Original article
Dependability, vol. 18 no.4, 2018 DOI: 10.21683/1729-2646-2018-18-4-36-44

Method of assessing the protection of computer-based control systems under information technology interference

Sergey M. Klimov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Korolyov, Russia*
Yuri V. Sosnovsky, *Physics and Technology Institute, V.I. Vernadsky Crimean Federal University, Simferopol, Russia*

Sergey M. Klimov

Yuri V. Sosnovsky

Abstract. *The aim of this paper is to develop models that would enable a standardized representation of the structure, functions of computer-based control systems (CBCS) and quantification of the risk (fault tolerance) of automated control systems and their primary components, i.e. CBCS, under information technology interference (ITI). The paper shows the relevance and importance of CBCS models and estimation of the risk of operation of automated process control systems (APCS) under various ITI (computer attacks). Intruder ITI under consideration includes hardware, firmware and software-based interference able of blocking communication channels, disrupting information availability and integrity, as well as targeted and lasting information technology interference with an automated system, namely with the use of malware. The structural and functional model of a computer-based control system as the primary component of a higher-level system (APCS) developed in this paper is composed of a set of diagrams and descriptions of functions. The structural and functional model includes the following: channel structure of the control system's main cycle (reading, processing of data, recording of output values, as well as communication subsystem operations), structural and functional diagram of CBCS of various types depending on the availability and utilization of a communication channel within the structure of the control cycles, standard vulnerability certificate. The diagrams detail the standard functions, operating procedures and information interaction of CBCS modules with the environment via communication channels. The ITI-specific risk model of APCS and CBCS as its part is described by indicators that characterize the conditional harm and condition of the control system, in which it is able to recover its operability, or whether external intervention is required that would affect not only the control system itself, but the controlled process as well. The following indicators were examined: characteristic points and parameters of risk function based on the Weibull-Gnedenko distribution, statistical estimation of CBCS protection, risk function, dynamic estimation of the risk of successful implementation of ITI against CBCS. It is assumed that the values of the parameters required for the calculation of the risk parameters and CBCS protection were obtained:*
- empirically based on structural and parametric analysis of the design features, functional dynamics and vulnerabilities of CBCS
- as part of testbed simulation of CBCS as computer network users under ITI
- experimentally based on the frequency of successful ITI threats,
and the protection indicators are also extrapolated to the whole CBCS lifecycle by means of a dynamic risk function-based correction using the Weibull-Gnedenko distribution.
In the conclusion it is noted that the developed method of assessment of CBCS protection under ITI allows evaluating the risks of successful implementation by an intruder of malicious actions against CBCS and APCS in general, which predetermines the requirement for timely elimination of CBCS vulnerabilities and adoption of additional organizational and technical measures aimed at improving information security of automated control systems.

Keywords: *information technology interference, computer-based control systems, information protection facilities, fault tolerance.*

For citation: *Klimov SM, Sosnovsky YuV. Method of assessing the protection of computer-based control systems under information technology interference. Dependability 2018;4: 36-44. DOI: 10.21683/1729-2646-2018-18-4-36-44*

Introduction

The Doctrine of Information Security of the Russian Federation approved by order of the President of the Russian Federation in 2016 defines the current threats of information technology interference against the nation's critical information infrastructure.

Today, the necessities of the nation's developing digital economy define the active introduction of information and communication technologies as part of automated process control systems (APCS). Worldwide, APCS are classified as SCADA systems for control of power, transportation and industrial systems. In practice, the deployment of information and communication technologies causes the emergence of additional vulnerabilities in software, which increases the probability of realization of information technology interference (ITI) against them by an intruder.

Today's ITI malware [1], e.g. Stuxnet, Flame, miniFlame, Duqu, Gauss, Reign, Wiper, Shamoon, Careto exploit the vulnerabilities of the APCS software code for hidden deployment, self-propagation and intentional disruption of a system's operation. The development of ITI tools and their functional capabilities is significantly ahead of the corresponding tools of detection and prevention of computer attacks (CADPS), especially in the form of malicious software.

The key element of APCS CADPS is the sensor (firmware or software display module) that detects the fact of a computer incident, i.e. successful implementation of an ITI by an intruder.

The basic element of APCS are computer-based control systems (CBCS) [2], whose software performs the functions of collection, processing and transmission of information for the purpose of real-time control of critical facilities. While earlier programmable industrial microprocessors were controlled by means of sets of special commands, today they operate under the control of general-purpose operating systems (OS) (e.g. Windows or Linux) and are available as users of computer networks with TCP/IP data protocols or Modbus data protocol typical for SCADA systems.

The assessment and protection of information in CBCS affected by an intruder's ITI requires a system of methods and tools for detection, identification of malicious actions and elimination of their consequences [9-14].

Thus, the task of developing a method of evaluation of CBCS protection against ITI for the purpose of a priori quantitative estimation of the risks of violation of critical facilities' CBCS operation is of relevance and practical interest.

Problem definition

The research is based on the following premises:

- estimation of the risks of an intruder's successful ITI must be carried out using a testbench that allows creating the required test conditions for the operation of functional equivalents of CBCS, elements of CADPS and ITI simulation

- the identified groups of risks of CBCS operation disruptions can be assessed on site using a mobile test suite

- preliminary assessment of CBCS vulnerabilities and an intruder's ITI threats allows defining possible information protection facilities (IPF) and choose the most efficient ones.

The CBCS protection parameters are defined:

- empirically based on structural and parametric analysis of the design features, functional dynamics and vulnerabilities of CBCS

- experimentally based on the frequency of an intruder's successful ITI

the identified protection indicators are also extrapolated to the whole CBCS lifecycle by means of a dynamic risk function-based correction using the Weibull-Gnedenko distribution [3-4].

The development of a method of evaluation of CBCS protection under ITI is based on the model of CBCS operation under ITI that enables comprehensive analysis of mutually related processes of CBCS operation, ITI implementation and elimination of consequences.

The final model implies the CBCS is equipped with a communication subsystem. The communication subsystem enables such functions as interaction with industrial systems of a higher level, remote reading of sensor data and recording of their values into executive devices by means of network interfaces.

The CBCS communication subsystem that is directly included into the process control loop, is the primary vulnerability for the implementation by the intruder of the ITI threats against its data communication protocols. It is assumed that an intruder, while implementing an ITI, may exploit undocumented features of both the hardware and software facilities of a CBCS, and programmable routers of the data communication network at various APCS levels. Additionally, an intruder may be both on the outside and inside and be aware of the specificity and time limits of a process (triggering conditions of the automatic and automated executive devices) and is able to implement an unknown zero-day action.

The diagram of the model of CBCS operation under ITI in terms of an augmented Petri net (APN) [5] is shown in Figure 1.

Model of CBCS operation under ITI includes three loops:

1. Normal CBCS operation loop that enables simulation and structure and parameter analysis of the CBCS control loop (CL).

2. ITI simulation loop designed to simulate an intruder's actions associated with the acquisition of unauthorized access to CBCS, passive and active vulnerability scanning, selection and launching of ITI. For the input information regarding the modern threats of malware-based ITI this paper refers to [1].

3. ITI consequences elimination loop that enables the simulation of the processes of prevention, detection and

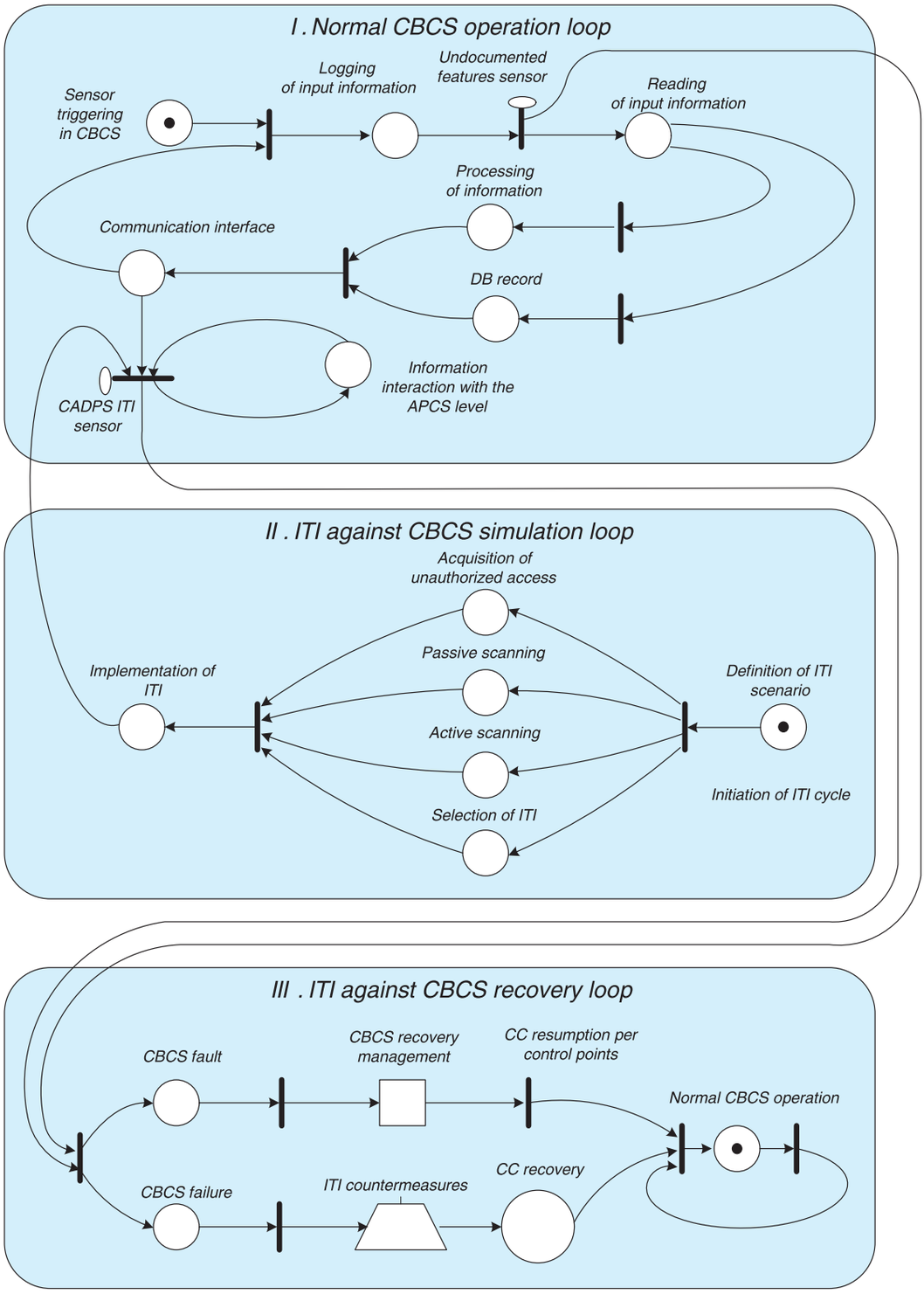

Figure 1. Diagram of the model of CBCS operation under ITI in terms of APN

elimination of ITI consequences based on the use of sensors (indication modules) of interference detection and identification.

In Figure 1, block III shows two alternative solutions for the elimination of ITI consequences for CBCS in case of their successful implementation by an intruder.

Branch I (upper) shows the situation in which a CBCS demonstrates the recovery after fault (relatively short CC, i.e. from several seconds to several minutes). A fault is understood as a short disruption of CC caused by ITI that yet does not entail CBCS failure. In this case, if a fault is identified, the system launches the CC recovery algorithm,

upon the completion of which the CBCS enters the state of normal operation.

Branch II (lower) shows the ITI implementation approach, under which the CBCS enters the state of failure that is characterized by long disruption of CBCS control processes (from 30 minutes to several hours).

The specificity of CBCS is such as the CC recovery after a long failure often requires the involvement of the operator and/or technical personnel and cannot be performed by means of a reset or deployment of an a priori operable CBCS.

Preventing faults and failures of CBCS under ITI requires prompt detection, localization of the interference and CC recovery based on the deployed redundant CADPS sensors (indication hardware and software facilities) [5-6].

Formalization of the model of CBCS operation under ITI and in terms of APN [5]:

$$S_{CBCS} = \{(P,V),T,D,M,Q,I_p,Y\}, \quad (1)$$

where $P = p_1, p_2, ..., p_i$ is a nonvacuous finite set of places that characterize the normal CBCS operation mode

$V = v_1, v_2, ..., v_i$ is the set of recovery places that reflect the procedures of recovery after an intruder's successful ITI (graphically presented as □)

$T = t_1, t_2, ..., t_i$ is a nonvacuous set of transitions. According to APN, each transition t_i can be associated with the triggering algorithm $a \vee g_i$ (if the algorithm is available the transition is marked with $a \vee g_i$)

D is a nonvacuous finite set of net arcs, while $D = (D_1 \cup D)$, $D_1 = (P \times T) \cup (V \times T)$ is a nonvacuous set of input arcs connecting places and transitions, $D_2 = (T \times P) \cup (T \times V)$ is a nonvacuous set of output arcs oriented from transitions to places

M is the set of Petri net markings

$F_p : (M_p : P \to N), F_v : (M_v : V \to N)$ are the functions of the initial marking of the places of normal operation and recovery, respectively, N={0,1,2,…} is a set of natural numbers (marked with a dot inside the place ⊙)

Q is the set of probabilities of transition firing that represents the probabilities of CBCS being in normal operation, moments of ITI implementation and CADPS sensors triggering, recovery processes

Z_{ACMi} is the set of places of ITI countermeasures ( )

$I_p = i_{p1}, i_{p2}, ..., i_{pm}$ is the set of priorities for arcs

$Y = y_1, y_2, ..., y_k$ is the set ITI temporal parameters.

The functions of description of APN structure in the form of set mapping are as follows:

$$F_{d1} : P \times T \cup V \times T \to N, \text{ or } F(p_i, v_j, t_n), \quad (2)$$

$$F_{d2} : T \times P \cup T \times V \to N, \text{ or } F(t_n, p_i, v_j),$$

where F_{d1} is the function of input places that associates the number of markings required for transition firing ("input") with the places and transitions

F_{d2} is the function of output places that associates the number of markings required for the modification of marking (correction of "output") with the places and transitions

N={0,1,2,…} is a set of natural numbers.

Given the above, the rule of transition firing has the following standard form:

$$\forall (p_i \in P \wedge v_j \in V) \to \exists (M(p_i) \geq F_{d1}(p_i, v_j, t_n)). \quad (3)$$

If transition t_n is triggered, out of each of its input places p_i and v_j the number of markings $m(p_i)$ and $m(v_j)$ is removed that is equal to the number of input arcs, while to the output places p_{i+1} and v_{j+1} the number of markings is added that is equal to the number of output arcs. The transition is triggered that corresponds with the highest probability of its firing (q_w) and is preceded with the arc with a higher priority (i_{pm}). The delay of transition triggering time is defined by the ITI parameters (y_k) in the net places connected to such transition with arcs. Accordingly, the APN marking change rule is as follows:

$$\forall (M_p \wedge M_v) : (p_i \in P \wedge v_j \in V) \to \exists (M_p' \wedge M_v') =$$
$$= F_p(Mp) + F_v(Mv) - F_{d1}(p_i, v_j, t_n) + F_{d2}(t_n, p_i, v_j). \quad (4)$$

Description of initial marking (M_i) in APN for presentation and analysis of causal relationships between processes in CBCS and CADPS under ITI. Condition of achieving APN:

$$\forall (p_i \in P \wedge V_r \in V \wedge Z_j \in Z_{ACM}) \to \exists M'(p_i, v_r, z_j) =$$
$$= M(p_i, v_r, z_j) - [F_p(M_p) + F_v(M_v) + F_z(M_z)] -$$
$$- [F_{ud1}(p_i, v_r, z_j, t_n) + F_{ud2}(t_n, p_i, v_r, z_j)]. \quad (5)$$

Definition of logical conditions of firing of APN transitions (T_i) under marking $M(p_i, v_r, z_j)$:

$$\forall (p_i \in P \wedge V_r \in V \wedge Z_j \in Z_{ACM}) \to$$
$$\to \exists [M(p_{i1}, v_{r1}, z_{j1}) \geq F_{ud1}(p_i, v_r, z_j, t_n)],$$
$$\Psi_t [(p_{i1}, v_{r1}, z_{j1}), ..., (p_{in}, v_{rn}, z_{jn})] = 1, \quad (6)$$

where Ψ_t is the function of marking distribution per APN input places.

Definition of relation for APN place, "subevents" P_i, V_r, Z_{ACMi} of ITI warning, detection, analysis, active countermeasures as well as CBCS recovery:

$$\forall (p_i \in P, e_i \in E_{ki}, n_i \in N_{ki}, b_i \in B_{ki}) \to$$
$$\to \exists \min (p_i, V_r, Z_j, E_{ki+1}, N_{ki+1}, B_{ki+1},) \to$$
$$\to Z^*_{SE} \to, \Psi_{tn} = \{(p_{i1}, V_{r1}, Z_{j1}), ..., (p_{in}, V_{rn}, Z_{jn})\}. \quad (7)$$

The function of the starting input distribution of marking Ψ_t over APN places takes the value (8) that defines the order of the starting allocation of markings to APN places

$$\Psi_{tn}\left(p_i, V_r, Z_j\right) = \left\{1,\ if\ m_{pi} \in M_p, m_{vr} \in M_v, m_{zj} \in M_z. \right. \quad (8)$$

Definition of CADPS sensor triggering conditions:

$$\forall t_i \in T, Q_{ki} \in Q, \exists Q_{i+1} \neq 0,$$
$$\phi_q\left(t_i, Q_{ki}\right) = \left\{1,\ if\ mp_i \in M_p, y_i \in Y, a \vee g_i = \right.$$
$$= 1, \left\{\frac{1}{R},\ if\ mp_i \in M_p, y_i \notin Y, a \vee g_i = 1, \right. \quad (9)$$

where $a \vee g_i$ is the sensor triggering algorithm. The sensor triggering conditions are as follows:

$\phi_q\left(t_i, Q_{ki}\right) = 1$, sensor triggered, attack detected

$\phi_q\left(t_i, Q_{ki}\right) = \frac{1}{R}$, false sensor triggering with the R-th transition triggering

$\phi_q\left(t_i, Q_{ki}\right) = 0$, sensor not triggered, unknown attack not detected.

Taking into account today's methods of information systems protection and risk management [1, 5, 7, 9, 13, 14], the method of assessment of CBCS protection under ITI is presented as the following sequence of steps:

1. Definition of the method of CBCS monitoring taking into account the particular operating principles (controlled processes and types of data communication protocol).

2. Analysis of vulnerabilities and generation of CBCS vulnerabilities certificate.

3. Development of the ITI threat model.

4. Development of the simulation model of the controlled CBCS CC taking into account the APCS communication interfaces.

5. Experimental research of CBCS under ITI based on testbed simulation.

6. Evaluation of CBCS protection indicators based on the simulation results.

7. Assessment of the risks of CBCS protection disruption under ITI.

Step1. CBCS monitoring is based on the classification of CBCS. CBCS classification is based on attributes that include the availability of wired and wireless communication channels, interfaces (unidirectional, bidirectional, multipoint), capability of remote firmware replacement and remote CBCS administration. Based on the above attributes, let us identify the basic CBCS types:

CBCS of the 1-st type, i.e. system with a local controller performing local reading of input signals, data processing and generation of output control signals by means of local output modules

CBCS of the 2-nd type, i.e. system that uses data communication interfaces as the information environment between remote input-output modules and processor units

CBCS of the 3-rd type, i.e. systems that use data communication protocols that implement two-way communication to transmit data to higher-level systems and receive data from them

CBCS of the 4-th type, i.e. systems that have the properties of the systems of the 3-rd type, but allow remote (using the common data communication environment) administration, including correction and change of the control program (firmware replacement).

The controlled processes include internal and external data exchange via CBCS interfaces, parameters of network traffic to APCS components. Data exchange monitoring in CBCS is divided by types of data communication protocols and is performed by CADPS sensors through signature analysis and functional analysis of abnormal CBCS behaviour, detection of distortions of protocol structure, signalling and synchronization parameters, data packet preambles and various service parameters of CBCS equipment.

Step 2. CBCS software vulnerabilities shall be identified based on the provisions of GOST R 56546-2015 [8] and formalized as a standard certificate of CBCS software vulnerabilities under ITI (Table 1). The BDU:2018-00543 database vulnerability certificate by the State Research and Design Experimental Institute of Technical Information Protection of the Federal Service for Technical and Export Control of Russia was taken as a model. The following characteristics must be introduced to compliment the standard vulnerability certificate:

1. Type of industrial data communication protocol (due to potential unique attacks against industrial protocols that take into consideration the specifics of their hardware and software design).

2. The vulnerability vector must include data on the controlled process (regular, important, critical), as information technology interference against CBCS, APCS causes not only the fault or failure of such system, but also the fault or failure of the controlled process.

3. The Vulnerability Hazard Level indicator depends on both the vulnerability threat level, and the type of the controlled process (regular, critical).

Step 3. The development of the ITI threat model is based on the analysis of the potential threats that depend on the type of the CBCS (per the classification), as well as the used protocols and control cycles (CC) under control.

Given that information security is examined at CBCS level, the following primary ways of ITI implementation can be identified:

- threats of information technology interference originating at a higher level of APCS (such threats may include incorrect settings for a specific process, their enforcement, other attempts of interfering with the CBCS operation through distortion of information and control parameters)
- threats of interference with the CBCS information input and output protocols (in the case of CBCS of the types 2 to 4) causing the blocking of the protocols or disruption of the integrity of transmitted data
- threats of interference with the software component of CBCS (in cases when remote firmware replacement is available).

An intruder's capability to implement ITI threats are directly associated with the characteristics of the employed equipment, protocols, controlled CBCS processes and cannot be considered out of this context.

Table 1. Standard vulnerabilities certificate (exemplified by BDU:2018-00543)

Vulnerability description	Vulnerability of the track_import_export.php scenario of the U.motion builder manufacturing and residential buildings management system is associated with non-adoption of measures for protection of SQL query
Vendor	Schneider Electric
SW name	U.motion Builder
SW version	up to 1.3.4
SW type	APCS software tool
OS and hardware platforms	TBD
Error type	Non-adoption of measures for protection of SQL query structure (SQL injection type of attack)
Error type identifier	CWE-89
Vulnerability class	Code vulnerability
Date of detection	02.03.2018
Underlying vulnerability vector	AV:N/AC:L/Au:N/C:C/I:C/A:C
Hazard level of vulnerability	Critical level (CVSS 2.0 base rate is 10) High level (CVSS 2.0 base rate is 8.8)
Possible vulnerability elimination measures	Application of recommendations given at https://www.schneider- electric.com/en/download/document/SE_UMOTION_BUILDER/
Vulnerability status	Confirmed by manufacturer
Presence of exploit	TBD
Method of exploitation	Injection
Method of elimination	Software update
Information on elimination	Vulnerability eliminated
Source reference	https://www.schneider-electric.com/en/download/document/SE_UMOTION_BUILDER/
Identifiers of other vulnerability description systems	CVE: CVE-2018-7765
Other information	

Step 4. Development of the simulation model of the controlled CC in CBCS (research object) subject to APCS communication interfaces consists in the development of the so-called "information environment" and basic CBCS functions. In the course of testbed experiments a CBCS model can be represented as a separate group of programmable devices, e.g. programmable logical switches, whose software enables CBCS CC modeling subject to changes in the intentional and non-intentional control and information actions. In the course of simulation the role of "information environment" is played by independent software blocks of the model, while in the course of full-scale simulation this role is played by real equipment involved in the CC control. As part of simulation, the real CBCS CC may remain inactive (due to the complexity of complete replication of APCS functions), while the simulation of its reactions to certain actions can be executed by adding independent software modules to the special software of the communication equipment.

Step 5. Experimental research of CBCS under ITI based on testbed simulation involves three primary processes:

- simulation of normal CBCS operation
- simulation of ITI against CBCS out of the database of interference models
- simulation of IPF (for the purpose of this paper, CADPS) configured for CC monitoring subject to the proposed CBCS classification.

The program code and ITI simulation scenarios are stored in the database and are developed subject to the employed protocols, types and potential vulnerabilities of CBCS (per the classification). Some ITI may include standard computer attacks, e.g. ARP spoofing, DDoS, while others are specific to the protocols employed within the APCS. Examples of special ITI include computer attacks against the PTP (IEEE 1588) and Modbus protocols, CBCS controller firmware.

Step 6. Statistical estimation of CBCS protection consists in the estimation of CBCS protection based on the results of simulation and field modeling. CBCS protection assessment

is based on the verification of the correctness of control system operation per the levels of the reference model of open systems interactions.

Calculation of the statistical estimation indicators of CBCS protection is based on the ALARP principle and four established risk categories: from unacceptable to negligible [13, 14]. Accordingly, for each type of ITI and specified (obtained empirically or as part of simulation) the level of acceptable risk is selected along with the factor of relative risk scale spacing that allows formalizing the classification of ITI consequences as one of the four risk categories adopted in accordance with the ALARP principle. The values of the importance function are also selected individually for each ITI type.

Given the above, the final integral estimate of system risk can be calculated using the formula

$$R_{CBCS} = \frac{\sum_{j=0}^{3} k_j z_j w_j}{RS}, \quad (10)$$

where k_j is the number of ITI with the risk level j

z_j is the value of the significance function of the respective risk

w_j is the conditional weight of the respective level of risk

$RS = N \cdot k_3 \cdot w_3$, N is the number of the types of implemented ITI per threat model.

Additionally, the method suggests taking into consideration the designed level of CBCS protection that corresponds with its structural design and functional capabilities defined based on the additional indicators of Table 2.

Step. 7. Evaluation of the dynamics of the risk of CBCS protection disruption under ITI consists in the recalculation of the risk function, in which an additional coefficient is introduced that is based on the Weibull-Gnedenko distribution, which provides a dynamic CBCS protection estimate.

The dynamics of the risks of CBCS protection disruption under ITI is described with the fault (failure) rate function based on the Weibull-Gnedenko distribution function. The distribution density function is defined by formula (11), where α is the parameter of the shape of distribution that defines the nature of the risk dynamics throughout all life-cycle stages of the model (Figure 2), R_{BAS} is the parameter that defines the value of the basic risk coefficient of the distribution function

$$f(t_{LC}) = \frac{at^{a-1} e^{-\left(\frac{t_{LC}}{R_{BAS}}\right)^a}}{R_{BAS}}. \quad (11)$$

The values of the Weibull-Gnedenko distribution function are concentrated on the semiaxis from 0 to infinity. For experimental research of the dynamics of the risks of CBCS protection disruption under diverse and massive ITI and minimization of testing let us introduce a shift coefficient and use the hypothesis of the three-parameter Weibull-Gnedenko distribution, as well as the concept of risk function [4].

The function of the dynamics of assessment of the risk of CBCS protection disruption is developed out if the three-parameter distribution. The result of the transformations is given in (12). In order to obtain the function of the dynamics of the risk of CBCS protection disruption $R_{DYN}(t_{LC})$, the shift parameter must be taken into consideration that is defined based on the results of simulation and enables the correct shape of the risk dynamics for each type of CBCS. The function's behaviour is defined by (14)

Table 2. Additional indicators that characterize the designed protection of CBCS

Structural and functional characteristics of CBCS	Designed level of CBCS protection		
	High	Medium	Low
Based on the type of interaction between CBCS levels: - autonomous, no interlevel interaction, interaction is unidirectional (to the upper level) - bidirectional interaction.	3	2	-
Based on the input-output interface design: - local physical (electrical) interfaces - communication interfaces are used; they are physically separated from other network segments - common communication environment.	3	2	1
CBCS firmware replacement tools - absent - available, local connection required - remote control enabled.	3	2	1
Based on the inbuilt CBCS supervision and self-diagnostics tools: - absent - fault (failure) identification available - fault (failure) identification, operability recovery and functional redundancy facilities available.	3	2	1

$$R_{DYN}(t_{LC}) = \frac{a_k (t_{LC} - t_k)^{(a_k - 1)}}{\left(\frac{1}{R_{BAS}}\right)^{a_k}}, \quad k \in [1, 2, 3]. \qquad (12)$$

The values of index t_k are different for different lifecycle stages of the model (Figure 2). In [3], their generation is described in detail. The standard form of the risk dynamics curve will be defined by three model components, for each of which their own coefficient values are selected by means of simulation. The basic conditions are given in (13)

$$a_k : \{k = 1 : 0 < a_k < 1 \{k = 2 : a_k = 1,$$

$$t_k : \{k = 1 : t_k = 0 \{k = 2 : t_k = 0, \qquad (13)$$

$$R_{DYN}(t_{LC}) : \{a = 1 : R_{DYN}(t) = Const \{a > 1 : R_{DYN}(t) \uparrow. \qquad (14)$$

Graphical estimation and prediction of the evolution of the function of the dynamics of risk assessment of CBCS protection disruption under ITI based on the Weibull-Gnedenko distribution is shown in Figure 2.

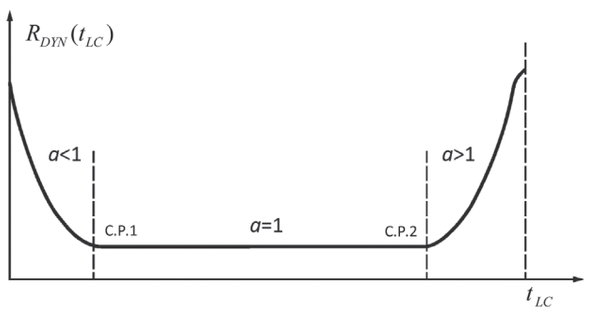

Figure 2. Standard form of the risk dynamics function

Risk dynamics (first stage, before characteristic point c.p.1) is defined by an increased level of risk due to the beginning of system operation and the following potential threats:

- fault (failure) of new version of software
- introduction of potential vulnerability in the new version of software and hardware
- insufficiently debugged information interaction between CBCS software and hardware facilities in the course of CC.

At the same time, the risk of CBCS protection disruption decreases over time due to CBCS software updates (patches), as well as improvement of the algorithms of control programs subject to the evolution of ITI threat model.

In Figure 2, risk dynamics $R_{DYN}(t_{LC})$ between two characteristic points c.p.1 and c.p.2 (second stage) are linear and correspond to the basic level of risk obtained by means of statistical estimation (10-12). This section corresponds to normal operation of a debugged system, when the patches are released regularly and the CBCS control algorithms have been debugged.

Within section after characteristic point c.p.2 (third stage) shows an even increase of the level of risk, which is both due to the possible decrease of hardware dependability, and accumulation of non-eliminated errors in software caused by zero-day ITI. Dynamic correction of risk $R_{DYN}(t_{LC})$ (formula (14) was generated is such a way as within the section between the points c.p.1 and c.p.2 (second stage) it has the value equal to one.

For a real CBCS, parameters $R_{DYN}(t_{LC})$ must be specified subject to the specificity of the system and the control cycle supervised by CADPS sensors. In the case of maximum possible compliance with the designed CBCS protection, the risk of protection disruption will be minimal. The adjustment of the value of the risk of protection disruption will be done based on the results of testbed experimental research under various ITI, as well as subject to risk dynamics over the control system lifecycle based on the risk function.

Conclusion. The proposed method of assessment of the protection of CBCS of critical information facilities enables numerical statistical and dynamic estimation of the risk of disruption of such system's protection under an intruder's ITI. The scientific novelty of the proposed method consists in the development of the model of CBCS operation under ITI based on augmented Petri nets and mathematics for the definition of the risk function of CBCS protection disruption using the Weibull-Gnedenko distribution.

The authors express their gratitude to Prof. I.B. Shubinsky for his assistance in the estimation of the integral risk of disruption of information protection of a control system.

References

[1]. Klimov SM, Kupin SV, Kupin DS. Models of malicious software and fault tolerance of information communication networks. Dependability 2017;4:36-43. DOI: 10.21683/1729-2640-2017-17-4

[2]. Collective of authors. «Umnye» sredy, «umnye» sistemy, «umnye» proizvodstva: seriya dokladov (seriya zelenykh knig) v ramkakh proekta «Promyshlennyy i tekhnologicheskiy forsayt Rossiyskoy Federatsii» ["Smart" environments, "smart" systems, "smart" plants: a series of reports (a series of green books) as part of the project Industrial and technological foresight of the Russian Federation]. Saint Petersburg: Center for Strategic Research North-West; 2012 [in Russian].

[3]. GOST R 50779.27-2017. Statistical methods. Weibull distribution. Data analysis [in Russian].

[4]. Kapur K, Lamberson L. Reliability in Engineering Design. Moscow: Mir; 1980.

[5]. Klimov SM, Astrakhov AV, Sychiov MP. Metodicheskie osnovy protivodeystvia kompiuternim atakam [Basic methods of computer attack response]. Moscow: Bauman MSTU; 2013 [in Russian].

[6]. Klimov SM, Astrakhov AV, Sychiov MP. Tekhologicheskiye osnovy protivodeystvia kompiuternim atakam

[Basic processes of computer attack response]. Moscow: Bauman MSTU; 2013 [in Russian].

[7]. Shubinsky IB. Nadiozhnie otkazoustoychivie informatsionnie sistemy. Metody sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016 [in Russian].

[8]. GOST R 56546-2015. Information protection. Vulnerabilities in information systems. The classification of vulnerabilities in information systems [in Russian].

[9]. Klimov SM, Kotyashev NN. Method of risk management for automated systems under conditions of cyber attacks. Dependability 2013;2:101-107 [in Russian].

[10]. Antonov SG, Klimov SM. Method for risk evaluation of functional instability of hardware and software systems under external information technology interference. Dependability 2017;17(1):32-39.

[11]. Klimov SM, Polovnikov AYu, Sergeev AP. A model of function-level fault tolerance of navigation signals provision processes in adverse conditions. Dependability 2017;17(2):41-47.

[12]. Klimov SM, Polikarpov SV, Fedchenko AV. Method of increasing fault tolerance of satellite communication networks under information technology interference. Dependability 2017:17(3):32-40.

[13]. Gapanovich VA, Shubinsky IB, Zamyshliaev AM. Risk assessment of a system with diverse elements. Dependability 2016;16(2):49-53.

[14]. Gapanovich VA, Rozenberg EN, Shubinsky IB. Some concepts of fail-safety and cyber protection of control systems. Dependability 2014;2:88-94 [in Russian].

About the authors

Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4-th Central Research and Design Institute of the Ministry of Defence of Russia, e-mail: klimov.serg2012@yandex.ru

Yuri V. Sosnovsky, Candidate of Engineering, Senior Lecturer, Department of Computer Engineering and Modeling, Physics and Technology Institute, V.I. Vernadsky Crimean Federal University, e-mail: yuri.sosnovskij@yandex.ru

Received on 23.08.2018