Article

Cyber Attack Prevention Based on an Evolutionary Cybernetics Approach

Dmitry Zegzhda, Daria Lavrova *, Evgeny Pavlenko and Anna Shtyrkina

Institute of Cybersecurity, Peter the Great St. Petersburg Polytechnic University,
195251 St. Petersburg, Russia; dmitry@ibks.spbstu.ru (D.Z.); pavlenko@ibks.spbstu.ru (E.P.);
anna_sh@ibks.spbstu.ru (A.S.)

* Correspondence: lavrova@ibks.spbstu.ru; Tel.: +7-950-034-9578

Abstract: The paper looks at the problem of cybersecurity in modern cyber–physical systems and proposes an evolutionary model approach to counteract cyber attacks by self-regulating the structure of the system, as well as several evolutionary indicators to assess the state of the system. The application of evolutionary models makes it possible to describe the regularities of systems behavior and their technical development, which is especially important regarding cyber attacks, which are the cause of a discontinuous evolution of complex systems. A practical example describes a system behavior during attacks and the self-regulation of its structure. The methodological approach consists of using evolutionary models to describe how modern cyber–physical systems can counteract cyber attacks and evolve, building on the experience of past security incidents. The main conclusions and recommendations are presented in the Discussion section, and they consist of the fact that using an evolutionary approach will not only increase the security of cyber–physical systems, but also define the principles of building systems that are resistant to cyber attacks.

Keywords: information security; cyber–physical systems; cyber attack; evolutionary cybernetics; self-regulation; graph theory

1. Introduction

Industry 4.0 is characterized by widespread digitalization of a large number of human activity areas. This fact has led to the creation of a certain class of systems in which the implementation and management of the physical processes take place through digital control. Later on, we will define such systems as cyber–physical systems (CPSs) [1–3]. Examples of CPSs are Smart Home systems, Smart Grid systems, IoT, and Industrial IoT. Obviously, there are a large number of CPS examples that work in rather critical areas of human activities (for example, nuclear power). Breaking of security in such systems can lead to disastrous consequences (financial losses, as well as threats to human life and health). In this regard, the task of security of CPSs is particularly important at the present time.

Information security of CPSs is a new and complicated issue due to a number of factors. In particular, ensuring the classic properties of confidentiality, integrity, and availability is no longer sufficient to ensure the security of a CPS. A CPS differs from information systems in that it includes not only information but also physical processes. Physical processes are separate from information processes and are irreversible. Therefore, to ensure the security of a CPS, it is necessary not only to maintain the classical principles of data protection, i.e., confidentiality, integrity, and availability of information, but also to take additional measures to ensure that the system correctly and continuously implements its physical processes.

To ensure resilience to cyber attacks, it is important to take into account the features of the CPS:

(1)　existence of the target function—the main purpose of the system, breaking of which leads to undesirable consequences threatening the process of controlling the system;

(2)　the systems constantly communicate with the environment via the Internet or parts of the network;

(3)　the development of digital control CPSs that use artificial intelligence technology, which is manifested in the properties of memory, automatic testing, and the ability to determine the damaging effects and counter them, the result of which is the property of self-regulation or reconfiguration to counter these effects in order to preserve the target function [4].

In critical infrastructure, a fast response to the attacks and prevention of serious consequences are important parts of security ensuring. In this regard, an important stage is cyber attack prevention, which allows realizing the response mechanism to ensure the system's sustainability during destructive influences.

One of the ways for automated attack prevention is to build a self-regulation structure of the system. This paper proposes an approach based on evolution cybernetics that allows to determine the process of a CPS's functioning and mechanism of automatic change in the CPS structure, which makes it resistant to cyber attacks. It is obvious that the laws that underlie the evolutionary process are quite effective, so it is proposed to adapt these rules to the principles of CPS security. The prevention of an attack within the scope of this article should be understood as both interrupting an attack during its implementation and mitigating its effects.

The topic of this paper is extremely important because the successful application of evolutionary models and equations to analyze the behavior of complex systems (in particular, cyber–physical) will provide information about the security of the system over time.

The objective of this study is to obtain the numerical and graphical characteristics of whether a cyber–physical system is safe or not. Such assessments will also allow to estimate the system's resistance (resilience) to cyber attacks of different types and intensities. Watching the state of the cyber–physical system in a dynamic environment, on the one hand, allows security professionals to quickly make an effective decision to protect the system. On the other hand, monitoring allows to identify some parts of the system that are resistant to some attacks, which opens up an opportunity to describe the regularities in the architecture of attack-resistant systems.

The authors' contribution to the article is to describe the functioning of the cyber–physical system in the form of a graph (including a description of the target function of the system), to make analogies between the genome, chromosomes, evolutionary mechanisms (selection, mutation, and crossing), and components and mechanisms of the cyber–physical system. The authors also contribute to the application of mathematical evolutionary models to the new subject area and to the obtaining of dynamic estimates characterizing the system stability reserve, its self-regulation capabilities, and its reaction to cyber attacks.

Applying this methodology in real-life conditions will allow to:

1.　Describe the space of acceptable CPS states. By building a landscape, it will immediately become clear which components of the system provide the largest number of reconfiguration routes. It is these components of the system that must be more protected against cyberattacks, since a large number of new routes will be passed through them.

2.　Simulate the different types of cyberattacks on the system and understand which type of attack this CPS is most vulnerable to. This will make it possible to immediately formulate recommendations on how to configure security features in the infrastructure.

3.　When implementing an attack on a system, the CPS will be able to accumulate the self-regulation scenarios chosen to neutralize these attacks and next time respond to an attack of the same type almost instantly.

The attack on the petrochemical plant in Saudi Arabia in 2017 is a real-life example. The attack disrupted six plant controllers at once, resulting in weeks of plant downtime. Using the approach proposed in this article, these controllers would have been replaced by other, less loaded or

redundant controllers as a result of self-regulation. So, downtime and financial losses would have been avoided.

2. Application of the Evolutionary Approach to the Security of a Self-Regulating CPS (SRCPS)

The evolutionary process that brings about change is crucial for cyber–physical systems. The evolution of their structure, their functioning, and their mechanisms is closely linked to the continuous evolution of technology. The emergence of new technologies and the ubiquitous digitalization lead to new technical concepts and solutions. However, new technologies always present security threats. This is why it is so important to give cyber–physical systems the ability to evolve by providing characteristics inherent in living organisms.

The process of ensuring security is a function of a self-regulating CPS (SRCPS). This function can be represented as an abrupt transition, carried out when the structure is changed by self-regulation, which allows to neutralize destructive effects to maintain functionality [5]. The structure in this case should be understood as the network configuration of the system, which is presented as a graph. Since the external effects are continuous, the sequence of state changes can be considered as evolution according to the existing generalized concept of evolution [6].

The article proposes to apply the evolution models to model the information security (cyber-resistance) process. An evolutionary process is a complex process of wildlife development, which is accompanied by changes in the genetic composition of populations, the formation of adaptive properties. At present, it is possible to trace the long way of formulating the general laws of evolutionary cybernetics, which made a great leap after the discoveries of genome structure and so on. Evolutionary processes are widely considered in biology and genetics, and the biological principles of complex organisms have been successfully applied when transferred to technical systems. In this connection, the authors believe that the mathematical apparatus of evolutionary models will successfully describe the process of confrontation with SRCPS by destructive external influences.

Evolutionary models are used for the first time to solve various cybersecurity problems, and for the first time for the new subject area of cyber–physical systems. As a rule, various aspects of evolutionary theory and genetics were used to solve optimization tasks, partly related to cybersecurity. This paper proposes to use mathematical aspects from the theory of evolution to obtain a system's global properties and its behavior characteristics under cyber attacks. The proposed approach is unique in that it provides an opportunity not only to solve the problems of system restructuring and thereby counteract cyber attacks, but also to solve an important technical problem of the synthesis of the structure for systems resistant to cyber attacks.

At the same time, it is necessary to take into account the features of the information security issue:

1. The change of state (change of SRCPS structure) occurs only under the external and purposeful influences. In the absence of such effects, the system is stable.
2. The change of state (actually, the process of evolution) occurs not casually, but under the influence of the programmed control, which can be initiated either decentralized or from an external control point.
3. The total allowed number of system states within which the evolution takes place is limited by two factors:

    (1) the need to unconditionally perform the general target function of the system, which is taken into account when selecting new states;
    (2) limited resources of the system as self-regulation is connected with its redundancy.

However, such a scheme of functioning can be compared with a great variety of evolutionary schemes, because as a result, in SRCPS, as in biological systems, two processes are continuous:

(1) a destructive process changing individual nodes of the system;

(2) a self-regulation process that opposes the destructive effects.

The ratio of intensity of these processes can lead both to an increase in the number of stable states, i.e., to a positive direction of evolution; an increase in the adaptability of the system to the flow of attacks; and to a reduction in the space of acceptable states, i.e., degradation of the system, both due to limited resources and as the intensity of attacks increases.

Finding out the possible causes and limits of this interaction is the essence of this article. To study the regularities of these processes, it is proposed to use the mathematical apparatus of evolution models in SRCPS taking into account the specifics of security problems.

The process of SRCPS operation, in accordance with the provisions of Anokhin and Turchin, consists of detecting attacks, the flow of which is almost continuous in their localization, and finding a new variant of structural links or composition of the modules involved, in which the attack is impossible (Figure 1).
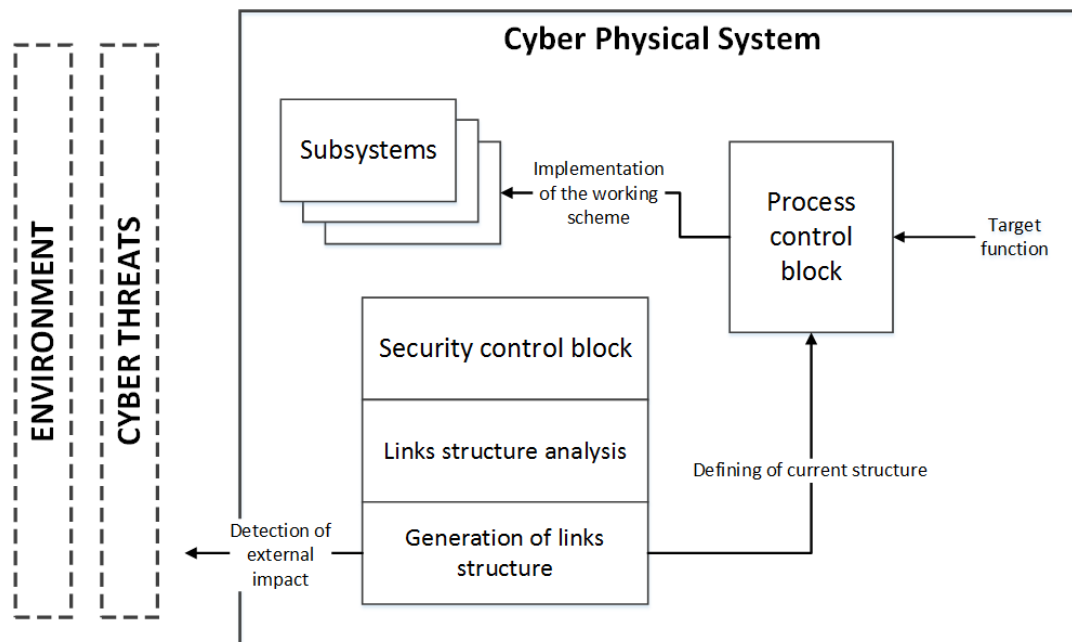

Figure 1. Scheme of a self-regulating cyber–physical system's (SRCPS) operation.

Figure 1 shows that the SRCPS implements an evolutionary process; it takes place primarily in the security control block—there are the detection, localization of the attack and generation of the system's self-regulation algorithm to prevent attacks or minimize their negative impacts.

Key elements of the cyber–physical system are the security control block, process control block and various subsystems. The security control block is designed to detect the harmful effects of the environment on the system, and to implement a link structure analysis because, as will be shown in Section 4 of the article, it is the graphical representation of the relationships between the system components that is most convenient for tracking cyber attacks and their consequences. The security control block also implements the configuration of link structures to restructure the system to counteract attacks and neutralize their impact. The tasks of the process control block include technical reproduction of the graph structure generated by the security control block using real components of the cyber–physical system. Another important task of the process control block is the control of the system's target function. The subsystems perform the implementation of the target function by replacing each other or distributing computing tasks to each other.

Such a process can be interpreted as a system evolution (development), in the course of which a number of structural blocks (or individual modules) are discarded or replaced, and the system maintains operability, preserving the variants of the structures and composition, while maintaining system security (i.e., maintaining a common target function) in case of permanent external perturbations.

3. Related Works

The context of this paper is the use of various evolutionary and bioinspired approaches for complex technical systems. This is necessary in order to establish whether someone has studied the possibility of using evolutionary models to improve technical systems. As an improvement, we are primarily interested in the area of cybersecurity. In the context of this work, we have found that evolutionary theory is extremely complex and involves many approaches and algorithms that can be used in technical systems in any way. It has been found that popular areas for evolution are genetic algorithms, mechanisms for self-regulation and homeostasis, and the behavioral principles of living organisms. Related works by Russian and foreign authors were investigated and it was identified which scientists focused more on which technical systems problem.

The related works will be divided into four groups:

A. Works in the field of optimization theory, which are based on genetic and evolutionary algorithms. Genetic algorithms are not fully suitable for the considered task of ensuring the SRCPS's information security, since they are aimed at solving optimization tasks, while in counteracting attacks the system requires not an optimal solution, but any of the algorithms suitable for restoring the target function. However, genetic algorithms provide high speed and have versatility, according to [7,8]. For example, in [8], the authors analyzed the results of different optimization techniques and noted that "The genetic algorithms achieve an excellent result in much shorter time than the others. It is to be noticed that, in all the previous experiments, the genetic algorithm has performed better than manual configuration and random search".

B. Works devoted to the self-regulation of systems and ensuring their viability [9–11], among them there are some works aimed at modeling the behavior of complex systems. The works devoted to functioning and modeling the behavior of self-regulating systems, such as the MANET and VANET networks [12,13], which have a clearly defined target function, can be noted. Complex adaptive and self-regulating systems must be characterized by the coherence of their components and be resistant to destructive influences. In addition, modeling the behavior of self-regulating systems is used to solve various practical tasks of important social importance [14–16]. Thus, in [15], four modern multipurpose evolutionary algorithms are used to solve the problem of designing transit transport networks. The authors of this paper [15] noted the good results of the evolutionary approach, in particular they observed the usefulness of the crossover operator, which randomly combines two solutions into one, and a simple mutation scheme, which is not biased to any objective function, to handle the many-objective nature of the transit network design problem. In [16], an evolutionary approach to the design of productive and resilient capacitive networks is presented, which minimizes costs and delays in data transmission.

C. Works devoted to the general theory of development and improvement of technical systems and application of the theory of evolution to describe the process of system intellectualization. Such models are based on the provisions of the works of Peter Kuzmich Anokhin and Valentin Fyodorovich Turchin [17–20], who were the founders of the idea that technical systems are a special case of any other systems and, therefore, they cannot obey some general biological laws. The theory of functional systems, proposed by Anokhin [17], has gained practical application in many branches of science and technology over more than half a century of its development, which confirms its versatility. The system-forming factor, according to this theory, is a specific result of the system's functioning: the system is a complex of selectively involved elements that interact in achieving a given useful result. This theory is used to transfer the most important properties of living organisms (adaptability, flexibility, and a proactive response) to technical systems. Continuing their ideas, Redko [21] shows that the development of any system includes their intellectualization, and in the course of their development the system expands its intellectual abilities. Anokhin has developed the theory of systems evolution as a generalization of mutation and natural selection processes, including before the advanced reflection of external influences on the system [17,18]. Turchin applied a cybernetic approach to evolution by

proposing the theory of metasystemic transitions that allow to apply the evolutionary approach to technical systems, treating the development of these systems as jump transitions causing structural changes [19,20]. From an information security point of view, Turchin's approach is more suitable, because when a system implements a cyber attack, at some random moment of time, it experiences a sudden change caused by external action; this is its development, its evolution [20]. Together, the provisions of Anokhin, Turchin, and Redko are applied to global industries, allowing to predict the development and evolution of various complex systems [17–21]. However, as a rule, such approaches are global in nature and do not address the problem of information security, although this problem is an integral part of the digital transformation of the technological mode. Thus, it can be concluded that these approaches are expedient to apply for solving information security problems.

D. Works devoted to the application of evolutionary models to solve the problem of information security in technical systems. Such works are very few in number, and they are usually devoted to solving certain narrow tasks in the field of information security. Thus, there are known works [22–25] devoted to the research of computer viruses and malware evolution—both in terms of the program structure itself and in terms of the speed of infecting system components. For example, in [23], the authors use an evolutionary approach to describe a change in the dynamic behavior of polymorphic worms, a family of computer viruses capable of changing their own structure, which makes them extremely difficult to detect. The authors use an evolutionary model of quasi species, where quasi species are polymorphic populations of the same species, which is fully consistent with the subject area of polymorphic computer viruses. Separate provisions of the theory of evolution are used in works that use genetic algorithms to solve various security issues.

Thus, analysis of the relevant works has shown that there is now a wide range of works that demonstrate the successful application of bioinformation methods in technical systems. The application of theory of evolution methods allows us to describe the technical development of complex systems and identify the limits of their permissible state.

In this paper, evolutionary models are used for the first time to solve global cybersecurity problems, and for the first time for the new subject area of cyber–physical systems. As a rule, various aspects of evolutionary theory and genetics were used to solve the optimization tasks, partly related to cybersecurity. This paper proposes to use mathematical aspects of the theory of evolution to obtain the global properties of the system and characteristics of its behavior under cyber attacks. The proposed approach is unique in that it provides an opportunity not only to solve the problems of system restructuring and thereby counteract cyber attacks, but also to solve an important technical problem of the synthesis of the structure for systems resistant to cyber attacks.

4. Model of Self-Regulating Cyber–Physical Systems' Functioning and Attacks on Them

As the object of the proposed approach, we will consider self-regulating cyber–physical systems and systems close to the systems of the Internet of Things, as well as intellectual and mobile agents. An example of such systems are wireless sensor networks and intelligent power consumption networks, such as the Smart Grid. For these systems, a common target function is a system-forming function, maintenance of which determines the target purpose of the system. In addition, the systems can be described in general terms by a graph structure.

The SRCPS model can be represented as a oriented graph $G = <V, E, R>$, where $V = \{v_1, \ldots, v_N\}$ —a set of its vertices (structural components); $E = \{e_1, \ldots, e_M\}$ —a set of its edges (intercomponent relations); $R = \{R_{ij}\}$ —a set of routes of graph G, the elements of which represent a set of different paths from the vertex v_i to the vertex v_j.

Each vertex v_i of the graph is described by a tuple $<\beta, type, \mu, \vartheta>$, where β is the identifier of the vertex, $type$ is the type of component, μ is the set of parameters of the vertex, and $\vartheta = \{p_1^m, p_2^m, \ldots\}$ is the set of functions supported by the node, where the index m indicates the mode of the function's execution (whether the node uses the p_i functionality in the current process or not).

Each connection is characterized by a set $< \delta, \omega, e_i >$, where δ is a node identifier and $\omega = \{v_1, v_2, \dots, v_k\}$ —a set of parameters that characterize the connection. Any technological process running in the system has a set of working paths, $R = \{R_{ij}\}, R_{ij} = r_{ij}^{(1)}, r_{ij}^{(2)}, \dots, r_{ij}^{(k)} =< v_i, \dots, v_j >, k = \overline{1, |R_{ij}|}$. The work paths are represented by the set $R_p \subseteq R$ on the set of routes of graph G, which in a functional sense has a set of functions $\Phi = \{\varphi_1, \varphi_2, \dots, \varphi_m\}$, associated with the nodes of the system and executed over the input data and external systems. According to the above notation, a process can be described by mapping $F_p : \Phi \to \Omega$, where $\Omega = \{p_1^m | m = 1, v_i \in R_p\}$ is a set of the nodes' functions that are involved in the process.

Cyber attacks of the CPS aimed at disabling individual nodes, at the breaking (appearing) arcs, and the number of which characterizes the intensity of cyber attacks Z, can be expressed by the operator as $Z \to G(V, E, R) \to G'(V', E', R')$.

Modeling attacks in terms of graph conversion has a proven completeness, as the attacks can be systematized by selecting the following types:

(1) structural: unary operations on the graph;
(2) functional: changes in vertex and edge parameters.

The danger of cyber attacks is determined by the following characteristics:

(1) type of implemented cyber attack (its criticality, intensity);
(2) the type of system components that failed as a result of an attack, based on an acceptable risk assessment;
(3) the involvement of the failed component in the many routes of the target function's implementation.

The proposed approach focuses on those cyber attacks that aim to disable the cyber–physical system. That is why this article does not focus on spy attacks, for example, as they do not disrupt the target function. An example of computer attacks in the form of structural transformations of the column expressed by unary operations is presented in Table 1.

Table 1. An example of computer attacks in the form of structural transformations of the graph, expressed by unary operations.

Cyber Attack (Unary Operation on the Graph)	Changes that Occur in the Column	Example of An Attack, Expressed as A Change in the Column
1. Removing the vertex v_i from graph G, transformation into a new graph G'.	The vertex and all the arcs incident to it are removed from the count: $G =< V, E >$, $G' =< V', E' >$, $V' = V \backslash \{v_i\}, E' \subseteq E$	Denial of Service attack (DoS, DDoS), system component failure.
2. Closing (merge or identification), transformation into a new graph G'.	A pair of vertices v_i, v_j in graph G is closed if they are replaced by such a new vertex v_k that all arcs in graph (orgraph) G, incident v_i and v_j, become incident new vertex v_k	Sinkhole attack, typical for wireless sensor networks. A compromised network node "listens" to route requests and responds to nodes that "knows" the shortest route to the base station.
3. Removal of arc e_{ij} from G, transformation into a new graph G'.	Only the e_{ij} arc is removed, vertex v_i, v_j remain: $G =< V, E >, G' =< V', E' >$, $V' = V, E' = E \backslash \{e_{ij}\}$	Changes to operating rules or system settings that prohibit the transfer of data between system components.
4. Breaking up the arc (adding a new vertex to the arc), transformation into a new graph G'.	A new vertex v_k is added to graph G, arc e_{ij} is removed, arcs e_{ik} and e_{kj} are added. $G' =< V', E' >$, $V' = V \cup \{v_k\}$ $E' = (E \backslash \{e_{ij}\}) \cup \{e_{ik}, e_{kj}\}$	Man-in-the-Middle (MITM) attack, intrusion by an intruder into data transmission or data interception.

The proposed model of the system and attacks describes network-like structures to which most systems come down. This model has a demonstrative completeness in relation to the types of computer attacks. The aim of this article is to analyze the development of the system during destructive processes and how the system can increase its resistance to cyber attacks.

The context of the developed model is limited by the network infrastructure of modern cyber–physical and industrial systems. The network structure can be either centralized or decentralized. Partially decentralized network options are also possible, which is typical of many industrial systems that include a large number of sensors, which are correctly organized into a sensor-based decentralized network. However, this model cannot yet be directly transferred to global and international networks, as in many ways the model is tied to the system's target function and for global networks it is difficult to identify it unambiguously.

Self-regulation only affects the structure of the system presented as a graph, namely, the communication links between the system components. Self-regulation is based on initiating new connections between devices or, conversely, severing certain connections (e.g., connections with compromised system components). The duration of self-regulation in this case is assessed in relation to the time of the attack. In order to prevent an attack (to prevent the attacker from reaching his final goal) or to quickly neutralize the consequences of an attack, self-regulation has to be carried out within a time frame of no more than 30% of the attack's time. This is a crude experimental assessment and the time for self-regulation must be minimized.

5. Evolutionary Cybersecurity Scheme

In [26], the method of reflection and prevention of computer attacks by dynamic reconfiguration of the system structure, consisting of exclusion or replacement of the typical nodes to save the performed target function, is proposed. The formal representation of the process of security breach and the process of self-regulation can be represented as an evolution of the system, consisting of the replacement of links and nodes with the subsequent selection of options for which an attack is not feasible.

The general task of ensuring self-regulation of complex systems can be represented as a search for a surjective mapping $\psi: \Gamma \to D$ (where Γ is a set of states, and D is an area of correct functioning), which translates the current state of a system $x(t) \in \Gamma$, in which the system is in time t, taking into account the destructive influence $z(t)$ that has been affected the system into the area of correct functioning D.

The quality of the process implementation is formalized in the following way:

$$Q = Q(\Phi = \{\varphi_1, \varphi_2, \dots, \varphi_m\}, \vartheta = \{p_1^m, p_2^m, \dots\}) \tag{1}$$

where Φ is a set of functions associated with the system nodes.

The object of self-regulation and evolution is a route—a sequence of pairs of connected nodes. From the point of view of evolution, it is the object of mutation and selection.

Within the proposed scheme of evolutionary cybersecurity, the population is a tuple, which includes components of an SRCPS and a set of routes to implement the target function: $\{N, \{P_1, \dots, P_N\}\}$. Thus, the population is all the permissible routes of the target function implementation, but taking into account the number of SRCPS components. Let us match the route of the target function implementation to the genome, and a pair of interacting devices of each route $x_{F_k, i}; x_{F_{k+1}, j}$ to the chromosome. Just as the genome contains the biological information needed to build and maintain the organism, so the target function contains a set of attributes needed to perform the system in question.

The intruder, acting on the SRCPS, implements a destructive information effect Z, determined by its input data z, the destruction of L, introduced into the system and associated either with the impact on the nodes, or with the impact on their connections, or with the impact on the functionality of the nodes. Z is a variable function described at alternating intervals and taking into account random influences denoted as L_k, here L_k is a pair of SRCPS components characterizing a cyber

attack localization point. When performing mutations, different effects on chromosomes are possible: replacement of the whole chromosome, a part, or rearrangement of the chromosomes.

Considering the self-regulating SRCPS for a certain period of time, we can speak about an evolving system of pair sequences, for which the evolution equation is generally represented by a formula:

$$\frac{\partial Q}{\partial t} = AQ(t) + BZ(t, L_k),$$ (2)

where A and B are constants.

Let us consider the evolutionary process in more detail. Evolution of an SRCPS is performed in two stages:

1. The first stage of evolution consists of the selection of adapted genomes. Adapted genomes are those whose chromosomes were not destroyed by a cyber attack. The mechanism of evolution at this stage is self-regulation of the system.
2. The second stage of evolution consists of the formation of a "skill" or "conditioned reflex", consisting of the association of a type of destructive cyber-influence and a type of genome resistant to this influence. At this stage, the signs and characteristics of the genomes resistant to the implemented cyber attacks are fixed and inherited during the course of the evolution.

The genetic equation of the security process characterizes the dependence of changes in the X population composition over time on the mutation and inheritance processes. Let us describe these processes mathematically before introducing the equation.

Mutation model *Mutation* can be presented as a tuple of elements $Mutation = <Z, Reserve, M >$, where

(1) Z is the destructive information effect (cyber attack) on the CPS, wherein the model of mutations should be considered in the context of the set of nodes of the X_Z system (cardinality of the set $|X_Z| = N_Z$), which it failed, and the intensity is the speed of its propagation in the $Z(t)$ system;
(2) Reserve is the system's ability to evolve (to change itself) to counteract a Z cyber attack and to exclude conditions for its implementation or elimination of consequences; these capabilities are characterized by the number of remaining chromosomes (node pairs) in the CPS: $X/X_Z = N - N_Z$ and the number of genomes (routes) that can be built on them: $P(X/X_Z) = P(N - N_Z)$;
(3) M is the mutation mechanism, which is characterized by the system modification rate $\vartheta_{X/X_Z}(t)$ to adapt to the changed environmental conditions resulting from Z and the set of actions on the many remaining chromosomes $R(X/X_Z)$.

The inheritance model will also be presented as a tuple: *Inheritance* $=< Z, \varphi >$, where

(1) Z is the destructive information impact (cyber attack) on the CPS, and within the framework of the inheritance model should be considered in the context of many nodes of the X/X_Z system, which it did not affect;
(2) $\varphi_{P(X/X_Z)}$ is the characteristics of the routes fixed in the system after a cyber attack. It is these characteristics that must be inherited during the evolution of the system in order to increase its cyber-resistance to attacks, similar to the type of cyber attack Z. $\varphi_{P(X/X_Z)}$ can be presented in more detail via the characteristics of the included nodes $\sum_i \varphi_{X/X_Z}^i$. It is also important to know how long the nodes already under consideration live in the system, as described by the function $\varphi_{P(X/X_Z)}(t)$.

When choosing an acceptable variant of evolution, it is necessary to take into account the limitations imposed on the evolutionary process. To do this, let us enter parameter E, which aims at keeping the number of chromosomes close to a constant, $E: \sum_i^K \sum_j^m x_{ij} = N = const$. In addition, this parameter is responsible for the limitations associated with the interaction of the chromosomes (not all SRCPS nodes are able to interact).

Let us write down the general genetic equation:

$$\frac{\partial X}{\partial t} = \frac{X_Z}{P(N - N_Z)R(X/X_Z)}Z(t)\vartheta_{X/X_Z}(t) + (N - N_Z)(X/X_Z)\varphi_{P(X/X_Z)}(t) - E \tag{3}$$

The SRCPS resistance to the current attack is also determined by the system structure and its ability to quickly adapt $\vartheta_{X/X_Z}(t)$. At the second stage of the SRCPS evolution, the features and characteristics of the genomes resistant to the implemented cyber attacks are fixed and the inheritance of these features should be determined at least in general terms as those features of the routes to be inherited.

Routes are characterized by the following factors:

(1) *time*: time of the route execution—this parameter actually means the system response speed;
(2) *perf*: average performance—this parameter allows to estimate how productive the nodes are in the route;
(3) *len*: the length of the route, which allows to assess the "fragmentation" of the route. The more "fragmented" a route is, the easier it is to transfer some functionality to the neighboring nodes.

Then we denote the density of routes in space at a time point t as $f(a, t)$, where a—route adaptability. It is determined by its parameters: $a = \{time, perf, len\}$.

According to [21], we believe that for a particular case—for a simple SRCPS type of sensor network—the solution of Equation (2) can be roughly represented as an envelope:

$$\frac{\partial Q}{\partial t} = \frac{\partial(\ln Q)}{\partial t} = A\left(1 + \frac{B}{A} \cdot \frac{Z}{Q}\right) \tag{4}$$

where $t = 0, Q = Q^0, Z = 0$.

With further simplification, this is reduced to a logistic curve:

$$Q(t) = \Gamma\left(1 - \frac{Q(t)}{Q}\right)Q \tag{5}$$

where $Q(t)$ is the number of routes at moment t.

Speaking about the limits of possibility of the evolution of the considered system, the indicator characterizing some reserve of stability of the SRCPS in relation to the cyber attacks is important. Let us consider that resistance to an attack, ψ, is the conservation of Q at Z. Then, the stability dynamics can be described by the following equation:

$$\frac{d\psi}{\partial t} = \alpha_1(f_1 + \alpha_2 f_2 + \alpha_3 f_3 + \alpha_4 f_4), \tag{6}$$

$$\psi = \ln Q = \frac{\Delta Q}{Q}. \tag{7}$$

Here,

(1) $f_1(t)$ expresses the number of potential routes at moment t with the current Z, building in an available set of chromosomes;
(2) f_2 is a function of the number of chromosomes preserved during the attack;
(3) f_3 is an attack function: proportional to the relative number of affected routes with the weight of connectivity of the attack node by the sequence of attacking nodes;
(4) f_4 is a weighted sum of the saved (stable) nodes, taking into account the technical reliability or potential vulnerabilities.

To specify the functions, let us enter the parameters:

(1) α_1: stability coefficient of the remaining nodes (number of generations);
(2) α_2: coefficient of the "danger" of attacks—it is proportional to the number of links with other nodes and the number of excluded routes;
(3) α_3: time intensity of the attacks;
(4) α_4: technical "aging" of the stored nodes (chromosomes), which allows taking into account such "physical" characteristics of the SRCPS, such as technical stability and reliability.

6. Security Evaluation and Proposed Security Indicators

This section is devoted to the following problems:

(1)　to analyze the development of the SRCPS and identify the cases where it is most sustainable;
(2)　to assess the degree of destructive power;
(3)　to evaluate the adaptability of SRCPS in terms of its ability to evolve, as well as the system's survivability.

Simulation modeling was used to solve the above tasks: the network infrastructure of the cyber–physical system was presented in the form of a graph, and all the research was conducted in this graph. The importance of the simulation modeling is based on the fact that it is this graph representation that makes it possible to study the state of the system as a whole by simultaneously seeing the entire structure of the graph and all the changes made to it. If the simulation had dealt with the parametric characteristics of the system, it would not have provided a single picture of the state of the system.

Therefore, the approach to cybersecurity based on evolution cybernetics can be done using the following steps:

1.　Represent the CPS as a graph. Each object of this graph (vertices, edges) should have characteristics (time, performance, and so on). Of particular importance for the vertices of the graph are the functions that these vertices are capable of performing. It is the community of functions that is based on the mechanism of self-regulation, because the replacement of the vertices should be carried out taking into account the ability of the new vertex to perform at least partly the functions of the previous vertex.
2.　Express the target function of the system as a working route on the graph—sequences of pairs of vertices. In terms of evolutionary cybernetics, a set of all the routes is a population, one route is an individual, and pairs of vertices are a chromosome.
3.　Select the signs and characteristics of the individuals in the population. This choice depends on the type and features of the systems. For example, it can be the time of route execution and the average performance of the route. Important characteristics of the individuals include: time to perform the necessary functions and the average performance of the top.
4.　Applying an evolution process to the cybersecurity of the CPS:

    a.　Modeling an attack on the systems provides the first stage of the evolution process: select adapted genomes. This stage is well suited for cyber–physical systems at the design stage and for cyber–physical systems that are in test mode (in order to identify vulnerabilities in the system). Various cyber attacks on the system were simulated, ranging from simple cyber attacks presented as unary transformations of the graph to complex, targeted attacks that disrupt several components of the system simultaneously. Such attacks are represented as multiple unary transformations of the graph;

    b.　Determine the mutation model, inheritance model and limitation of the evolution process, through formulation of the general genetic Equation (3). This stage provides new knowledge about the cyber–physical system; in particular, its ability to evolve and how long the system can exist and perform its intended function during cyber attacks;

    c.　Provide the second stage of the evolution process: fix the signs and characteristics of the genome resistant to the implemented cyber attacks. Such sets of chromosomes (pairs of vertices of the graph modeling system) will allow both to increase the system resilience to cyber attacks and to reveal the subgraphs of the graph resilient to the different types of cyber attacks. This will be the starting point for solving the fundamental and practical task of synthesizing the structure of systems resilient to cyber attacks.

    d.　If possible, obtain solutions to Equations (3)–(5), because, for a cyber–physical system under the influence of cyber attacks, the approximate limits of its resilience will be determined as well as the margin of survivability, depending on the type of destructive action realized at

the moment. This is necessary to ensure a rapid response from cybersecurity specialists to keep the system running.

5. Estimate resilience to cyber attack of the considered system using Equations (6) and (7). This step allows determining the limitations of the evolution process in the considered system.

A system of indicators was proposed to assess the safety of the SRCPS under the proposed evolutionary approach:

1. Cyber resilience SRCPS indicator. Let us denote it as LF. It is calculated as the ratio of the number of "survivor" pairs of the interconnected system components to the destructive impact of cyber attacks—i.e., to the number of disabling components. Analyzing this indicator allows to develop approaches to optimize the design of complex intelligent systems and solve the problem of automating the design of cyber-resilient intelligent systems.
2. The indicator of danger of destructive information impact is denoted as DGR. It is calculated as the ratio of change in the number of routes of target function implementation to the damage from cyber attacks. The optimal value of this indicator will be achieved at such a ratio of components, at which the number of possible routes of the target function implementation will be the maximum.
3. SRCPS vitality reserve indicator. Let us denote it as DS. It is calculated as the ratio of the component distribution by types to the number of possible routes of target function implementation.

7. Experimental Studies on Cybersecurity Using Evolutionary Models

To assess the effectiveness of the proposed approach, a series of experiments related to the already functioning cyber–physical system was conducted. The importance of such an evaluation is connected with the fact that, for the first time, the application of evolutionary models and equations will allow to estimate for an already designed and operating system its reserve of resistance to attacks and the characteristics of its recovery (namely, the ability of a system to recover, depending on the intensity of the cyber attack). It is also important to determine the space of possible states for a given system and to analyze how to increase the system's self-regulation abilities.

The proposed approach was applied to a Smart Grid power control subsystem (Figure 2).
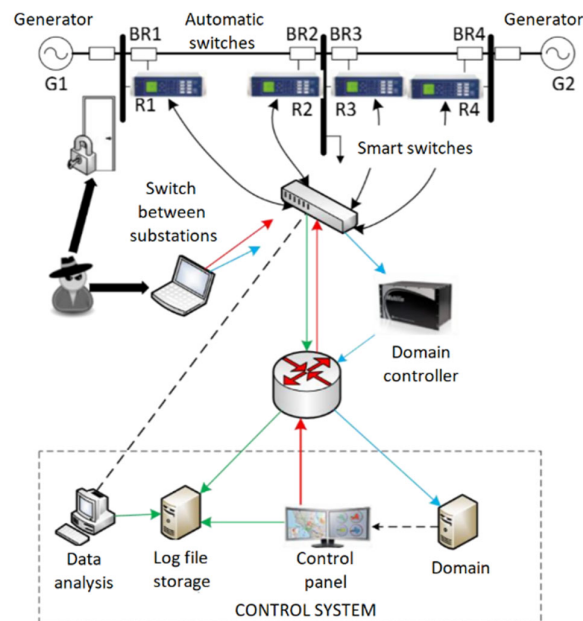

Figure 2. Power control subsystem scheme.

The target function expresses the process as a sequential activation of the nodes. Taken together, the system components perform the following functions: receiving data from the switches, aggregation of switch data, data preprocessing, comparing the results with the indicators in the database, updating the data in the database, making decisions about regulating the network parameters, and sending control commands.

The experimental CPS can be represented as a graph. The possible examples of attacks and recovery actions on such systems are:

- node deleting, recovery actions—add one node;
- edge deleting (with edge we delete those nodes for which this edge is the only one), recovery actions—add one edge and number of deleted nodes.

To estimate the speed of the system recovery at a different intensity of the attacking action, an approximate solution of Equation (2) was used; the results are presented in Figure 3. Different ratios between recovery speed and attack intensity are considered. The intensity of attack/recovery means that we delete/add different number of node/edges. This number was chosen randomly according to a Poisson distribution, with a given parameter, which can be considered the intensity of the attack/recovery.
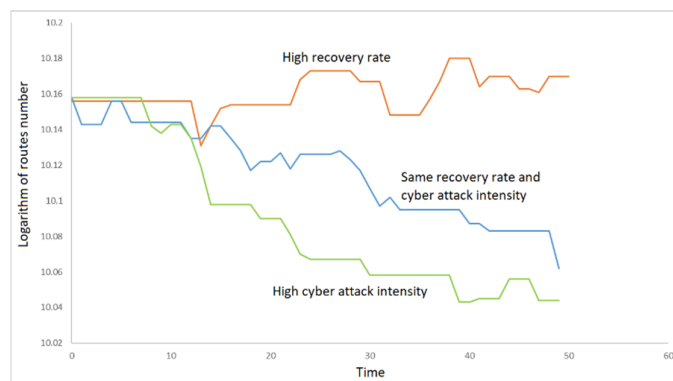

Figure 3. Ratios of recovery rate to attack intensity.

Data for Figure 3 were collected experimentally. The sequence of different cyber attacks on the system was simulated and this was reflected in the graph that simulates the system. After each attack, the number of remaining routes with which the target function can be implemented was automatically estimated. These parameters were used for Figure 3.

Figure 3 shows that the positive direction of evolution for the considered system is possible only in case of the self-regulation rate significantly exceeding the intensity of the attacking action.

After application of the mathematical models presented in Section 5, the space of acceptable system states was obtained (Figure 4). The landscape presented in Figure 4 allows to select the most effective system states where the number of possible routes is large. The spikes reflect such numerical relations between the parameters, at which the system will have the largest number of possible routes of target function implementation.
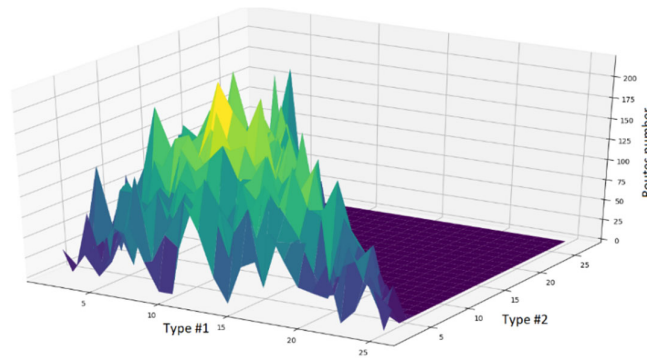
Figure 4. Space of possible states.

After a number of destructive actions were made on the system, some other types of devices were activated.

Destructive effects were simulated cyber attacks, which consisted of removing one or more vertices from the column. Given the design of modern CPSs, for a number of components, the developers have included similar components for the reserve. In the event of a failure of such components, the redundant components are activated, and the CPS can continue to function. When simulating attacks, we used this, and periodically created a new vertex for some remote vertices, similar to the one in terms of functions performed.

This has significantly changed the space of acceptable states of the system, which can be seen in Figure 5. The peaks shifted noticeably closer to the center; therefore, the state in which the system has the largest stock of routes for reconfiguration is no longer the same as it was before the attacks on the system.
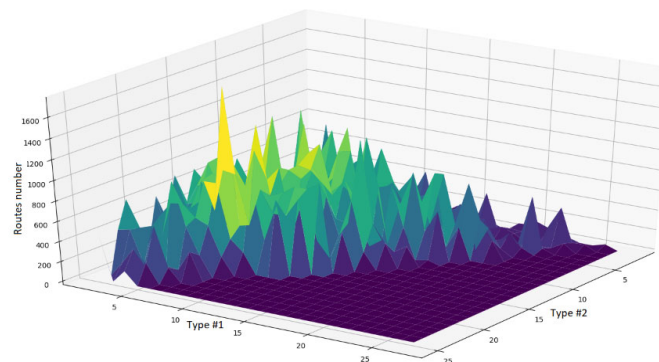

Figure 5. Space of possible states after the cyber attacks.

To identify the most attack-resistant pairs of nodes in the system under consideration, two types of cyber attacks were simulated: an attack leading to the removal of an edge from a graph and an attack leading to a strong removal of an edge from a graph.

From the point of view of graph theory, these two operations are different in that in the first case only the edge is removed from the graph; the incident vertices remain. In the second case, the edge and all its incident vertices are removed.

An edge removal attack corresponds to a practical cyberattack aimed at changing the operating rules or system settings, which results in a ban on communication between some components of the system. For example, in a real system, such as the energy system discussed in this article, this attack can result in a house not being alerted to power problems and the house not being supplied with energy.

A strong edge removal attack is similar to a previous attack, but its consequences are greater. It aims to change the rules of operation or the system settings, thus prohibiting the exchange of data in a group of devices, and then disabling this group of devices. A real-life example of such an attack

would isolate a whole complex of residential buildings (or industrial facilities) from the power supply network, and as a result, they would no longer function due to power shortages.

In the first case (Figure 6), a random edge is removed from the graph, and it does not matter if a pair of nodes connected by it is used in the target function implementation route.

In the second case, a targeted cyber attack was simulated, which is reflected in the graph as a strong edge removal (Figure 7).

The peaks in Figures 6 and 7 correspond to pairs of interconnected nodes, most often used in the graph that simulates the system. It can be concluded from the drawing that the system experiences a degradation at the sharp color change and a change of peak in the plane, while the flat and gentle areas of the surface characterize the acquisition of a stability reserve by the system.
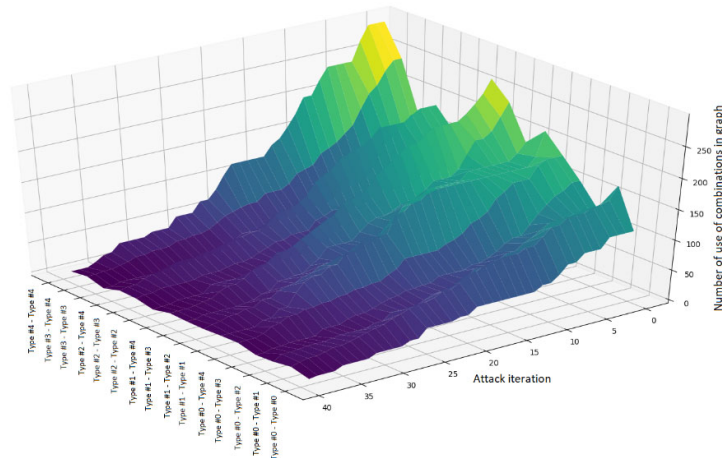

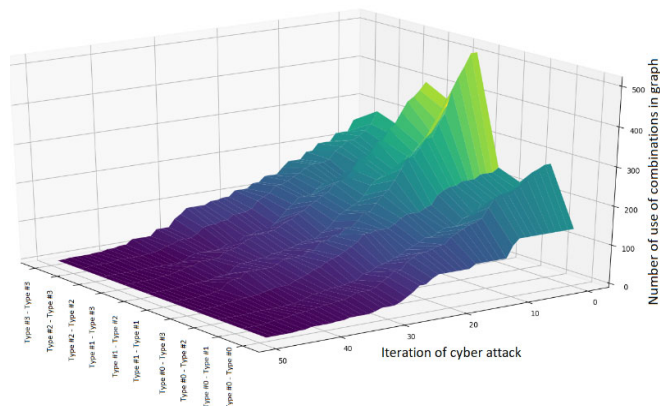**Figure 6.** Non-targeted attack by removing edges.

Figure 7. Targeted attack by strongly removing edges.

The following conclusion can be drawn from Figures 6 and 7: combinations whose number of uses is high are decreasing faster and more sharply than combinations whose initial number of uses is smaller. This suggests the need for "species diversity"—in relation to the system structure, the differences in types of relationships between nodes. In order to form a network infrastructure resistant to cybernetic impacts, it is necessary to diversify the types of connections used in the system as much as possible.

The following trend can also be highlighted: at about the 20th iteration of the attack, the number of node pairs is compared for all types of pairs—regardless of how often they were encountered in the system or used in the route of the target function implementation.

8. Discussion

This paper is aimed at academic researchers and technicians involved in the design and development of cyber–physical systems, in particular the deployment of their network infrastructure.

The purpose of this article is not only to provide an increased level of security for modern cyber–physical systems, but also to determine which cyberthreats the different architectures of cyber–physical systems are exposed to and which cyberthreats they are resistant to; how long these systems are able to maintain their correct functioning under conditions of destructive impact; what the architecture of the cyber–physical systems should be in order to achieve the greatest resistance to attacks; and what types of components of the system should be duplicated by a large number of people.

The application of evolutionary models to cyber–physical systems is therefore of great importance for cybersecurity in general, and it also makes it possible to assess the future resilience of cyber–physical systems to attacks. The evolutionary approach is much broader and more extensive than its individual areas of application to private tasks for optimizing and securing complex technical systems (similar to the studies presented in Section 3).

The advantages of the proposed evolutionary approach in cyber–physical environments are as follows:

1. CPS has a pronounced target function—a set of processes characterized by parameters whose values lie within a certain range during normal system operation. Undoubtedly, there are other environments that have been affected by digitalization. For example, distributed banking systems and mass service systems. However, their target function is not so pronounced due to the great influence of humans on all processes performed by such systems. As a result, it is much more difficult to model and control the functioning of such systems.
2. The abovementioned influence of a human on the system in the CPS has been minimized. First of all, this applies to a CPS of the industrial sector. In Germany, for example, there is a trend towards full automation and the exclusion of humans from the production process (Siemens plant). This makes the work of the CPS much more predictable and permanent.
3. Many systems that are being digitized have an established architecture. In turn, for a CPS, the final architecture has not yet been formed, and to a large extent this is due to the need to work independently from humans.

That is why, in the opinion of the authors, application of the evolutionary approach is more suitable for a CPS. These systems are actively developing and their behavior is more deterministic by minimizing human influence.

In addition, various CPSs have different network infrastructures—distributed and centralized, including powerful computing servers and based predominantly on sensors and controllers. Therefore, different types of CPSs will require different methods to implement the proposed approach. For example, for distributed sensor networks, it will be necessary to introduce more powerful devices that will start the self-regulation process. Decision to replace a component in a system must be based on messages from multiple devices. This is a significant difference from client–server CPS infrastructure, where the decision is made by a centralized control component with greater computing power.

In addition to theoretical research, the practical testing of the proposed approach, implemented through simulation modeling, was of great importance. The conducted experiments demonstrate the expediency and effectiveness of the proposed approach, as the results of the experiments are the same as other experts' opinion and do not contradict the existing theoretical models.

The approach developed in this article allows:

A. Estimate the frequency of self-regulation and correlate it with the intensity of attacks to determine the conditions of a system's positive evolution. The positive evolution of the system will mean that its ability to resist cyber attacks will not decrease, and in some cases will even increase.

B. Identify the components and links of the system that remain in the process of self-regulation, i.e., have adaptability to the attacks under test. These links (or subgraphs of the graph modeling system) can then be used to synthesize an attack-resistant structure (at least for a specific type of attack).

C. Suggest reasonable types of indicators of the system cybersecurity assessment, i.e., preservation of operability under attack conditions and efficiency of the system architecture in the form of a measure of many possible states, which will determine the potential margin of the system's survivability under various types of attacks.

D. In addition, it is possible to solve a number of practical issues:

(1) Comparison of various self-regulation algorithms;
(2) Determining resistance to a particular type or set of attacks;
(3) Selecting a model of attacks for which the system has a certain resistance or cannot resist;
(4) Estimate the amount of system damage during different types of attacks.

The direction of further development of the proposed approach is to automate the estimation of the correspondence between the attack types and the types of changes in the CPS. This method allows providing prevention of attacks or mitigation of their impacts.

It should be noted that the results obtained are important in terms of integrating evolutionary models with artificial intelligence methods. Taken together, they will open up great opportunities to develop complex technical systems and provide them with the ability to independently generate a set of reaction templates for various types of cyber attacks. In the future, these systems will be able to acquire the ability to learn by themselves, like living organisms, automatically and at an early stage by determining the optimal reaction scenario for an attack.

Accumulation of data of such correspondences can be used as training data for machine learning methods, which can help to protect against a certain type of attack, i.e., acquiring immunity from exposure to certain links.

The proposed approach is considered in terms of cyber–physical systems for two reasons. The first reason is the digitalization of technological infrastructure around the world, which has led to the emergence of, and increase in, cyber–physical systems. Cyber–physical systems are being integrated with various important areas of activity: industry, medicine, energy, and transport. The impact of successfully implemented cyber attacks on these industries can be disastrous and may cause irreparable damage to the environment and to human life and health. Ensuring the security of cyber–physical systems and designing them to withstand attacks is therefore one of the top technical priorities in the area of cybersecurity.

The second reason is that for most cyber-physical systems, it is sufficient to simply define the target function by identifying a set of processes that the system must implement and analyzing the characteristics of these processes. The model and assessments developed on the basis of evolutionary theory will be much more effective for such systems than for more global systems that do not have a clear target function.

Author Contributions: Conceptualization, D.Z. and D.L.; methodology, D.Z.; software, A.S.; validation, E.P., A.S. and D.L.; formal analysis, E.P.; investigation, D.L.; resources, D.Z.; data curation, A.S.; writing—original draft preparation, A.S.; writing—review and editing, E.P.; visualization, A.S.; supervision, E.P.; project administration, D.L.; funding acquisition, D.Z. All authors have read and agreed to the published version of the manuscript.

References

1. Zegzhda, D.P.; Pavlenko, E.Y. Digital Manufacturing Security Indicators. *Autom. Control Comput. Sci.* **2018**, *52*, 1150–1159, doi:10.3103/S0146411618080333.

2. Sadiku, N. Cyber-physical systems: A literature review. *Eur. Sci. J.* **2017**, *13*, 52–58, doi:10.19044/ESJ.2017.V13N36P52.

3. Henshaw, M. Systems of systems, cyber-physical systems, the Internet-of-things. What next? *Insight J.* **2016**, *19*, 51–54, doi:10.1002/inst.12109.

4. Lavrova, D.S. Maintaining Cyber Sustainability in Industrial Systems Based on the Concept of Molecular-Genetic Control Systems. *Autom. Control Comput. Sci.* **2019**, *53*, 1026–1028, doi:10.3103/S0146411619080145.

5. Perales Gómez, Á.L.; Fernández Maimó, L.; Huertas Celdrán, A.; García Clemente, F.J. MADICS: A Methodology for Anomaly Detection in Industrial Control Systems. *Symmetry* **2020**, *12*, 1583, doi:10.3390/sym12101583.

6. Urmantsev, Y.A. The Symmetry of Nature and the Nature of Symmetry; Moscow Muisl. 1974. Available online: http://sci.su/OTS_Simmetry.pdf (accessed on 20 November 2020).

7. Kumar, P.; Sharma, A. Data security using genetic algorithm in wireless body area network. *Int. J. Adv. Stud. Sci. Res.* **2018**, *3*, 118-122.

8. Magliani, F.; Sani, L.; Cagnoni, S.; Prati, A. Genetic Algorithms for the Optimization of Diffusion Parameters in Content-Based Image Retrieval. In Proceedings of the 13th International Conference on Distributed Smart Cameras, Trento, Italy, 9–11 September 2019; pp. 1–6, doi:10.1145/3349801.3349815.

9. Saviano, M.; Bassano, C.; Piciocchi, P.; Di Nauta, P.; Lettieri, M. Monitoring viability and sustainability in healthcare organizations. *Sustainability* **2018**, *10*, 3548, doi:10.3390/su10103548.

10. Alqurashi, E.; Wills, G.; Gilbert, L. A viable system model for information security governance: Establishing a baseline of the current information security operations system. In Proceedings of the IFIP International Information Security Conference, Auckland, New Zealand, 8–10 July 2013; pp. 245–256, doi:10.1007/978-3-642-39218-4_19.

11. Cho, T.H. Simulation Methodology-Based Context-Aware Architecture Design for Behavior Monitoring of Systems. *Symmetry* **2020**, *12*, 1568, doi:10.3390/sym12091568.

12. Maratha, B.P.; Sheltami, T.R.; Salah, K. Performance study of MANET routing protocols in VANET. *Arab. J. Sci. Eng.* **2017**, *42*, 3115–3126, doi:10.1007/s13369-016-2377-y.

13. Sagar, S.; Javaid, N.; Khan, Z.A.; Saqib, J.; Bibi, A.; Bouk, S.H. Analysis and modeling experiment performance parameters of routing protocols in MANETs and VANETs. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 1867–1871, doi:10.1109/TrustCom.2012.89.

14. Abbasi, A.; Hossain, L.; Wigand, R.T. Evolutionary Dynamics of Complex Networks: Theory, Methods and Applications. *arXiv* **2015**, arXiv:1503.06652. Available online: https://arxiv.org/ftp/arxiv/papers/1503/1503.06652.pdf (accessed on 20 November 2020).

15. Nayeem, M.A.; Islam, M.M.; Yao, X. Solving Transit Network Design Problem Using Many-Objective Evolutionary Approach. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 3952–3963, doi:10.1109/TITS.2018.2883511.

16. Konak, A.; Smith, A.E. Capacitated network design considering survivability: An evolutionary approach. *Eng. Optim.* **2004**, *36*, 189–205, doi:10.1080/03052150310001633223.

17. Anokhin, P.K. Philosophical aspects of the theory of a functional system. *Sov. Stud. Philos.* **1971**, *10*, 269–276.

18. Anokhin, P.K. Systemogenesis as a general regulator of brain development. *Prog. Brain Res.* **1964**, *9*, 54–86.

19. Turchin, V.F. A meta-algorithmic language. *Cybernetics* **1968**, *4*, 40–47.

20. Burtsev, M.S.; Turchin, P.V. Evolution of cooperative strategies from first principles. *Nature* **2006**, *440*, 1041–1044.

21. Redko, V.G. *Evolutionary Cybernetics*; Nauka: Moscow, Russia, 2001.

22. Suarez-Tangil, G.; Tapiador, J.E.; Peris-Lopez, P.; Ribagorda, A. Evolution, detection and analysis of malware for smart devices. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 961–987.

23. Stephenson, B.; Sikdar, B. A quasi-species model for the propagation and containment of polymorphic worms. *IEEE Trans. Comput.* **2009**, *58*, 1289–1296, doi:10.1109/TC.2009.63.

24. del Rey, A.M. Mathematical modeling of the propagation of malware: A review. *Secur. Commun. Netw.* **2015**, *8*, 2561–2579, doi:10.1002/sec.1186.

25. Amro, S.A.; Elizondo, D.A.; Solanas, A.; Martínez-Ballesté, A. *Evolutionary Computation in Computer Security and Forensics: An Overview*; Springer: Berlin/Heidelberg, Germany, 2012; p. 394, doi:10.1007/978-3-642-25237-2_3.
26. Lavrova, D.; Zegzhda, D.; Yarmak, A. Predicting cyber-attacks on industrial systems using the Kalman filter. In Proceedings of the 3rd World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4), London, UK, 30–31 July 2019; pp. 317–321, doi:10.1109/WorldS4.2019.8904038.

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.