УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2022 Том 22 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2022 Vol. 22 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2022 Том 22 Номер 3

doi: 10.17586/2226-1494-2022-22-3-480-491

Application of failure detection methods to detect information attacks on the control system

Alexey A. Margun[1], Radda A. Iureva[2], Daria V. Kolesnikova[3]✉

[1,2,3] ITMO University, Saint Peterburg, 197101, Russian Federation
[1] Institute for Problems in Mechanical Engineering of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation

[1] alexeimargun@gmail.com, https://orcid.org/0000-0002-5333-0594
[2] raddaiureva@itmo.ru, https://orcid.org/0000-0002-8006-0980
[3] Kolesnikova_d@itmo.ru✉, https://orcid.org/0000-0003-0942-3926

Abstract

The problem of ensuring the security of control systems is an important and urgent problem. It consists of eliminating the impact of failures and attacks on control objects and the environment, etc. Prevention of critical failures is important. The purpose of this study is to analyze the similarities between the consequences of attacks on complex technical systems and failures of these systems. In the course of the work, a hypothesis about the similarity of the impact of failures and information attacks on a complex technical system is presented. Both information attacks and failures cause anomalous dynamics of the control object. Analysis of the deviation of the dynamics of the control object from the normal mode of operation will allow us to detect and isolate information attacks and failures. The paper examines the influence of information attacks on the dynamics of automatic control systems. Comparison of abnormal dynamics of control objects during attacks and device failures is carried out. The similarity of the consequences of information attacks and failures of the control system are analyzed, a method for identifying attacks based on the methods developed for detecting failures is developed. Computer modeling of the influence of information attacks and failures on the control system of a DC motor has been carried out. The simulation results allow making a conclusion about the applicability of the failure detection algorithms for detecting attacks. It is shown that failures and information attacks can lead to dangerous consequences for the control system. It seems relevant to study the intersection of the field of information security and failure detection.

Keywords

failure detection, failure isolation, reliability, dangerous failure, functional safety, fault tolerance, attack

For citation: Margun A.A., Iureva R.A., Kolesnikova D.V. Application of failure detection methods to detect information attacks on the control system. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 3, pp. 480–491. doi: 10.17586/2226-1494-2022-22-3-480-491

УДК 004.052

Применение методов детектирования отказов для обнаружения информационных атак на систему управления

Алексей Анатольевич Маргун[1], Радда Алексеевна Юрьева[2], Дарья Викторовна Колесникова[3]✉

[1,2,3] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[1] Институт проблем машиноведения РАН, Санкт-Петербург, 199178, Российская Федерация

[1] alexeimargun@gmail.com, https://orcid.org/0000-0002-5333-0594
[2] raddaiureva@itmo.ru, https://orcid.org/0000-0002-8006-0980
[3] Kolesnikova_d@itmo.ru✉, https://orcid.org/0000-0003-0942-3926

Аннотация

Обеспечение безопасности систем управления – важная и актуальная проблема. Она состоит в исключении влияния отказов и атак на объекты управления, окружающую среду и др. Большое значение имеет предотвращение критических отказов. Выполнен анализ сходств последствий атак на сложные технические системы и отказов этих систем. Рассмотрено влияние информационных атак на динамику систем автоматического управления. В ходе работы представлена гипотеза о сходстве влияния отказов и информационных атак на сложную техническую систему. Как информационные атаки, так и отказы вызывают отклонения динамики объекта управления. Анализ отклонения динамики объекта управления от нормального режима функционирования позволит детектировать и изолировать информационные атаки и отказы. Проведено сравнение аномальной динамики объектов управления при атаках и отказах устройств, обнаружены зависимости, и сделаны выводы. Проанализировано сходство последствий информационных атак и отказов системы управления, разработана методика идентификации атак на основе методов, разработанных для детектирования отказов. Выполнено компьютерное моделирование влияния информационных атак и отказов на систему управления двигателем постоянного тока, приведены результаты в виде графиков. Результаты моделирования позволяют сделать вывод о применимости алгоритмов детектирования отказов для обнаружения атак. Показано, что отказы и информационные атаки могут привести к опасным последствиям для системы управления. Актуальным представляется исследование пересечения области информационной безопасности и детектирования отказов.

Ключевые слова
детектирование отказов, изоляция отказов, надежность, опасный отказ, функциональная безопасность, отказоустойчивость, кибератака

Ссылка для цитирования: Маргун А.А., Юрьева Р.А., Колесникова Д.В. Применение методов детектирования отказов для обнаружения информационных атак на систему управления // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 3. С. 480–491 (на англ. яз.). doi: 10.17586/2226-1494-2022-22-3-480-491

Introduction

Information systems protection is becoming urgent and requires increased attention in connection with the development and use of global computing systems and networks, information complexes, and remote-control systems.

However, the pace of research in fault-tolerant functioning and cyber-physical systems security significantly lags far behind the field of development of information technologies. Today, the functioning of technical systems leads to an increase in the volume of processed information which reduces their work reliability. As a result, to ensure systems fault-tolerant functioning, there are not enough tools and methods. Consequently, the risk of various vulnerabilities and information threats, faults, and attacks increases.

Technical systems should improve the following properties: adaptability, fault tolerance, security, and simplicity of use.

Prime examples of modern technical systems are the Internet of Things, multi-agent digital production systems, unmanned vehicles, and intelligent robotic systems. The structure and function logic of such systems are significantly different from classical information systems. Therefore, the existing methodologies for ensuring security and fault-tolerant functioning for complex systems are not sufficiently effective.

The relevance of solving the problem of ensuring the secure and fault-tolerant functioning of technical systems is caused by the importance of improving their correct operation, especially in critical infrastructure. Thus, victims may be commercial organizations that have received financial damage with a successful attack or fault and the population and the environment of the entire state. In this regard, it is necessary to consider both cybersecurity and the quality of all pro-cases.

This paper aims to analyze the combination of techniques for ensuring information and operational security of technical systems.

Even at the early development of technical systems, researchers noted a similarity in the description of security technologies evolution and control theory systems evolution. The focus of both approaches is on keeping the system within a certain set of states. In this regard, managing the security of complex systems capable of changing their state and self-regulation has gained great importance.

The problem of ensuring the safety of the functioning of control systems is to exclude the influence of failures and attacks on control objects and the environment, i.e., in the elimination of critical failures. This study aims to analyze the similarities between the consequences of attacks on complex technical systems and failures of these systems.

Information and functional security

Attack and fault concept

Information security is a set of protecting information means from accidental or intentional impact. Regardless of what is the basis of the impact: natural factors or artificial reasons, information owner incurs losses.

The key areas for assessing the damage and impact of threats and attacks on information security are:

- Enterprise operation (can slow down processes and operations work, it is typical not only for commercial, but also for government organizations).
- Decrease in profits and other funds (company part in the market, revenue, and margin).
- Deterioration in product quality or developed service.
- Negative impact on the company's image (change in the market position, among sponsors), impact on the company's goal, business project.

A fault is an event that means complete or partial disruption of the object, element, or system performance.

Faults are classified and characterized by different types and parameters. For example, it can be categorized by type: parametric or functional. In the first case, object parameters change within unacceptable limits. In the second case, there is complete or partial functions termination.

Also, fault can be distinguished by nature: random and systemic. Accidental faults occur in unforeseen situations (defects, failures, personnel errors, breakdowns in the control system). Systemic failures occur in the cases of natural and unavoidable facts, for example, with erroneous commands or secondary failures.

Reliability is the property of an object to continuously perform specified functions for the required time in given modes and operating conditions.

Fault tolerance is the system's ability to maintain its properties and perform specified functions even in the event of individual components fault or faults at system modules levels.

It should be noted that the behavior of the system may be similar during an attack or fault. This allows concluding that the methods used to detect, identify, isolate, and adaptively compensate negative effects can be combined to solve a complex problem in a destructive environment. The developed algorithms and approaches can provide the accurate determination of destructive impact type and investigate the high level of system security, reduce the number of vulnerabilities, and maintain the quality of technical systems functioning throughout the operation phase.

Maintaining stable functioning and ensuring information security comes to the fore during the attack for dynamic protection. The solution of this problem may consider technical systems ability to change their structure to counter destructive impacts.

The scientific problem relevance depends on the growing need for modern methods of technical system intelligent control which can ensure the implementation of the high demands placed on them in the work process. Such requirements are related to security, reliability, and fault tolerance in case of destructive impact.

From a safety standpoint, both in the event of a destructive information impact and in case of failure of a system component, its operation should be stopped while maintaining stability, or the performance should be reduced to the prescribed limits if a dangerous failure is inadmissible. To do this, it is necessary to timely detect and isolate information attacks and failures. By isolation we mean the definition of the type of failure and its localization. Hence, there exists the need to create technologies for reliable isolation of information attacks and failures in complex technical systems. In the theory of automatic control, several approaches have been developed that provide detection and isolation of failures based on available measurements and description of the dynamics of control objects. However, no such conceptual schemes, applicable to a wide range of systems, have been proposed for identifying information attacks. In this study, a hypothesis is put forward about the similarity of the influence of failures and attacks on the components of a technical system which in the future will make it possible to develop approaches for detecting and isolating attacks based on the theory of reliability and the scientific and methodological apparatus of the theory of automatic control.

The main triad of information security (IS) is availability, integrity, and confidentiality of the data of the technical system. The property of functional security (FS) is to ensure the correct execution of system functions, and in the event of failures, to transfer the control object to a safe state. The analysis of the properties of IS and FS in the complex (Fig. 1) has become relevant in connection with the development of cyber-physical systems that interact with objects of the real world using global networks and cloud services. These systems can be vulnerable both in the real (physical) world and at the information level, and these levels are inextricably linked in their architecture.

Thus, it is required in modern technical systems to ensure reliability in relation to both information attacks and failures. The solution of this problem can be developing

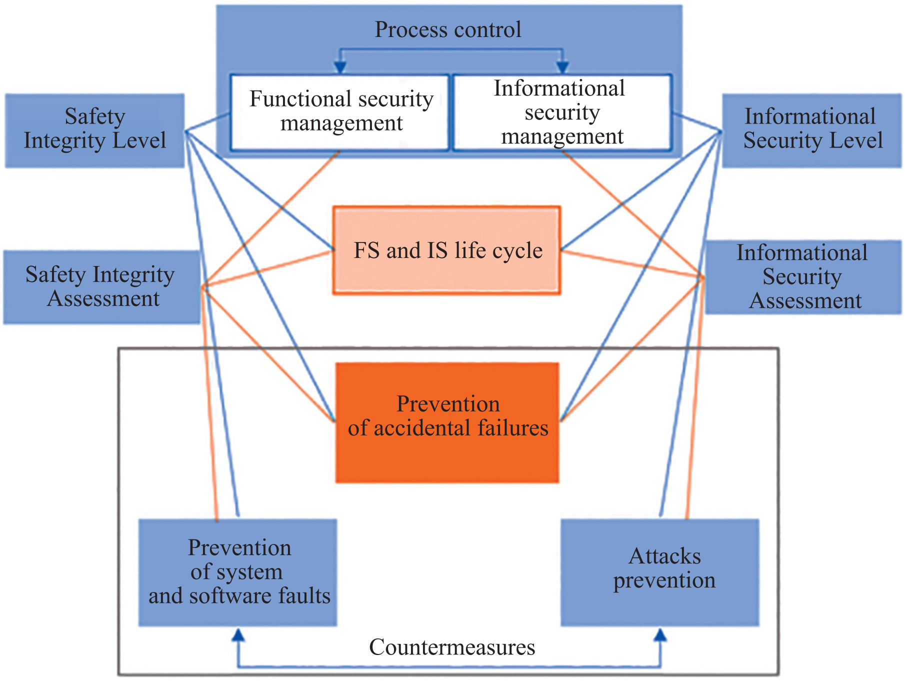
Process control
Functional security management
Informational security management
Safety Integrity Level
Informational Security Level
FS and IS life cycle
Safety Integrity Assessment
Informational Security Assessment
Prevention of accidental failures
Prevention of system and software faults
Attacks prevention
Countermeasures

Fig. 1. The structure of requirements for functional and information security of technical systems a methodology for the simultaneous detection of attacks and failures and their isolation. It is required to determine which failure or attack occurs in the system in order to take the most effective measures to compensate for the negative effects.

Literature review

This section provides an overview of the works that are related to the detection of failures and attacks on control systems (Table 1).

Since both failures and information attacks can lead to dangerous consequences for the control system, it is relevant to study the intersection of the information security area and failure detection. The research is based on the hypothesis about the similarity of failures and information attacks on a complex technical system. Both information attacks and failures cause anomalous dynamics of the control object. Analysis of the deviation of the control object dynamics from the normal mode of operation makes it possible to detect and isolate information attacks and failures.

Table 1. Comparison of attacks from the point of view of theory of automated control and IS

Reference	Review
[1, 2]	The emergence of complex systems class was facilitated by the need of processes qualitative reorganization in many areas, implying the intellectual automation of complex operations using robotic systems. Increased attention to technical systems is associated with the concept of Industry 4.0 representing the fourth industrial revolution which involves the deep integration of advanced information technologies in physical processes. Modern technical systems and technological facilities are equipped with increasingly sophisticated control tools that enable them to maintain normal operation and increase process efficiency while meeting safety requirements. Complexity of synthesizing algorithms for coordinated interaction of components increases with higher complexity of systems. Thus, malfunctions and vulnerabilities that can lead to faults, attacks, casualties, and accidents increases. There are special algorithms based on model adaptive approaches, fault-tolerance control methods; and software and/or hardware redundancy to solve system control problems. These solutions are highly specialized for individual systems, are not scalable and do not allow integration at different levels of management (low — operational, medium — tactical, high — strategic).
[3]	The ability to provide desired performance of technical systems both in the absence and in the presence of faults is an important task in many control systems. One of the techniques for monitoring system performance is Fault detection, isolation, and re-configuration (FDIR). In the paper various FDIR methods are considered classified based on reliable fault detection methods, statistical decision-making methods, and reconfiguration management methods.
	Technical systems in practice are distorted due to the presence of noise, unknown disturbances, and uncertainties in the system model. Consequently, many methods for determining faults are aimed to create stable residual that can be insensitive to noise and uncertainties, but sensitive to faults and attacks. Such methods can be grouped into several basic approaches:
[4, 5]	1) full-state observer-based methods;
[6–8]	2) unknown input observers;
[9–11]	3) parity relations approach;
[12]	4) optimization-based approach;
[13–15]	5) Kalman filter-based approach;
[16]	6) stochastic approach;
[17]	7) system identification approach;
[18, 19]	8) nonlinear systems approach;
[20, 21]	9) discrete event systems/hybrid systems approach;
[22, 23]	10) artificial intelligence techniques.
[24]	In the article, detailed review of existing methods for troubleshooting and fault-tolerant operation is presented.
[25–28]	The principles of fault-tolerance control can be based on a re-configuration of the system, adaptive methods of fail-safe control of nonlinear systems and active methods of fail-safe control.
[29]	The first studies on attacks identification in technical systems date back to the early 2000s. The article provides an overview of the current state of the industry.
[30]	The attacks have complex and multi-level schemes, they are multi-step and extended over time, and can also consider individual characteristics of the technical system. Most defense systems oriented on physical- and cybersecurity operate independently of each other.
[31]	Existing information security methodologies do not consider specifics of technical systems and are not able to ensure the functioning of such systems under conditions of destructive influences.
[32, 33]	Attacks can affect system physical state, they can be scalable, easily automated and replicated. Attacks affect: confidentiality (maintaining the security of users' data in systems); integrity (modification of data or resources without permission); availability (failures in computer technology, equipment, management, etc.); reliability (user authentication in the system).

Table 1. Continuation

Reference	Review
[34, 35]	Basically, when attacking complex technical systems, attackers use the so-called APT attacks (complex targeted attacks, advanced persistent threat attack) consisting of several stages and include attacks of a lower level of complexity. In general, such attacks can be divided into levels and these levels can be classified according to the method presented in the given articles: Social engineering to obtain confidential information or distribute malicious software, and one of the main goals is to reduce the level of trust in the system and "damage" the reputation. Phishing attacks are used to gain access to information channels. Hacking, as one of the first steps to attack the system. When using hacking, an attacker looks for vulnerabilities in software and hardware, uses errors in protection mechanisms or other shortcomings of the system under attack (attacks through third-party channels). Interception of data circulating in the system (Man-in-the-Middle, injection). Selection of credentials to obtain passwords and access to all resources of the victim. Exploitation of web vulnerabilities, theft of information from web resources. DDoS attacks that can lead to the execution of arbitrary code, unauthorized control of industrial equipment and failure of its operation. At the same time, most vulnerabilities can be exploited remotely without authentication, and their exploitation does not require special knowledge and a high level of skills from the attacker. Use of malicious software to collect data from computers inside the system. It is this method that is used in most complex targeted attacks for integration into the target system. In general, from the point of view of technical systems, the most dangerous attacks are Advanced Persistent Threats (APT) attacks, Man-in-the-Middle attacks, channel attacks, and injection.
[36]	Article provides assessment of the possible impact on electric network and its ability to withstand potential faults after attack. It emphasizes the importance of cyberinfrastructure security combined with applications security to mitigate and prevent cyberattacks. A multi-level approach to risk assessment is introduced.
[37]	Review explores heterogeneous data streams from autonomous technical systems. Aspects of security and confidentiality in the management of big data for such systems are considered as well as the latest problems in the data field confidentiality are considered.
[38, 39]	The successful implementation of attacks on complex systems is closely integrated with various industries. It can lead not only to financial damages but also to human casualties because of technological and environmental disasters. At the same time, the number of attacks on industrial facilities is steadily growing. These reasons and criticality of systems operation disruption demonstrates the relevance of the research.
[40]	There are several approaches for fault detection: parity relationships, observer based and identification methods. Parity relationship approaches are based on hardware or temporal redundancy. Hardware redundancy solutions require duplication of sensors and actuators. This leads to additional technological and financial costs. The approach based on time redundancy proposes to analyze not the current mismatch of the sensor data with the expected ones, but with the mismatches at the preceding current moment certain time interval.
[41]	Observer-based approaches propose to analyze the residual signal. The residual signal is a mismatch between sensor data and it estimates the plant state variables obtained by observers. The problem of fault isolation is solved based on structured residual sets, directional residual vectors and special residual signal generators or filters that sensitive only for special residual signals corresponding to respective faults. Observer-based methods are effective for sensor and actuator faults detection.
[42]	Identification-based approaches are used for component fault detection and isolation where a component fault is a deviation of physical parameters from their nominal value.
[43]	Authors propose two fail-safe methods for calculating reconciliation sensors for installations with increased sensitivity, as well as two methodologies for designing a failure detection system. The first is based on a formulation with a linear parameter change, and the second is based on the linear fractional transformation paradigm.
[44]	Various approaches are used to detect information attacks – an overview of control systems attacks presents four types of attacks (response and measurement injection, command injection and denial of service) and analyzes the consequences of these attacks on the nodes of the control system.
[45]	The paper presents an analysis of vulnerabilities and detection of attacks which was carried out on programmable logic controllers (PLCs), as one of the most important components, on the test bench, and a set of rules was created to detect active start/stop attacks. The analysis used a mirroring method to prevent the detection system from placing additional stress on the existing system and adversely affecting system performance.
[46]	Authors have proposed an algorithm for detecting and preventing DDoS attacks based on network changes and it is used to overcome the problem of DDoS attacks and protect routing tasks. Through various transactions, a fault can be identified in each sensor node. The DDoS attack identifier is decoupled from network failures based on the error value.
[47]	In this work, a mathematical basis for monitoring attacks on cyber-physical systems is proposed, and a description of the fundamental limitations of monitoring from a system-theoretical point of view and a graph theory point of view.
[48]	In the paper the authors proposed methods and measures to counter cybersecurity threats in various approaches to the system design.

Classification of attacks and failures

By cybersecurity, we mean ensuring information and functional security of a cyber-physical system's functioning — a technical system that includes a physical component and a virtual one (algorithms, calculations, channel data transmission medium). The main threats to cybersecurity breaches in complex technical systems are (Fig. 2):

- information attacks;
- failures in the operation of system nodes, including hardware and software failures and errors.

Considering various classification signs of failures and attacks according to their influence on the dynamics of the control system from the nature point of view of changes in the parameters that determine the technical state of the object, it is possible to distinguish abrupt or gradual deviations. An abrupt change in parameters can be caused by a critical defect that changes the system's structure (for example, a breakdown of a mechanical part or a failure of a power source) or an information attack (for example, an attacker substitutes the values measured by sensors). A gradual change in parameters is typical for equipment deterioration and change in its parameters due to operating conditions. An example would be the change in resistance of a heating element due to thermal expansion, which affects heating. Similar features can be used to isolate failures and attacks.

From the point of view of the interrelation of destructive processes, they can be independent (only one element of the system works incorrectly, which does not disable others) and dependent (the failure of one element entails several others' failure and the system as a whole). From the functional safety point of view, the latter case is the most critical.

The reasons for equipment failures can be classified as structural, production, and operational (Table 2). According to this classification, compliance with the attribute will not be essential for the dynamics of the system which reduces its value for the task set in the study.

An idle state can persist for a long time, be short-term, or occur periodically under similar conditions. The first case is typical for both attacks and failures. If after taking measures to prevent the attack, the inoperable state persists, then its reason is the failure, and vice versa. The second case is more typical for information attacks, the third — for technical failures caused by a certain mode of operation of the control object.

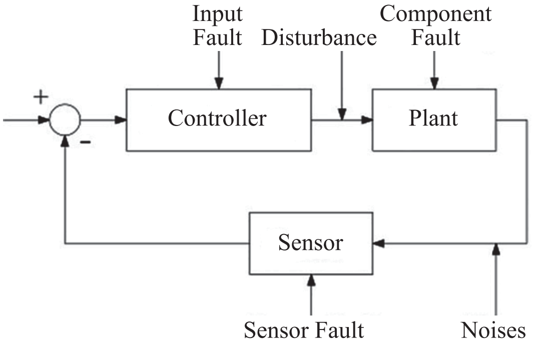

Fig. 2. Typical structure of an automatic control system and possible destructive factors

For the reliable functioning of control systems, it is necessary to ensure continuous monitoring of its state, a method for detecting failures and attacks, and also a set of measures to compensate and prevent their influence. This approach will provide a guaranteed level of cyber security in case of hardware and software failures and destructive influences by integrating the scientific and methodological apparatus for identifying and isolating failures for similar tasks when attacking complex technical systems.

Analysis of the impact of attacks and failures on the dynamics of control systems

Let us analyze the impact of information attacks on the dynamics of control systems and represent how the anomalous dynamics is interpreted from the fault detection and isolation algorithms perspective (Table 3). Consider an attacker acting on a controller, plant, and sensors as a source of information attacks.

An attacker can remotely penetrate a controller (a device that calculates control signals and implements control laws). In this case, he can restart the controller or stop its work. During the restart, the controller values are reset (for example, the outputs of the control law's integrators are reset to zero), and the controller will be stopped for a while (initialization). When the controller is stopped, the control signal becomes a constant (including zero). From the theory of automatic control point of view, plant dynamics looks like an input disturbance inverse to the control signal. These destructive effects can be identified by actuator fault detection and isolation methods. The following signs can also detect this type of attack: there are no controller output signals (signal is equal to zero or last value of controller), the control signal becomes constant when the sensors data changes.

In the local controller penetration, the attacker intercepts control, i.e., the control signal becomes independent from the sensor data. An approach similar to the described above can be used to detect this type of attack. Possible signs of controller local penetration include a jump-like change of the control signal; the controller output does not correspond to the value calculated on the base of the input data and signals from the sensors; the dynamics of the plant does not correspond to the controller input signal (tracking or stabilization error).

In the case of a local sensor penetration, an attacker alters its measurements. From the automatic control point of view, it is a noise in the measurement channel. However, the amplitude of the noise can reach the limits of the sensor measurement range. Algorithms of sensor faults detection and isolation can be used to detect this type of attack. The following signs correspond to this attack: a rapid increase of the noise amplitude; an abrupt change of the sensor signal; the signal measured by the sensor does not correspond to the predicted value calculated based on the control signal and the plant model.

The controller stops its operation when a remote denial of service attack is implemented. The same features characterize this attack as remote penetration of the controller.

Table 2. Classification feature and its meaning

Classification feature	Values (nature of change) of the classification feature	Type of failure	Reasons
The nature of the change in the parameters that determine the technical state of the object	Abrupt change in one or more parameters	Sudden	Internal defects, operator errors, operational disturbances, local penetration
	Gradual change in one or more parameters	Gradual	Aging of materials, corrosion, wear of parts, etc.
Interrelation of failures	The failure of an element is not caused by damage or failure of other elements of this object	Independent	—
	Element failure due to damage or failure of other elements	Dependent	Damage and failures of other elements of an object or system
Origin of failure	Violation of established rules and (or) design standards, imperfection of accepted design methods	Structural	Errors in the development and design of an object, underestimation of safety margins, violation of GOST standards, etc.
	Violation of the established process of manufacturing or repairing an object, imperfection of manufacturing technology	Manufacturing	Failure to comply with documentation standards, use of low-quality materials and components, insufficient level of production quality control, etc.
	Violation of the established rules and (or) operating conditions	Operational	Errors of low-qualified service personnel, ignoring / violation of the rules of technical documentation as well as aging and wear of equipment for the above reasons
Stability of an inoperative state	Stable persistent	Stable	Change of object parameters, irreversible damage to system elements
	It remains for a short time, after which the operability is self-healing or restored by the operator without repairs	Self-eliminating (sporadic failure)	Short-term external influences, short-term change in object parameters
	It has the same character, arises and removes itself many times	Intermittent	External interference and impacts that go beyond the permissible technical limits and are reversible

Table 3. Comparison of attacks from the point of view of theory of automated control and IS

Attack	Object	Action	According to fault
Remote penetration	Controller	Remote restart or shutdown	Input disturbance equal to inverse of input signal
Local penetration	Controller	Control Intercept	Input disturbance with amplitude up to input signal range
	Sensor	Data modification	Output noises with amplitude up to sensor measurement range
Remote denial of service	Controller	Full stop	Input disturbance equal to inverse of input signal
	Sensor	Full stop	Output noises with amplitude up to sensor measurement range
Jamming and data spoofing on sensor	Sensor	Jamming or data spoofing	Output noises with amplitude up to sensor measurement range
Decommissioning of component	Component	Destructive effect, manifested in the unstable functioning of the component	Dramatic deviation between measured and predicted dynamics of the plant

In remote denial of service, signals from the sensor are stopped (nothing, zero, or the last sent value comes as a measurement signal). The same approaches and features for local sensor penetration can be applied to detect this type of attack.

During sensor jamming or data substitution, the sensor signal does not correspond to measured physical values. The following signs can accompany this attack: a sharp increase of the noise amplitude; an abrupt change of the sensor signal; the measured output of the plant does not correspond to the predicted one based on the model of the plant. Sensor fault detection and isolation algorithms are effective for the detection of this attack.

In the case of an attack that entails the failure of one of the plant components, its dynamics becomes unpredictable. This attack can be determined by the method of elimination: if all previous faults and attacks are excluded, and the component's dynamics do not correspond to the nominal, then the dynamic model is incorrect. Therefore, one of the components has failed. Also, it is possible to build a set of models with faults. The attack detection can be based on the similarity of the system's behavior and faulty system dynamics.

Modeling attacks on a control system

Consider DC motor. Its dynamics is described by equations:

$$L\frac{dI}{dt} + RI = U - E_b,$$

$$L\frac{dI}{dt} + RI = U - E_b,$$

$$J\dot{\omega} = M - M_{fr},$$

where ω is an angular velocity; I is a current; L is an armature inductance; R is an armature resistance; U is an input voltage; $E_b = k_e\omega$ is a back-EMF; k_e is a constant; $J = J_d + J_m$ inertia momentum; J_d is a rotor inertia momentum; J_m is a load inertia momentum; $M = k_mI$ is a motor force momentum; k_m is a constant; $M_{fr} = k_f\omega$ is a friction momentum; and k_f is a friction coefficient.

Rewrite model under faults in state space representation:

$$\dot{x} = Ax + Bu + f_a,$$

$$y = Cx + f_s,$$

where $x^T = [\omega \quad i]$ is a state vector.

$$A = \begin{bmatrix} -k_f/J & k_m/J \\ -k_e/L & -R/L \end{bmatrix} = \begin{bmatrix} a1 & a2 \\ a3 & a4 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1/L \end{bmatrix},$$

f_a is an impact of attack on the controller, f_s is an impact of attack on the sensor.

Assume that motor equipped with a velocity sensor. Therefore:

$$C = [1 \quad 0].$$

Attack on the executive device

Controller that calculates the supply voltage with an integrated or connected driver is an actuator for a DC motor. Fig. 3 shows the signal of the DC motor angular velocity sensor during attacks on the controller, where ω is a sensor data without attack; ω_{local} is a sensor signal under controller local penetration; and ω_{remote} is a sensor signal under controller remote penetration. Local penetration simulates the case when attacker intercepted control of the motor and applied excess voltage from 5 to 10 seconds. The controller was disconnected from 5 to 10 seconds under remote penetration.

The dynamics of the output in the considered cases is identical to the dynamics in the case of actuator fault. Therefore, abnormal behavior during attacks on the controller can be detected using the state observers-based methods of fault detection. Attack isolation can be implemented using methods of actuator fault isolation, for example, [41].

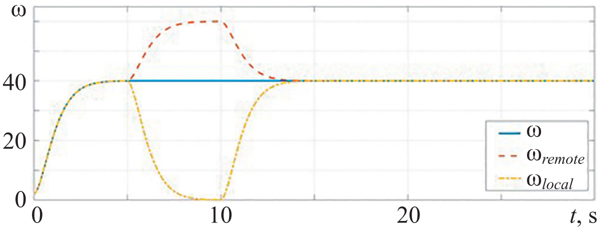

Fig. 3. Readings of the DC motor speed sensor during attacks on the controller

Attack on the sensor

Consider the effect of sensor attacks on motor velocity transients. Fig. 4 shows examples of the angular velocity sensor signal during attacks on it. Graph ω illustrates transients without attacks.

Graph ω_{stuck} illustrates jammed sensor data from 1.6 to 1.5 seconds. A sensor jamming can be caused by local penetration or a remote denial of service. Case of sensor data replacement on $\omega_{replace}$ is presented in Fig. 4.

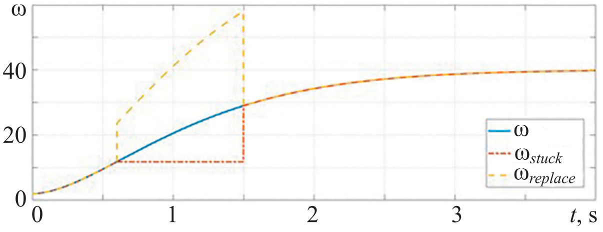

Fig. 4. Readings of the angular velocity sensor when attacking it

Simulation results show that sensor signals during information attacks are similar to signals during failures. Thus, we can conclude that the sensor signals are similar in the cases of faults and attacks. Therefore, such methods of sensor fault detection and isolation, as based on observers and generators of residuals, hardware and time redundancy, can be used to detect attacks on the sensor.

Component failure/component attack

An attack on one of an automatic control system component can lead to parametric and structural disturbances. Fig. 5 graphs of velocity sensor under normal functioning (ω) and under sufficient deviation of motor parameters (ω_{fault}) are presented below.

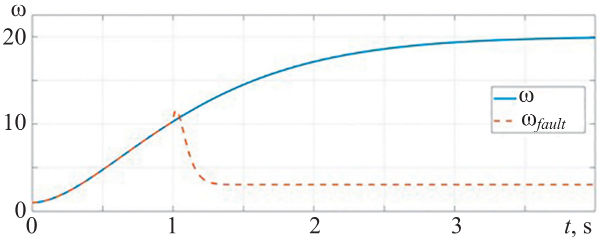

Fig. 5. Attack on a component

The similarity of the behavior of the system under component fault and under attack acting on plant parameters is due to the same physical impact on the plant. Therefore, it is advisable to use such methods based on the identification of the parameters of the plant for attack detection and isolation [42] as gradient approach, the least squares and dynamic regressor extension and mixing [49]. It is difficult to directly determine which element resulting in changes of the plant structure has been attacked since the behavior of the system becomes unpredictable. In this case, it is advisable to build faulty plant models under such attacks with further analysis of dynamics similarity.

Conclusion

In technical systems, detection of one malfunction does not guarantee the preservation of system integrity since attacks and faults can mutually reinforce each other and do more harm to the technical system, up to its destruction. Faults and attacks can function at different system levels, creating and reinforcing vulnerabilities that open the way to any destructive impact.

The field of research is a new area of scientific development which naturally appeared with the development of automatic control theory, mechanics, electronics, and digital and information technologies.

Research in detection and protection from faults has been conducted for a long time, but no approach allows analyzing attacks and faults together using uniform algorithms and approaches.

Recent research results focus on either information security analysis or robust and adaptive control. The intersection of information security and automatic control theory approaches will allow synthesizing algorithms and approaches that can significantly increase both information and functional security of technical systems.

Moreover, such an interdisciplinary approach can contribute to a positive economic effect by reducing repair time, increasing system quality indicators, etc.

In the course of the work, it was noted the patent purity of the study. Thus, it can be concluded that today it is extremely important to solve the problem of generally-purpose methods synthesis of multilevel control of systems with scalability and fault tolerance.

Also, in the paper the impact of information attacks and failures on automatic control systems is analyzed, the reasons and behavioral portraits of various types of attacks on technical systems and failures of actuators, sensors, and components are considered. The analysis revealed that the detection and isolation of failures can be used to detect and isolate a wide class of attacks on controllers, measuring devices and control system components. Computer modeling using a DC motor as an example revealed that the dynamics of control systems subjected to information attacks is similar to the dynamics of control systems with failures. This conclusion can be extended to a wide class of technical systems. Based on the results obtained, in the future, a structure for ensuring information and functional security can be developed (Fig. 1), based on the scientific and methodological apparatus for detecting and isolating failures of technical systems, which will increase the level of reliability, timely identify failures and information attacks within one control system, take timely measures to compensate their impact, reduce the time to restore the correct operation of the system.

References

1. Lee J., Bagheri B., Kao H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 2015, vol. 3, pp. 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001
2. Lasi H., Fettke P., Kemper H.G., Feld T., Hoffmann M. Industry 4.0. *Business & Information Systems Engineering*, 2014, vol. 6, no. 4, pp. 239–242. https://doi.org/10.1007/s12599-014-0334-4
3. Hwang I., Kim S., Kim Y., Seah C.E. A survey of fault detection, isolation, and reconfiguration methods. *IEEE Transactions on Control Systems Technology*, 2010, vol. 18, no. 3, pp. 636–653. https://doi.org/10.1109/TCST.2009.2026285
4. Patton R.J., Chen J. On eigenstructure assignment for robust fault diagnosis. *International Journal of Robust and Nonlinear Control*, 2000, vol. 10, no. 14, pp. 1193–1208. https://doi.org/10.1002/1099-1239(20001215)10:14<1193::AID-RNC523>3.0.CO;2-R
5. Wünnenberg J., Frank P.M. Sensor fault detection via robust observers. *System Fault Diagnostics, Reliability and Related Knowledge-Based Approaches. V. 1*. Springer, Dordrecht, 1987, pp. 147–160. https://doi.org/10.1007/978-94-009-3929-5_5
6. Watanabe K., Himmelblau D.M. Instrument fault detection in systems with uncertainties. *International Journal of Systems Science*, 1982, vol. 13, no. 2, pp. 137–158. https://doi.org/10.1080/00207728208926337
7. Frank P.M., Wünnenberg J. Robust fault diagnosis using unknown input observers schemes. *Fault Diagnosis in Dynamic Systems: Theory and Application*. New York, Prentice-Hall, 1989, pp. 47–98.
8. Gertler J. Fault detection and isolation using parity relations. *Control Engineering Practice*, 1997, vol. 5, no. 5, pp. 653–661. https://doi.org/10.1016/S0967-0661(97)00047-6
9. Patton R.J., Chen J. Robust fault detection using eigenstructure assignment: A tutorial consideration and some new results. *Proc. of*

Литература

1. Lee J., Bagheri B., Kao H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems // Manufacturing Letters. 2015. V. 3. P. 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001
2. Lasi H., Fettke P., Kemper H.G., Feld T., Hoffmann M. Industry 4.0 // Business & Information Systems Engineering. 2014. V. 6. N 4. P. 239–242. https://doi.org/10.1007/s12599-014-0334-4
3. Hwang I., Kim S., Kim Y., Seah C.E. A survey of fault detection, isolation, and reconfiguration methods // IEEE Transactions on Control Systems Technology. 2010. V. 18. N 3. P. 636–653. https://doi.org/10.1109/TCST.2009.2026285
4. Patton R.J., Chen J. On eigenstructure assignment for robust fault diagnosis // International Journal of Robust and Nonlinear Control. 2000. V. 10. N 14. P. 1193–1208. https://doi.org/10.1002/1099-1239(20001215)10:14<1193::AID-RNC523>3.0.CO;2-R
5. Wünnenberg J., Frank P.M. Sensor fault detection via robust observers // System Fault Diagnostics, Reliability and Related Knowledge-Based Approaches. V. 1. Springer, Dordrecht, 1987. P. 147–160. https://doi.org/10.1007/978-94-009-3929-5_5
6. Watanabe K., Himmelblau D.M. Instrument fault detection in systems with uncertainties // International Journal of Systems Science. 1982. V. 13. N 2. P. 137–158. https://doi.org/10.1080/00207728208926337
7. Frank P.M., Wünnenberg J. Robust fault diagnosis using unknown input observers schemes // Fault Diagnosis in Dynamic Systems: Theory and Application. New York: Prentice-Hall, 1989. P. 47–98.
8. Gertler J. Fault detection and isolation using parity relations // Control Engineering Practice. 1997. V. 5. N 5. P. 653–661. https://doi.org/10.1016/S0967-0661(97)00047-6
9. Patton R.J., Chen J. Robust fault detection using eigenstructure assignment: A tutorial consideration and some new results // Proc. of

the 30th IEEE Conference on Decision and Control, 1991, pp. 2242–2247. https://doi.org/10.1109/CDC.1991.261546

10. Patton R.J., Chen J. Review of parity space approaches to fault diagnosis for aerospace systems. *Journal of Guidance, Control, and Dynamics*, 1994, vol. 17, no. 2, pp. 278–285. https://doi.org/10.2514/3.21194
11. Stoustrup J., Niemann H.H. Fault estimation — a standard problem approach. *International Journal of Robust and Nonlinear Control*, 2002, vol. 12, no. 8, pp. 649–673. https://doi.org/10.1002/rnc.716
12. Maqill D.T. Optimal adaptive estimation of sampled stochastic processes. *IEEE Transactions on Automatic Control*, 1965, vol. 10, no. 4, pp. 434–439. https://doi.org/10.1109/TAC.1965.1098191
13. Maybeck P.S. *Stochastic Models, Estimation and Control. V. 1*. Arlington, VA, Navtech Press, 1994, 423 p.
14. Maybeck P.S. *Stochastic Models, Estimation and Control. V. 2*. Arlington, VA, Navtech Press, 1994.
15. Wang H., Lin W. Applying observer based FDI techniques to detect faults in dynamic and bounded stochastic distributions. *International Journal of Control*, 2000, vol. 73, no. 15, pp. 1424–1436. https://doi.org/10.1080/002071700445433
16. Simani S., Fantuzzi C., Patton R.J. *Model-Based Fault Diagnosis in Dynamic Systems Using Identification Techniques*. London, U.K., Springer, 2003, XV, 282 p. https://doi.org/10.1007/978-1-4471-3829-7
17. Chen R.H., Ng H.K., Speyer J.L., Guntur L.S., Carpenter R. Health monitoring of a satellite system. *Journal of Guidance, Control, and Dynamics*, 2006, vol. 29, no. 3, pp. 593–605. https://doi.org/10.2514/1.15012
18. Pertew M., Marquez H.J., Zhao Q. Design of unknown input observers for Lipschitz nonlinear systems. *Proceedings of the American Control Conference*, 2005, vol. 6, pp. 4198–4203. https://doi.org/10.1109/ACC.2005.1470637
19. Baroni P., Lamperti G., Pogliano P., Zanella M. Diagnosis of a class of distributed discrete-event systems. *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, 2000, vol. 30, no. 6, pp. 731–752. https://doi.org/10.1109/3468.895897
20. Lunze J., Schröder J. Sensor and actuator fault diagnosis of systems with discrete inputs and outputs. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2004, vol. 34, no. 2, pp. 1096–1107. https://doi.org/10.1109/TSMCB.2003.820593
21. Cordier M.O., Dugue P., Dumas M., Lévy F., Montmain J., Staroswiecki M., Travé Massuyès L. AI and automatic control approaches of model-based diagnosis: Links and underlying hypotheses. *IFAC Proceedings Volumes*, 2000, vol. 33, no. 11, pp. 279–284. https://doi.org/10.1016/S1474-6670(17)37373-1
22. Cordier M.O., Dague P., Lévy F., Mountmain J., Staroswiecki M., Travé-Massuyès L. Conflicts versus analytical redundancy relations: A comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2004, vol. 34, no. 5, pp. 2163–2177. https://doi.org/10.1109/TSMCB.2004.835010
23. Blanke M., Kinnaert M., Lunze J., Staroswiecki M. *Diagnosis and Fault-Tolerant Control*. Berlin, Springer, 2006, XIX, 672 p. https://doi.org/10.1007/978-3-540-35653-0
24. Zhang Y., Jiang J. Bibliographical review on reconfigurable fault-tolerant control systems. *Annual Reviews in Control*, 2008, vol. 32, no. 2, pp. 229–252. https://doi.org/10.1016/j.arcontrol.2008.03.008
25. Zhang X., Parisini T., Polycarpou M.M. Adaptive fault-tolerant control of nonlinear uncertain systems: an information-based diagnostic approach. *IEEE Transactions on Automatic Control*, 2004, vol. 49, no. 8, pp. 1259–1274. https://doi.org/10.1109/TAC.2004.832201
26. Iureva R.A., Margun A.A., Maltseva N.K., Vedernikov K. Electromechanical drive fault detection. *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 643, no. 1, pp. 012114. https://doi.org/10.1088/1757-899X/643/1/012114
27. Zhang Y.M., Jiang J. Active fault-tolerant control system against partial actuator failures. *IEE Proceedings: Control Theory and Applications*, 2002, vol. 149, no. 1, pp. 95–104. https://doi.org/10.1049/ip-cta:20020110
28. Khurana H., Hadley M., Lu N., Frincke D.A. Smart-grid security issues. *IEEE Security and Privacy*, 2010, vol. 8, no. 1, pp. 81–85. https://doi.org/10.1109/MSP.2010.49
29. Desnitsky V.A., Levshun D.S., Chechulin A.A., Kotenko I.V. Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system. *Journal of Wireless Mobile*

the 30th IEEE Conference on Decision and Control. 1991. P. 2242–2247. https://doi.org/10.1109/CDC.1991.261546

10. Patton R.J., Chen J. Review of parity space approaches to fault diagnosis for aerospace systems // Journal of Guidance, Control, and Dynamics. 1994. V. 17. N 2. P. 278–285. https://doi.org/10.2514/3.21194
11. Stoustrup J., Niemann H.H. Fault estimation — a standard problem approach // International Journal of Robust and Nonlinear Control. 2002. V. 12. N 8. P. 649–673. https://doi.org/10.1002/rnc.716
12. Maqill D.T. Optimal adaptive estimation of sampled stochastic processes // IEEE Transactions on Automatic Control. 1965. V. 10. N 4. P. 434–439. https://doi.org/10.1109/TAC.1965.1098191
13. Maybeck P.S. Stochastic Models, Estimation and Control. V. 1. Arlington, VA: Navtech Press, 1994.
14. Maybeck P.S. Stochastic Models, Estimation and Control. V. 2. Arlington, VA: Navtech Press, 1994.
15. Wang H., Lin W. Applying observer based FDI techniques to detect faults in dynamic and bounded stochastic distributions // International Journal of Control. 2000. V. 73. N 15. P. 1424–1436. https://doi.org/10.1080/002071700445433
16. Simani S., Fantuzzi C., Patton R.J. Model-Based Fault Diagnosis in Dynamic Systems Using Identification Techniques. London, U.K.: Springer, 2003. XV, 282 p. https://doi.org/10.1007/978-1-4471-3829-7
17. Chen R.H., Ng H.K., Speyer J.L., Guntur L.S., Carpenter R. Health monitoring of a satellite system // Journal of Guidance, Control, and Dynamics. 2006. V. 29. N 3. P. 593–605. https://doi.org/10.2514/1.15012
18. Pertew M., Marquez H.J., Zhao Q. Design of unknown input observers for Lipschitz nonlinear systems // Proceedings of the American Control Conference. 2005. V. 6. P. 4198–4203. https://doi.org/10.1109/ACC.2005.1470637
19. Baroni P., Lamperti G., Pogliano P., Zanella M. Diagnosis of a class of distributed discrete-event systems // IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans. 2000. V. 30. N 6. P. 731–752. https://doi.org/10.1109/3468.895897
20. Lunze J., Schröder J. Sensor and actuator fault diagnosis of systems with discrete inputs and outputs // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. 2004. V. 34. N 2. P. 1096–1107. https://doi.org/10.1109/TSMCB.2003.820593
21. Cordier M.O., Dugue P., Dumas M., Lévy F., Montmain J., Staroswiecki M., Travé Massuyès L. AI and automatic control approaches of model-based diagnosis: Links and underlying hypotheses // IFAC Proceedings Volumes. 2000. V. 33. N 11. P. 279–284. https://doi.org/10.1016/S1474-6670(17)37373-1
22. Cordier M.O., Dague P., Lévy F., Mountmain J., Staroswiecki M., Travé-Massuyès L. Conflicts versus analytical redundancy relations: A comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. 2004. V. 34. N 5. P. 2163–2177. https://doi.org/10.1109/TSMCB.2004.835010
23. Blanke M., Kinnaert M., Lunze J., Staroswiecki M. Diagnosis and Fault-Tolerant Control. Berlin: Springer, 2006. XIX, 672 p. https://doi.org/10.1007/978-3-540-35653-0
24. Zhang Y., Jiang J. Bibliographical review on reconfigurable fault-tolerant control systems // Annual Reviews in Control. 2008. V. 32. N 2. P. 229–252. https://doi.org/10.1016/j.arcontrol.2008.03.008
25. Zhang X., Parisini T., Polycarpou M.M. Adaptive fault-tolerant control of nonlinear uncertain systems: an information-based diagnostic approach // IEEE Transactions on Automatic Control. 2004. V. 49. N 8. P. 1259–1274. https://doi.org/10.1109/TAC.2004.832201
26. Iureva R.A., Margun A.A., Maltseva N.K., Vedernikov K. Electromechanical drive fault detection // IOP Conference Series: Materials Science and Engineering. 2019. V. 643. N 1. P. 012114. https://doi.org/10.1088/1757-899X/643/1/012114
27. Zhang Y.M., Jiang J. Active fault-tolerant control system against partial actuator failures // IEE Proceedings: Control Theory and Applications. 2002. V. 149. N 1. P. 95–104. https://doi.org/10.1049/ip-cta:20020110
28. Khurana H., Hadley M., Lu N., Frincke D.A. Smart-grid security issues // IEEE Security and Privacy. 2010. V. 8. N 1. P. 81–85. https://doi.org/10.1109/MSP.2010.49
29. Desnitsky V.A., Levshun D.S., Chechulin A.A., Kotenko I.V. Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system // Journal of Wireless

Networks, Ubiquitous Computing, and Dependable Applications, 2016, vol. 7, no. 2, pp. 60–80. https://doi.org/10.22667/JOWUA.2016.06.31.060

30. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*, 2018, vol. 100, pp. 212–223. https://doi.org/10.1016/j.compind.2018.04.017
31. Wang E.K., Ye Y., Xu X., Yiu S.M., Hui L.C.K., Chow K.P. Security issues and challenges for cyber physical system. *Proc. of the IEEE/ACM International Conference on Green Computing and Communications (GreenCom), 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, (CPSCom)*, 2010, pp. 733–738. https://doi.org/10.1109/GreenCom-CPSCom.2010.36
32. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. *Computer Networks*, 2015, vol. 76, pp. 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
33. Sridhar S., Hahn A., Govindarasu M. Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, 2012, vol. 100, no. 1, pp. 210–224. https://doi.org/10.1109/JPROC.2011.2165269
34. Gifty R., Bharathi R., Krishnakumar P. Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection. *Neural Computing and Applications*, 2019, vol. 31, no. 1, pp. 23–34. https://doi.org/10.1007/s00521-018-3635-6
35. Iureva R.A., Kremlev A.S., Margun A.A., Vlasov S.M., Timko A.S. Measures to design secure cyber-physical things. *Smart Innovation, Systems and Technologies*, 2019, vol. 142, pp. 315–322. https://doi.org/10.1007/978-981-13-8311-3_27
36. Iureva R.A., Danenkov I.S., Timko A.S., Vlasov S.M., Vasilkov S.D. Optical sensors in IoT. *Proceedings of SPIE*, 2019, vol. 11028, pp. 1102816. https://doi.org/10.1117/12.2517076
37. Iureva R.A., Belov A.A., Margun A.A., Kremlev A.S. Electric drive attack detection based on state observers. *Proc. of the 20th International Carpathian Control Conference (ICCC)*, 2019, pp. 8766015. https://doi.org/10.1109/carpathiancc.2019.8766015
38. Iureva R., Margun A., Maltseva N., Vedernikov K. Electromechanical drive fault detection. *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 643, no. 1, pp. 012114. https://doi.org/10.1088/1757-899X/643/1/012114
39. Dobriborsci D., Margun A., Kolyubin S. Theoretical and experimental research of the discrete output robust controller for uncertain plant. *Proc. of the 16th European Control Conference (ECC)*, 2018, pp. 533–538. https://doi.org/10.23919/ECC.2018.8550138
40. Chen J., Patton R.J. *Robust Model-Based Fault Diagnosis for Dynamic Systems*. Boston, MA, U.S.A., Kluwer Academic Publishers, 1999, pp. 354.
41. Patton R.J., Chen J. Observer-based fault detection and isolation: Robustness and applications. *Control Engineering Practice*, 1997, vol. 5, no. 5, pp. 671–682. https://doi.org/10.1016/S0967-0661(97)00049-X
42. Isermann R. Supervision, fault-detection and fault-diagnosis methods — An introduction. *Control Engineering Practice*, 1997, vol. 5, no. 5, pp. 639–652. https://doi.org/10.1016/S0967-0661(97)00046-4
43. Behzad H., Casavola A., Tedesco F., Sadrnia M.A. Fault-tolerant sensor reconciliation schemes based on unknown input observers. *International Journal of Control*, 2020, vol. 93, no. 3, pp. 669–679. https://doi.org/10.1080/00207179.2018.1484568
44. Morris T., Gao W. Industrial control system cyber attacks. *Proc. of the 1st International Symposium for ICS & SCADA Cyber Security Research*, 2013, pp. 22–29. https://doi.org/10.14236/ewic/icscsr2013.3
45. Yılmaza E.N., Gönenb S. Attack detection/prevention system against cyber-attack in industrial control systems. *Computers and Security*, 2018, vol. 77, pp. 94–105. https://doi.org/10.1016/j.cose.2018.04.004
46. Rathika R.K., Marimuthu A. An improved detection and prevention of DDoS attacks in nuclear power plants machine monitoring. *Proc. of the Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2017, pp. 1–7. https://doi.org/10.1109/ICECCT.2017.8117897
47. Pasqualetti F., Dorfler F., Bullo F. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 2013, vol. 58, no. 11, pp. 2715–2729. https://doi.org/10.1109/TAC.2013.2266831
48. Danenkov I., Kolesnikova D., Babikov A., Iureva R. Security by design development methodology for file hosting case. *Smart*

Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2016. V. 7. N 2. P. 60–80. https://doi.org/10.22667/JOWUA.2016.06.31.060

30. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues // Computers in Industry. 2018. V. 100. P. 212–223. https://doi.org/10.1016/j.compind.2018.04.017
31. Wang E.K., Ye Y., Xu X., Yiu S.M., Hui L.C.K., Chow K.P. Security issues and challenges for cyber physical system // Proc. of the IEEE/ACM International Conference on Green Computing and Communications (GreenCom), 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, (CPSCom). 2010. P. 733–738. https://doi.org/10.1109/GreenCom-CPSCom.2010.36
32. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead // Computer Networks. 2015. V. 76. P. 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
33. Sridhar S., Hahn A., Govindarasu M. Cyber-physical system security for the electric power grid // Proceedings of the IEEE. 2012. V. 100. N 1. P. 210–224. https://doi.org/10.1109/JPROC.2011.2165269
34. Gifty R., Bharathi R., Krishnakumar P. Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection // Neural Computing and Applications. 2019. V. 31. N 1. P. 23–34. https://doi.org/10.1007/s00521-018-3635-6
35. Iureva R.A., Kremlev A.S., Margun A.A., Vlasov S.M., Timko A.S. Measures to design secure cyber-physical things // Smart Innovation, Systems and Technologies. 2019. V. 142. P. 315–322. https://doi.org/10.1007/978-981-13-8311-3_27
36. Iureva R.A., Danenkov I.S., Timko A.S., Vlasov S.M., Vasilkov S.D. Optical sensors in IoT // Proceedings of SPIE. 2019. V. 11028. P. 1102816. https://doi.org/10.1117/12.2517076
37. Iureva R.A., Belov A.A., Margun A.A., Kremlev A.S. Electric drive attack detection based on state observers // Proc. of the 20th International Carpathian Control Conference (ICCC). 2019. P. 8766015. https://doi.org/10.1109/carpathiancc.2019.8766015
38. Iureva R., Margun A., Maltseva N., Vedernikov K. Electromechanical drive fault detection // IOP Conference Series: Materials Science and Engineering. 2019. V. 643. N 1. P. 012114. https://doi.org/10.1088/1757-899X/643/1/012114
39. Dobriborsci D., Margun A., Kolyubin S. Theoretical and experimental research of the discrete output robust controller for uncertain plant // Proc. of the 16th European Control Conference (ECC). 2018. P. 533–538. https://doi.org/10.23919/ECC.2018.8550138
40. Chen J., Patton R.J. Robust Model-Based Fault Diagnosis for Dynamic Systems. Boston, MA, U.S.A.: Kluwer Academic Publishers, 1999. P. 354.
41. Patton R.J., Chen J. Observer-based fault detection and isolation: Robustness and applications // Control Engineering Practice. 1997. V. 5. N 5. P. 671–682. https://doi.org/10.1016/S0967-0661(97)00049-X
42. Isermann R. Supervision, fault-detection and fault-diagnosis methods — An introduction // Control Engineering Practice. 1997. V. 5. N 5. P. 639–652. https://doi.org/10.1016/S0967-0661(97)00046-4
43. Behzad H., Casavola A., Tedesco F., Sadrnia M.A. Fault-tolerant sensor reconciliation schemes based on unknown input observers // International Journal of Control. 2020. V. 93. N 3. P. 669–679. https://doi.org/10.1080/00207179.2018.1484568
44. Morris T., Gao W. Industrial control system cyber attacks // Proc. of the 1st International Symposium for ICS & SCADA Cyber Security Research. 2013. P. 22–29. https://doi.org/10.14236/ewic/icscsr2013.3
45. Yılmaza E.N., Gönenb S. Attack detection/prevention system against cyber-attack in industrial control systems // Computers and Security. 2018. V. 77. P. 94–105. https://doi.org/10.1016/j.cose.2018.04.004
46. Rathika R.K., Marimuthu A. An improved detection and prevention of DDoS attacks in nuclear power plants machine monitoring // Proc. of the Second International Conference on Electrical, Computer and Communication Technologies (ICECCT). 2017. P. 1–7. https://doi.org/10.1109/ICECCT.2017.8117897
47. Pasqualetti F., Dorfler F., Bullo F. Attack detection and identification in cyber-physical systems // IEEE Transactions on Automatic Control. 2013. V. 58. N 11. P. 2715–2729. https://doi.org/10.1109/TAC.2013.2266831
48. Danenkov I., Kolesnikova D., Babikov A., Iureva R. Security by design development methodology for file hosting case // Smart Innovation, Systems and Technologies. 2020. V. 188. P. 383–390. https://doi.org/10.1007/978-981-15-5584-8_33

Innovation, Systems and Technologies, 2020, vol. 188, pp. 383–390. https://doi.org/10.1007/978-981-15-5584-8_33

49. Belov A.A., Aranovskiy S., Ortega R., Barabanov N., Bobtsov A.A. Enhanced parameter convergence for linear systems identification: The DREM approach. *Proc. of the 16th European Control Conference (ECC)*, 2018, pp. 2794–2799. https://doi.org/10.23919/ECC.2018.8550338

Authors

Alexey A. Margun — PhD, Assistant Professor, ITMO University, Saint Petersburg, 197101, Russian Federation; Researcher, Institute for Problems in Mechanical Engineering of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation, SC 55521791600, https://orcid.org/0000-0002-5333-0594, alexeimargun@gmail.com

Radda A. Iureva — PhD, Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57190606805, https://orcid.org/0000-0002-8006-0980, raddaiureva@itmo.ru

Daria V. Kolesnikova — PhD Student, Assistant, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57206781641, https://orcid.org/0000-0003-0942-3926, Kolesnikova_d@itmo.ru

Received 14.02.2022
Approved after reviewing 14.04.2022
Accepted 15.05.2022

49. Belov A.A., Aranovskiy S., Ortega R., Barabanov N., Bobtsov A.A. Enhanced parameter convergence for linear systems identification: The DREM approach // Proc. of the 16th European Control Conference (ECC). 2018. P. 2794–2799. https://doi.org/10.23919/ECC.2018.8550338

Авторы

Маргун Алексей Анатольевич — кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; научный сотрудник, Институт проблем машиноведения РАН, Санкт-Петербург, 199178, Российская Федерация, SC 55521791600, https://orcid.org/0000-0002-5333-0594, alexeimargun@gmail.com

Юрьева Радда Алексеевна — кандидат технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57190606805, https://orcid.org/0000-0002-8006-0980, raddaiureva@itmo.ru

Колесникова Дарья Викторовна — аспирант, ассистент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57206781641, https://orcid.org/0000-0003-0942-3926, Kolesnikova_d@itmo.ru

Статья поступила в редакцию 14.02.2022
Одобрена после рецензирования 14.04.2022
Принята к печати 15.05.2022