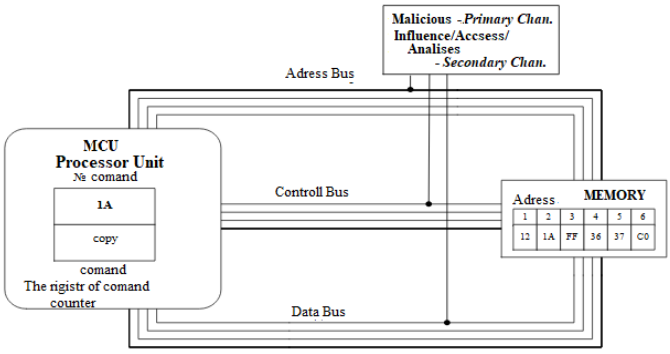


Fig. 5. Illustration of main intrusion zones or potencial points of influences in MCUs

But the difference between this method and cyber defense approaches is the creation of a single variable perimeter with a differential protection function:

$$F_{sec}(x_i, y_i n_i t_i) = f_{sec}(x_i, y_i n_i t_i)_{MICRO\ IDS} U$$
$$U\ f_{sec}(x_i, y_i n_i t_i)_{MICRO\ FIREWALL}\ U\ f_{sec}(x_i, y_i n_i t_i)_{CRYPRO\ SEC} U$$
$$U f_{sec}(x_i, y_i n_i t_i)_{MICRO\ TUNEL} U f_{sec}(x_i, y_i n_i t_i)_{MON} U$$
$$U\ f_{sec}(x_i, y_i n_i t_i)_{ZONE\ PERM}\ U\ f_{sec}(x_i, y_i n_i t_i)_{OPTICAL}$$
$$U f_{sec}(x_i, y_i n_i t_i)_{MON} U\ f_{sec}(x_i, y_i n_i t_i)_{ZONE\ PERM}\ ;$$

$$F_{sec}(x_i, y_i n_i t_i) = \bigcup_{J=1}^{N} \{f_{sec}(x_i, y_i n_i t_i)_J\};$$
$$f_{sec}(x_i, y_i n_i t_i)_J \in M\{x_i \dots x_n,\ y_i, \dots y_n,\ n_i \dots n_n,$$
$$t_i \dots t_n\};\ x_i \in X_i\ ; y_i \in Y_i;\ n_i \in N_i\ ;\ t_i \in T_i\ , \qquad (3)$$

where $Fsec(x_i, y_i, t_i)$ - differential and variable safety function of the protective zone (perimeter) MCU); $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ IDS}$ and $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ FIREWALL}$ - safety function components responsible for the micro-protection system in the MC at the level of the MC firmware or architecture, and the micro-shielding component on the interfaces and input/output (I/O) ports; $f_{sec}(x_i, y_i, n_i\ t_i)_{CRYPRO\ SEC}$ and $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ TUNNEL}$ - components of the security function responsible for cryptographic protection of information in the MC and protection at the level of creating micro tunneling (with obfuscation of interface addresses) over MC interfaces (as a promising technology for protecting inter-component communications in long lines); $f_{sec}(x_i, y_i, n_i\ t_i)_{MON}$ - a component of the safety function responsible for monitoring events, values x_i, y_i and processes at the MC firmware level (can be implemented in a micro-version and/or external protection and with external connection) from monitoring indicators; $f_{sec}(x_i, y_i, n_i\ t_i)_{ZONE\ PERM}$ - a component of the security function that corresponds to the restriction and delimitation of access rights the different levels of the MC's firmware; $f_{sec}(x_i, y_i, n_i\ t_i)_{OPTICAL}$ - a component of a complex protection function based on the optical and/or optoelectronic part of the MC, for example, based on an optical interface or optical sensor integrated into the MC; $f_{sec}(x_i, y_i, t_i)_i$ - an unitary function protection component of the protection function; operator "*U*" - signs of logical disjunctions operations

(logical "And") that can be applied and are responsible for the logical inclusion/exclusion of variable components of the cyber protection function. Component $f_{sec}(x_i, y_i, n_i, t_i)_i$ means separate functional safety defense function that work with many arguments safety parameters: x_i, y_i, n_i, and which are modified in the time parameter t_i, i.e. are dynamic, corresponding to the safety parameter. Cyber security model (3) may be describes as a model, which shown in Tabl. I. Protection of MC with optical interface is formed by the cyber security MC's function $F_{sec}(x_i, y_i, n_i, t_i)$ by each their component.

Each specific component in Tabl. I of the complex cyber defense function $fsec(x_i, y_i, t_i)i$ is described by a probabilistic nature and constitutes a complete version of protection against cyber threats. Components of cyber defense, network traffic shielding in MC $f_{sec}(x_i, y_i, n_i, t_i)_{MICRO\ IDS}$; $f_{sec}(x_i, y_i, n_i, t_i)_{MICRO\ FIREWALL}$ and crypto security $f_{sec}(x_i, y_i, n_i, t_i)_{CRYPRO\ SEC}$ and $f_{sec}(x_i, y_i, n_i, t_i)_{MICRO\ TUNNEL}$ characterises and can describe security in any type of MCs: electronic or opto-electronic. This involves monitoring of information indicators and cyber protection in MC. Component $f_{sec}(x_i, y_i, n_i, t_i)_{OPTICAL}$ characteristic only for optical and/or optoelectronic MCs, which include an optical interface. It is shown in fig.5.

The protection function component is responsible for protecting information in MCs with optical interfaces. $f_{sec}(x_i, y_i, n_i, t_i)_{OPTICAL}$. This component of the complex protection function for the optical and/or optoelectronic part of the MC in the optical interface (or digital optical sensor, DOS), which is integrated into the MC - is usually organized on the hardware part Hardware L1 - the first level of the well-known OSI model at the level of physical optical protection methods and technologies.

The components of cybersecurity model (3) are different and form a protection actions, describes and shown in Tabl. I.

Components of cyber defense, network traffic shielding in MC $f_{sec}(x_i, y_i, n_i, t_i)_{MICRO\ IDS}$; $f_{sec}(x_i, y_i, n_i, t_i)_{MICRO\ FIREWALL}$ and crypto security $f_{sec}(x_i, y_i, n_i, t_i)_{CRYPRO\ SEC}$ and $f_{sec}(x_i, y_i, n_i, t_i)_{MICRO\ TUNNEL}$ characterises and can describe security in any type of MCs: electronic or opto-electronic. This involves monitoring of information indicators [1] and cyber protection in MC. Component $f_{sec}(x_i, y_i, n_i, t_i)_{OPTICAL}$ characteristic only for optical and/or optoelectronic MCs, which include an optical interface. It is shown in Fig.6.

In mathematical approximation, under the conditions of simplification, the arguments of functions, such x_i, y_i, n_i, t_i and the function $f_{sec}(x_i, y_i, n_i, t_i)_i$ itself, may be simplify to function with one argument x_i, . Under the conditions of simplification of the problem in static representation ($dt_i \to 0$):

$$f_{sec}(x_i, y_i, n_i, t_i)_i \to f_{sec}(x_i)_i \qquad (4)$$

Each separate component $f_{sec}(x_i)_i$ may be describes as a function of average exponential quadratic sequences: $f_{\sec i}(x_i) = b_i + a_i k \frac{x_i^2 - \Delta x + e^x}{\sqrt{x_i}}$. It's function may be simplified to $f_{\sec i}(x_i) = b_i + a_i k x_i^2$ or $f_{\sec i}(x_i) = b_i + a_i k e^{xi}$ in real cases in practice .

Such representation could permit a analyses MCU more simply to understating of nature and contribution of security function components.

The progressive practices to neutralize and timely prevent cyber threats are used :

- analysis of the data processes of the MC functioning;
- active data access and real time changes methods in information processes in MC memory;
- neutralization and blocking of cyber threats and harmful effects and influences ;
- use of comprehensive, complex and flexible approaches to information protection in the MC system;
- isolation of the MC work area and specific algorithmic modules as part of the MC firmware;
- apply approaches of monitoring and use of crypto-resistant and reliable fault-tolerance algorithms;
- use of special micro-antivirus (micro AV) local data access methods and outside platforms and data traffic control.

The effectiveness of these methods and approaches to protect the MC IS and quite often - the costs of their implementation do not fully allow to obtain the required full security level of the MC system.

Thus, in this points are possible to make changes of active data parameters in data processing in MCU for real time identification and decrease of malicious factors.

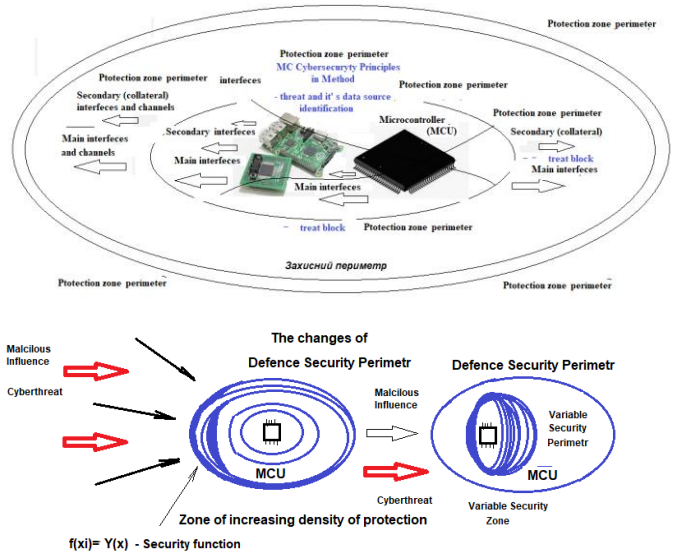


Fig.6. Illustration of forming variable security perimeter with data zones(points) in MCU architecture

Thus, as it shown at Fig.7 and also it was illustrate in Fig.2, data changes zones(points) are include inside in defence security perimeter, as a part of MCU architecture. They are forming different special places in MCU architecture with data change points. In this zones are forming potential points of active changes of data parameters(including threats data variables) to intrude and reduce of malicious threat factors by change data parameters (in memory variables) in MCU microprogram at memory, registers and special variables. It makes possible real active data accesses and special memory access methods in MCU such as x-DNA, x-SMA, or x-RMA.

In process of data mathematical simulation where built a dependence of security functions, which are describes an average characters of security actions under conditions with active malicious influences. It is shown at Fig.7.

TABLE I
CYBER DEFENSE MODEL FOR OPTICAL MCU WITH COMPLEX SECURITY FUNCTION $F_{SEC}(X_I, Y_{I,} N_I T_I$

Components of cyber defense MCU function $Fsec(x_i, y_i, n_i\ t_i)$ when forming a differential variable perimeter and the components of its formation	**Functionality and method of cyber protection in the MC's as part of the complex differential perimeter**	**Argum. x_i**	**Argum. y_i**	**Argum. n_i**	**Argum. of time dt_i (мкс)**	**P{f} V**	**Cyber threat type indicator f_i**	*** Criteria and function type $f_{sec}(x_i, y_i, n_i, t_i)_i$**
$f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ IDS}$	*Micro IDS*	0.1..0.2	0.1..0.3	2	0.01	0.1	+	$> f_{por}$
$f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ FIREWALL}$	*Micro FirewalL*	0.1..0.5	0.1..0.4	3	0.01	0.25	+	$> f_{por}$
$f_{sec}(x_i, y_i, n_i\ t_i)_{CRYPRO\ SEC}$	*Cryptograph. Sec*	0.1..0.4	0.1..0.3	3	0.01	0.15	+	$> f_{por}$
$f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ TUNNEL}$	*Micro Tunnel*	0.1..0.3	0.1..0.2	2	-	0.1	+	$> f_{por}$
$f_{sec}(x_i, y_i, n_i\ t_i)_{SIEM}$	*Monitor. & Detect.*	0.1..0.2	0.1..0.2	2	-	0.1	+	$< f_{por}$
$f_{sec}(x_i, y_i, n_i\ t_i)_{ZONE\ PERMITIONS}$	*Restrict Permis.*	0.1..0.2	0.1..0.2	1	-	0.1	-	$< f_{por}$
$f_{sec}(x_i, y_i, n_i\ t_i)_{OPTICAL}$	***Optical Technique***	0.1..0.3	0.1..0.2	2	-	0.2	-	$< f_{por}$

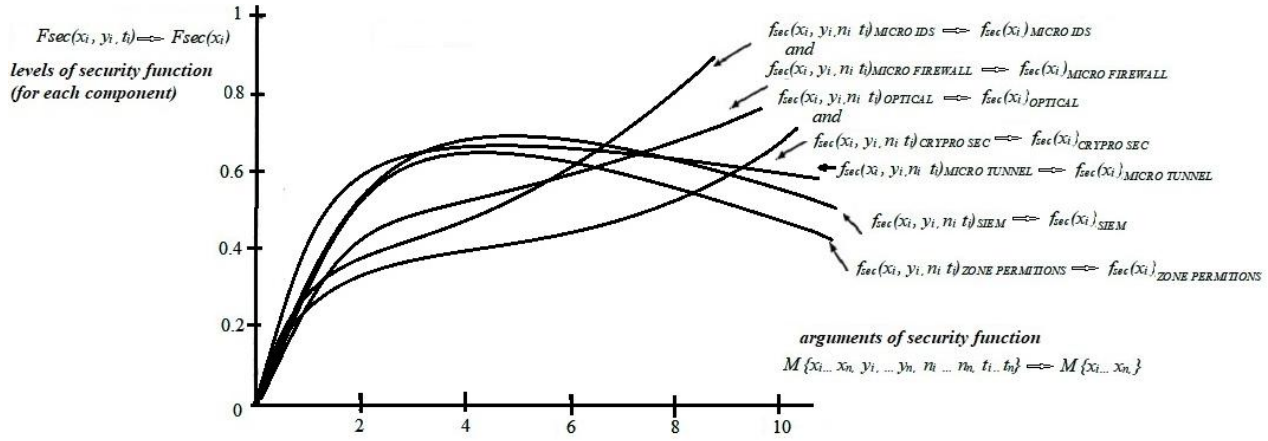


Fig. 7. Illustration of influences contribution for each security components $f_{sec\ i}(x_i, y_i, n_i, t_i)_i$.

Each specific component of the complex cyber defense function $fsec(x_i, y_i, t_i)i$ is described by a probabilistic nature of cyber threat protection (fig.7). Analyzing the results (Fig. 7), it can be shown that the greatest contribution is still made by the preventive protecttion system of the MC – the component $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ IDS}$, as well as the component responsible for creating a protective barrier $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ FIREWALL}$ – as a kind of micro-analog of a network firewall in classic security information systems.All components of cyber defense, in $Fsec(x_i, y_i, n_i\ t_i)$ play an important role and have a significant total contribution in MCU defence and active security.

This components is MC's security function: $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ IDS}$; $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ FIREWALL}$; $f_{sec}(x_i, y_i, n_i\ t_i)_{CRYPRO\ SEC}$ and $f_{sec}(x_i, y_i, n_i\ t_i)_{OPTICAL}$ are the most important in MC security. The protection function component is responsible for protecting information in MCs with optical interfaces. $f_{sec}(x_i, y_i, n_i, t_i)_{OPTICAL}$. This component of the complex protection function for the optical and/or optoelectronic part of the MC in the optical interface (or digital optical sensor, DOS), which is integrated into the MC. Optical protection function component $f_{sec}(x_i, y_i, n_i\ t_i)_{OPTICAL}$ corresponds to the crypto protection component in terms of impact level $f_{sec}(xi, y_i, n_i\ t_i)_{CRYPRO\ SEC}$.

The second level of contribution is the tunnel protection component $f_{sec}(x_i, y_i, n_i\ t_i)_{MICRO\ TUNNEL}$, if functions of obfuscation of address information (for example, bus addresses) and tunneling over MK interfaces are provided. Protection components $f_{sec}(x_i, y_i, t_i)_i$ in MCU can have a hardware or program basis: software; hardware and as a rule as part of the general protection function $Fsec(x_i, y_i, n_i\ t_i)$ in electronic and optoelectronic MCs have both the first and the second components. In the probabilistic description (in the particular case), the limits of the criteria $Fsec(x_i, y_i, n_i\ t_i) \in \{0..1\}$ witch form basic on complex protective function (2) are: $0 < \{Fsec(x_i, y_i, n_i\ t_i)\} < 1$, and at the same time, the approximation comes to "1" will mean greater protection of the MC system. And conversely, if its proximity to "0" – it means a lower level of protection and, accordingly, a need for a better security perimeter. The protection method, based on the principle of a protective imagine variable perimeter of a controlled zone with a microcontroller, involves the following stages:

- initialization and determination of MCs parameters;
- traffic analysis in primary and secondary interfaces;
- interactive blocking of traffic and cyberthreat source;
- implementation of optical protective practices for main data optical stream isolation in optical interface;
- quick restoration of the previous data states in MC. Implementation of flexibility, obfuscation of MC's parameters.

Implementation of adaptability and external support of MC's can provide key protection principles: flexibility, isolation, obfuscation, threats indicators(sensors) operating by parameters of the information MC's system. The interactive protection allows to create more dynamic and significantly more effective different levels of protection in various zones of the MC perimeter with the protection function $F_{sec}(x_i, y_i, n_i\ t_i)$.

The method involves the creation of a variable conditional imagine security perimeter in the structure of the microcontroller and the zone of active interaction with the threat itself when it

appears, and this perimeter is variable as the zone of contact with the cyberthreat itself and, and the impact itself is directly proportional to the impact and intensity of the cyberthreat processes. The methods have the following stages:

- shielding(covering) the information system;
- creating a variable secure perimeter in the structure of the MC to counteract the cyberthreat, with active increase density, defence of cybert threat intencity and opposite to cyberthreat direction;
- identification and block of the cyberthreat and influences;
- application of techniques for determinate of cyberthreat;
- neutralization of the consequences and verification of normal parameters and data states of the MC information system.
- monitoring and logging parameters of the cyber threat in MC.

IV. FEATURES AND EXPERIMENTS OF CYBER DEFENSE IN MK WITH OPTICAL INTERFACES

Considering cyber threats and types of information influences in MCs with an optical interface and individual digital optoelectronic sensors based on MC, have some specifics. For example, such attacks:

- unauthorized access and optical fault injections via the optical port at the operating wavelength λ_i [2- 4];
- optical MITM attacks (Optical MITM) with Y/T influence model at the working wavelength λ_i [2- 3];
- suppression of optical interference with power P_x in Y/T-models by third-party sources on λ_i ,
- direct influence on the optical medium, with modulation of it's parameters (such as, refractive index);
- can make the process of data transmission via the MC's with optical interface very difficult or impossible at all.

For more information protection over the optical interface in MC, the component of the complex protection function $f_{sec}(x_i , y_i , n_i , t_i)_{OPTICAL}$ is used in model (3) must have a more value. This component of the complex protection function must be organized on hardware level (L1 OSI) and provide better protection of optical flow $S_i(x_i , P_i)$ at the wavelength λ_i. A generalized scheme using optical protection technologies in method shown on Fig. 8.

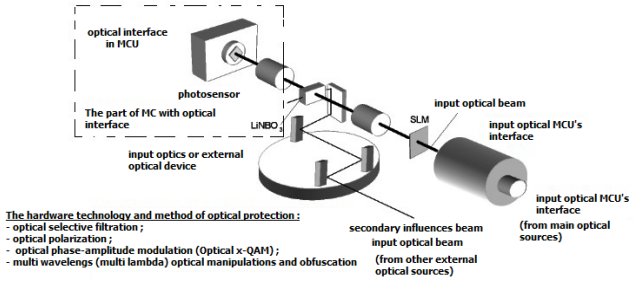


Fig. 8. Illustration of the application of optical technologies in MC protection method for component $f_{sec}(x_i , y_i , n_i , t_i)_{OPTICAL}$

In MCU's with optical interfaces, some physical optical techniques may be used additionally for protection (Fig.8):

- optical selective filtering, optical physical isolation, polarization, optical coding and modulation techniques in MC's ;
- use of optical multi-wave (Multi-λ) protection methods during transmission on lot of wavelength.

To prevent interception of optical signals and unauthorized access via the optical (including fiber-optic) interface in a microcontroller according to the T/Y-scheme model of optical MITM attacks, the cryptographic protection component $f_{sec}(x_i , y_i , n_i \ t_i)_{CRYPRO\ SEC}$ in model (3) can be used, which is an additional component of the cyber protection of the MC and operates at the software or hardware level in the MC. The main task is to increase the level of cyber defense by optical component $f_{sec}(x_i , y_i , n_i , t_i)_{OPTICAL}$ in the model (3). It is dominant in optical MC's $f_{sec}(x_i , y_i , n_i , t_i)_{OPTICAL} \rightarrow F_{sec}(x_i , y_i , n_i , t_i)$.

The cost/technological ratio of protection is not always optimal. The functional level of cyber protection of MCU systems do not always correspond to the necessary and sufficient level, especially considering modern "0"-day(Zero day) threats and the level of modern spyware and hacker software for MC and their based systems.

The experimental results of simulation of the information influences in optical interface in MC are shown on fig.9.

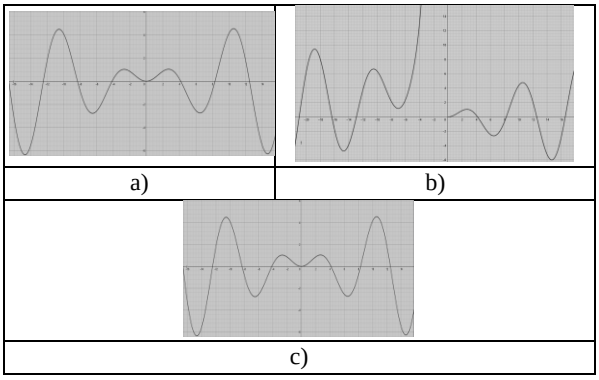


Fig. 9. Illustration of experimental character of the information influences on signal $S\ (t, \lambda i)$ in optical interface in MC: a) primary optical signal; b)optical signal with information influence; c) optical signal with protection by method (3)

Optical signal as it is, describes as $S(t, \lambda i)$ (fig.9, a) and described a normal data transfer process in simulation. The noise level (noise factor) $NR_e(t, \lambda_i)$ can conditionally describe a influence by optical interface side, which is shown (fig.9, b). Noise factor level forms additive interference in optical interface by third party sources at the transmission time t,, which forms the simulation system dynamics. It is main influence factor on hardware level in MC's with optical interface. For counter this, it's needed to compensate for the influence factor on optical hardware level by optical part in method (fig.9, c).But in some cases it is does not correspond to the real state of required protection level. To implement the cyber protection method in practice, it is necessary to take into account the specifics of the construction and architecture of the MC. It may be effective and functionality in difficult and high anisotropic electronic MC circuits (Fig.10).

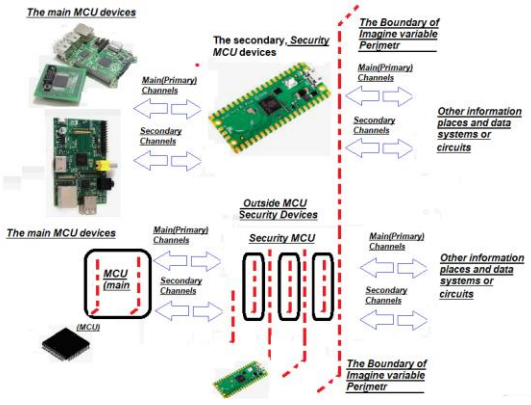


Fig.10. Illustration of forming a outbound part of variable security perimeter on secondary security MC devices

Therefore, the task of blocking and localizing cyber threats in the MC architecture is implements a universal set of cyberprotection measures and techniques for minimization information harmful effects and factors in MC structure.

V. CONCLUSIONS

The paper reviewed materials of research of cyber security of microcontrollers with optical interfaces. There had been considered the main factors of cyber threats in MC/MCU and shown principles for its neutralization. The protection method for MC's/MCU's with optical interfaces, which allows to increase the level of protection in MC's architecture was presented. A theoretical and experimental research of cyber protection method for MCUs with optical interfaces had been provided.

ACKNOWLEDGEMENTS

We are very grateful to experts for their appropriate and constructive suggestions to improve this material.

REFERENCES

[1] Malinovskyi V.I., Kupershtein L.M. "The analysis of cyber threats in microcontrollers // Information technologies and computer engineering, Vinnitsia, VNTU, Vol. № 3 [10] (2022), pp. 21-32, https://doi.org/10.31649/1999-9941-2022-55-3-21-32

[2] Jasper G. J. van Woudenberg, Marc F. Witteman, Federico Menarini. "Practical optical fault injection on secure microcontrollers // IEEE Xplore, Conference materials, Workshop on Fault Diagnosis and Tolerance in Cryptography Date of Conference, 28-28 September (2011), IEEE Conference, ResearchGate, Print ISBN:978-1-4577-1463-4, Doi: 10.1109/FDTC.2011.12. https://researchgate.net/publication/221427387

[3] Vanthanh Khuat, Jean-Luc Danger, Jean-Max Dutertre, Laser Fault Injection in a 32-bit Microcontroller: from the Flash Interface to the Execution Pipeline, //Workshop on Fault Detection and Tolerance in Cryptography (FDTC), Sep. 2021, Milan, Italy, pp.74-85, https://doi.org/10.1109/FDTC53659.2021.00020

[4] Joe Loughry "Oops! Had the silly thing in reverse" — Optical Injection Attacks via LED Status Indicators// arXiv, 2019, 30 june 2019, URL: https://arxiv.org/abs/1907.00479"/1907.00479, https://doi.org/10.48550/arXiv.1907.00479

[5] Dmytro Petryk, Zoya Dyka, Jens Katzer, Peter Langendoerfer. Metal Fillers as Potential Low Cost Countermeasure against Optical Fault Injection Attacks // arXiv, 2021.URL: www.arxiv.org/abs/2103.1243 https://doi.org/10.48550/arXiv.2103.12436

[6] White, D., Clark, E., & Lee, S. Optical security for integrated circuit designs: From classical to quantum approaches// Journal of Lightwave Technology, 2023, №41(2), pp.456-472. https://doi.org/10.1109/JLT.2023.3089512

[7] Walker, C., Turner, I., & Lee, B. Designing secure hardware systems with optical interface protection// In Proceedings of the Design Automation Conference (DAC), 2023, pp.1215-1221, https://doi.org/10.1109/DAC.2023.9254897

[8] National Security Agency. Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments//NSA, https://web.archive.org/web/20121002051613 https://www.nsa.gov/ia/_files/support/defenseindepth.pdf (Retrieved 2026-02-03)

[9] Chris Sanders, Jason Smith . Applied Network Security Monitoring Collection, Detection, and Analysis, 2014. p.496, ISBN: 9780124172166.

[10] What is defense in depth? Layered security. CloudFlare, https://www.cloudflare.com (Retrieved 2025-10-02)

[11] Cybersecurity Spotlight - Defense in Depth (DiD). CIS. https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did (Retrieved 2026-02-05).

[12] Shevchenko, P. V., J. Jang, M. Malavasi, G. W. Peters, G. Sofronov, and S. Trück .The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity, 2023, №9(1), pp.016, https://doi.org/10.48550/arXiv.2202.10189

[13] Pavel Yermalovich. Determining the Probability of Cyberattacks European Journal of Formal Sciences and Engineering, February 2020, №4(1):46, https://doi.org/10.26417/ejef.v4i1. pp.46-63

[14] Md Hasan Shahriar, Yang Xiao, Pablo Moriano, Wenjing Lou. "Signal-Based Intrusion Detection for CAN. Researchgate, SAE International, 2022. Url: https://www.researchgate.net/publication/360353566_CANShield_Signal-based_Intrusion_Detection_for_ Controller_Area_Networks