Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2017, 51 (123), 95–100
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/236

Received: 17.03.2017
Accepted: 30.08.2017
Published: 15.09.2017

A method of determining influencing parameters and predicting random, critical events in complex technical objects

Jerzy Korostil

Maritime University of Szczecin
1–2 Wały Chrobrego St., 70-500 Szczecin, Poland
e-mail: j.korostil@am.szczecin.pl

Key words: model, prediction, random event, attack, critical event, catastrophe

Abstract

A method of predicting the influence random events on the critical functionality of an object is discussed. Research is performed regarding the possibility of extending a prediction model to a prediction system by functionally uniting this model with additional models or recognizing the type of influence of a random event on a complex technical object. The proposed solution is importatnt because executing a prediction system instead of a prediction model allows one to detect critical situations that, when influencing technical objects, can result in the catastrophic loss of functionality of the corresponding objects.

Introduction

Critical random events Vp_i^K, that occur, alongside non-critical random events, that influence complex technical objects (*CTO*) and can result in catastrophic events or system failures ($\mathcal{K}a_i$). ($\mathcal{K}a_i$). Predicting the occurrence of various random events Vp_i instead of only Vp_i^K could fail to ensure the necessary accuracy in all cases. This inaccuracy results from calculation uncertainties that are intrinsic to the data used, the choice of the prediction model, and other considered and unconsidered random event inputs.

Assume that critical random events (CRE) that can lead to catastrophic situations occur quite rarely. To distinguish from the concept of rare events defined along with introducing the Poisson distribution function, critical random events will be called super-rare random events.

Occurrence of rare and super-rare events is typical for slow or super-slow processes. Examples of such processes are economic processes, processes that represent changes in social environments, processes of ecologic changes caused by natural factors and others. The concepts of rare and super-rare events will be related to the time parameter and the measurement scale for this parameter. In order to predict events that can occur during these processes, non-linear prediction models are used, examples of which can be logistic models, equipotential models and so on (Anderson, 1982).

The occurrence of critical random events relating to technological processes (TP_i) will be considered a super-rare event because they result in catastrophic situations in these TP_i. It would be incorrect not to consider events that cause catastrophic situations during the super-rare events, because in this case *CTO* with the corresponding TP_i could not function according to the specified requirements. We will assume the equivalence of concepts regarding a critical super-rare event Vp_i^K and a catastrophic situation $\mathcal{K}a_i$ that occurs in CTO_i. A prediction in most cases is implemented in time, so time as an variable of the function used in the prediction model $M(PG_i)$.

For the purposes of this article the following terms are defined:

Definition 1. A time interval Δt_i between the moment of occurrence of a predicted event t_i and the

moment of finishing the prediction process τ_i will be called a prediction interval: $\Delta t_i = t_i - \tau_i$.

Let us consider the possibility of using non-linear models for predicting events of Vp_i^K type.

Occurrence of Vp_i^K is influenced on by a series of factors that are identified by single symbol $\mathcal{X}_i$. A set of these factors sums up to a danger Nb_i that causes the occurrence of Vp_i^K. Because, in many cases, it is difficult to build a model Nb_i that could describe correlations between single factors $\{\mathcal{X}_1,\ldots,\mathcal{X}_n\}$ and, if it is known that these factors influence the occurrence of Vp_i^K, then, with some approximation, we can assume that the corresponding factors are independent from each other. Each single factor $\mathcal{X}_i$ will be considered a time function $\mathcal{X}_i(t)$. Each factor that leads to the occurrence of a random event, causes the occurrence of Vp_i^K to a degree defined by a proportionality coefficient β_i. Any object of CTO_i has its basic degree of a safety level μ_0.

Given conditions correspond to requirements relating to the use of non-linear prediction models that use exponential dependences. Due to random events of Vp_i^K type that lead to $\mathcal{K}a_i(CTO)$ catastrophic situations that are super-rare, using an exponential dependence of a dependent variable from an argument, which in this case is time t, allows to approximate the time scale of an extra large interval. This makes it possible to speak about the occurrence of a CRE of type Vp_i^K . An example of this type of model, widely used in various branches of science, are the Cox prediction models (Korolyov, 1998).

Interpretation of the corresponding random events Vp_i lies in considering each random event Vp_i that influences CTO_i a corresponding attack At_i on CTO_i (Korostil, 2016). This interpretation of Vp_i random events is reasonable because random events Vp_iinfluence on CTO_i by activating some attack process $Pr_i(At_i)$, implemented in CTO_i, and is a process of influence of an attack At_i. Because the attack event At_i is activates in the CTO_i, $Pr_i(At_i)$ the attack process can be described on the basis of using components and corresponding parameters of the CTO_i object. This description can be considered an attack model, written as follows:

$$M(At_i) = [M(Pr_i(At_i))\&M_i^{\varphi}(CTO_i)] \qquad (1)$$

where $M_i^{\varphi}(CTO_i)$ is a model of a single CTO_i fragment that takes part in the attack process $Pr_i(At_i)$. This allows for the follow transformation to occur when the random event occurs:

$$Vp_i \rightarrow [At_i(CTO_i) \rightarrow M(At_i)] \qquad (2)$$

Features of tasks of predicting critical events

According to classification of Vp_i, just among Vp_i^N it is possible for Vp_i^K and, respectively, At_i^Kattack to occur, which leads to occurrence of system failure defined as $\mathcal{K}a_i(CTO_i)$. Corresponding to the relation (2) we can assume that Vp_i^N and Vp_i^K are equivalent to attacks At_i^N and At_i^K. Because attacks can be described by a large number of parameters comparing to the number of parameters usable for describing random events, formulations that regard random events will be correct regarding attacks and vice versa. Thus it is relatively easy to perform analysis of attacks instead of random events. The number of parameters that can be used to describe attacks is larger than the number of parameters that describe the corresponding random events because any attack implemented in CTO_i uses a threat (Zg_i), placed in CTO_i and during its development an attack can extend the range of CTO_i parameters that At_i can use.

An occurrence of a single Vp_i^K is only possible when a single Vp_i^N appears with intensity not less than a given value and the corresponding events are different from each other. This condition can also be related to attacks At_i^N. If it turns out in practice that the same event Vp_i^K can use different threats, thus generating attacks different from each other, let us assume that this Vp_i^K has hidden parameters that cause the possibility to use different $Zg_i \in CTO_i$. For the purposes of this article the following terms are defined:

Definition 2. A critical number $q_i(At_i^N)$ of various attacks At_i^N is defined as the number of attacks of type At_i^K that occurs, resulting in $\mathcal{K}a_i(CTO_i)$.

Definition 3. A critical number $q_i(At_i^N)$ of various attacks At_i^N is a random number, and its possible values are given by a certain number interval that is defined as $Q_i = \{q_{i1}(At_i^N),\ldots,q_{in}(At_i^N)\}$.

Despite the fact there is no sufficient information regarding the danger Nb_i that generates random events Vp_i, the number of random unexpected events Vp_i^N is limited. This is demonstrated in the following proof.

Statement 1. In case of unlimited number of Vp_i that Nb_i can generate, or $Nb_i \rightarrow Vp_i \rightarrow N(Vp_i) \rightarrow \infty$, the number of events Vp_i^K, or attacks At_i^K is limited, which means the following relation is true:

$$\left[\sum_{i=1}^{m} Sg\left[At_i^K\left(CTO_i\right)\right] = m\right]\&\left[m << N\right]$$

where:

$$\left\{\left\{\left[A_i^K\left(CTO_i\right)\right] \neq 0\right\} \rightarrow \left\{Sg\left[At_i^K\left(CTO_i\right)\right] = 1\right\}\right\}$$
$$\&\left\{\left\{\left[A_i^K\left(CTO_i\right)\right] = 0\right\} \rightarrow \left\{Sg\left[At_i^K\left(CTO_i\right)\right] = 0\right\}\right\}.$$

Let us assume this statement is not true. Then the number of At_i^K can increase up to infinity, or $m(At_i^K) \rightarrow \infty$. Each attack At_i^K is described by a model $M(At_i^K)$, that is a synthesis $M(Pr_i(At_i))\&M_i^{\varphi}(CTO_i)$, where $M_i^{\varphi}(CTO_i)$ is $Pr_i^{\varphi}[Pr_i(CTO_i)]$. Since the number of fragments $\varphi_i(CTO_i)$ of CTO_i structure is limited, for an arbitrary object of CTO_i type has finite structure, then the number $Pr_i^{\varphi}[Pr_i(CTO_i)]$ is limited as well. This leads to the fact that the number of $At_i^K(CTO_i)$ is limited too, because $M(At_i^K) = \{M(At_i^K)$ & $M_i^{\varphi}(CTO_i)\}$, and $M_i^{\varphi}(CTO_i) = Pr_i^{\varphi}[Pr_i(CTO_i)]$. This means that in the case where $Nb_i \rightarrow Vp_i \rightarrow N(Vp_i) \rightarrow \infty$, and the number $Sg[At_i^K(CTO_i)] = m$ and $m << N(Vp_i)$, $N(Vp_i) - m = H$, where H is a number of random events Vp_i, that either cannot influence CTO_i or are related to Vp_j that can be withstood by a safety system $SB(CTO_i)$. Correctness of the relation $Nb_i \rightarrow Vp_i \rightarrow N(Vp_i) \rightarrow \infty$ is based on the fact that Nb_i can extend its possibilities of generating various Vp_i by extending or modifying its functional possibilities regardless of single CTO_i.

A model, oriented towards solving the task of predicting the occurrence of a certain event Vp_i that activates an attack At_i, is related to a certain threat $Zg_i(CTO_i)$ of the corresponding CTO_i object. A threat $Zg_i(CTO_i)$ is an important object parameter and, in general, is independent from Nb_i and attacks At_i, and can be used for activating attacks. This leads to the conclusion that the number of attacks that can be activated in CTO_i by events Vp_i depends on the number of threats existing in CTO_i. Due to the number of attacks of type At_i^K and, respectively, events of $\mathcal{K}_i(CTO_i)$ depend on the number of attacks of At_i^N type, their number depends on the number of attacks of type At_i. The number of threats of a corresponding type that would correlate to all possible attacks At_i^N is absent in the corresponding CTO_i so the number of attacks of type At_i^K that can lead to $\mathcal{K}_i(CTO_i)$ is lower. In this case, in the task of building such a prediction model that belongs to a certain model class and can consider the decrease of the general number of events among which one would have to be predicted during a given time interval Δt_i.

According to the theory of time series, concepts of trends of probable events are introduced and are described by certain functions with time variable t as an argument (Andersen, 1976). Using these concepts leads to certain prediction models, which can lead to additional modifications of general prediction models, including those involving exponentials.

An important factor that affecst prediction adequacy is input data, on the basis of which calculations performed by the corresponding model are implemented. The input data allows for the detection of the possibility of occurrence of a certain event in a time interval Δt_i. A source of data is a certain dangerous event that generated the corresponding data. Interpretation of the corresponding random event Vp_i has to be closely related to the interpretation of the corresponding data. So, functional possibilities $M(PG_i)$ have to approximate processes that generate data $\mathcal{X}_i(t)$. This means that, in a perfect case, functional possibilities $M(PG_i)$ have to be close to the model of $\mathcal{X}_i(t)$ data source, which in this case is Nb_i. If we assume that Nb_i generates some factors characterized by data $\mathcal{X}_i(t)$ in order to affect CTO_i, the model $M(PG_i)$ can be interpreted as a certain approximation to an unknown functioning model Nb_i, or $M(Nb_i)$. This means that a model $M(PG_i)$ can be built so that on the basis of immediate data $\mathcal{X}_{i+k}(t)$, a random event Vp_i and a given interval Δt_i would make it possible to modify $M(PG_i)$ so that it is closer to the functioning model of Nb_i, or to $M[Pr_i(Nb_i)]$. Where $Pr_i(Nb_i)$ are functioning processes of Nb_i. In general, the following relation can be written:

$$\Phi[\mathcal{X}_i(\delta t_i)\&Vp_i(\mathcal{X}_i(\delta t_i + \Delta t_i))] \rightarrow [M(PG_i) \rightarrow M[F(Nb_i)]].$$

In this case, the task of building a model $M(PG_i)$ so that, if possible, $M(PG_i)$ would approximate $M(Nb_i)$ with the highest accuracy possible (Vazirani, 2004).

The process of building a certain $M(PG_i)$, within this approach, is not finished at the stage of forming the initial version of a model $M(PG_i)$. During the process of operation of a safety system $SB_i(CTO_i)$, within which a model $M(PG_i)$ is used and analysis of data $\mathcal{X}_i(t)$ and Vp_i is performed, the task of of modifying $M(PG_i)$ so that at single steps of using prediction data it would be possible to implement such a modification $M(PG_i)$. When the following relation is true: $M(PG_i) \rightarrow M[F(Nb_i)]$, would leads to the following relation: $M(PG_i) = M[F(Nb_i)$.

Analysis of processes of occurrence of critical random events

Random processes $\mathcal{X}_i(t)$ relating the analysis performed are assumed to be independent and values of their influence on the occurrence of a certain random event Vp_i are assumed proportional to a certain constant value β_i. Actually, the value of their influence on the process of Vp_i occurrences can change during the prediction interval Δt_i, which can increase up to the ΔT_i value depending on the type of prediction model and on the nature of the random processes $\mathcal{X}_i(t)$.

To take into account this feature of random processes, approximating these processes on Δt_i interval must be accomplished.

In order for a random event Vp_i to occur as a result of certain set of random processes $\{\mathcal{X}_1(t),\ldots,\mathcal{X}_k(t)\}$ interacting with each other, it is necessary that during Δt_i functions $\{[\mathcal{Y}_1 = f(\mathcal{X}_1)],\ldots,[\mathcal{Y}_k = f(\mathcal{X}_k)]\}$ possess certain values. In case of events Vp_i, affecting technical objects of CTO_i type, functions $\mathcal{Y}_1 = f(\mathcal{X}_1)$ can be related to various sources of their occurrence, which are dangers $\mathcal{N}b = \{Nb_1,\ldots,Nb_m\}$. The corresponding Nb_i from $\mathcal{N}b$ differ from each other, which leads to the possibility to distinguish single $\mathcal{Y}_i = f(\mathcal{X}_i)$. When single $\mathcal{Y}_i$ reach certain values y_i^* and a certain event Vp_i occurs, it does not always mean the possibility for the corresponding Vp_i to affect CTO_i. In order for Vp_i to be able to activate the corresponding attack At_i at CTO_i, it is necessary for CTO_i to be characterized by a certain threat $Zg_i(CTO_i)$, that can be used by Nb_i and, respectively, Vp_i. Activating an attack At_i can be written as the following relation:

$$Nb_i(CTO_i) \rightarrow \mathcal{Y}_i(\mathcal{X}_i) \rightarrow Vp_i \rightarrow At_i \rightarrow [Ne_i(CTO_i) \vee \mathcal{K}a_i(CTO_i)] \quad (3)$$

where $Ne_i(CTO_i)$ is a malfunction that occurs because of the influence of At_i, $\mathcal{K}a_i(CTO_i)$ is a catastrophic event that can occur in cases when $Ne_i(CTO_i)$ is an unexpected malfunction $Ne_i^N(CTO_i)$. In the given relation $Nb_i(CTO_i)$ is used. This means that Nb_i has some information regarding CTO_i and can use it to organize a certain influence on CTO_i. This situation is possible regarding CTO_i and, in this case, $Nb_i(CTO_i)$ is called not a danger, but an enemy of CTO_i. The given relation can be written in an extended form:

$$Nb_i \rightarrow \{[\mathcal{Y}_i(\mathcal{X}_i)]\&[\mathcal{Y}_i \geq b_i(\mathcal{Y}_i)]\} \rightarrow \rightarrow [Vp_i\&Zg_i(CTO_i)] \rightarrow At_i(CTO_i) \rightarrow \rightarrow [Ne_i(CTO_i) \vee \mathcal{K}a_i(CTO_i)] \quad (4)$$

In accordance with this relation, to implement an influence of Vp_i on CTO_i the two conjunctions $[\mathcal{Y}_i(\mathcal{X}_i)]$ & $[\mathcal{Y}_i \geq b_i(\mathcal{Y}_i)]$ and Vp_i & $Zg_i(CTO_i)$ have to possess the value "1", or to be true. In this case, the occurrence of an event Vp_i and the arise of a catastrophic a situation at CTO_i is caused by the following factors:

1. Nb_i generates functions $[\mathcal{Y}_1 = f(\mathcal{X}_1)],\ldots,[\mathcal{Y}_k = f(\mathcal{X}_k)]$.
2. Values $[[\mathcal{Y}_1 = f(\mathcal{X}_1)] \geq b_1(y_1)],\ldots,[[\mathcal{Y}_k = f(\mathcal{X}_k)] \geq b_k(y_k)]$.
3. $(Vp_i\&Zg_i) \rightarrow At_i(CTO_i) \rightarrow \mathcal{K}a_i(CTO_i)$.

When building prediction models, an increase in prediction efficiency for a chosen model in most cases is based on using the most representative samples that ensure a certain degree of efficiency of a prediction process (Bidyuk, Romanenko & Timoshchuk, 2003).

Within the scope of this paper, the possibility of increasing the degree of prediction efficiency $\mu[M(PG_i)]$ at the expense of extending the model $M(PG_i)$ with components functionally related to it is researched. To ensure unambiguousness in the interpretation of this approach to increasing $\mu[M(PG_i)]$, let us consider the following initial condition.

Condition 1. A random event Vp_i, that activates an attack At_i in CTO_i, can lead to appearance of new threats Zg_i. Since the process of implementing the attack $Pr(At_i)$ is related not only to one initial component that is characterized by a threat Zg_i, but also to other components related to each other, including the initial component, which can be described as:

$$\{[Vp_i\&Zg(k_i)]\&(k_i \rightarrow k_j)]\} \rightarrow \{[Vp_i \rightarrow Pr_{i,r}(At_i(k_i)] \rightarrow [Pr_{i,(r+1)}(At_i(k_j)]\} \quad (5)$$

If $Pr_i(At_i)$ has finished successfully, the components $\{k_{ij},\ldots,k_{im}\}$ can be characterized by threats $\{Zg_{ij},\ldots,Zg_{im}\}$ because At_i uses these components in $Pr_i(At_i)$. In Nb_i, information is transferred via independent, separate channels regarding the success of At_i activated by an event Vp_i, which appeared because of Nb_i. A random event Vp_i, generated by a danger Nb_i, is characterized by a set of parameters $\{h_{i1},\ldots,h_{ik}\}$ that describe the type of Vp_i and, when activating At_i, define certain features of the corresponding attack. Examples of these parameters depend on the type of Nb_i and types of CTO_i components toward which the corresponding Vp_i and At_i are oriented. In cases when k_{ij} is an information system that is used in CTO_i and written as $IS(CTO_i)$, then Nb_i is also an information system that generates streams of packages directed into $IS(CTO_i)$. An example of information that is transferred in this stream can be viruses, intrusion programs that are activated in $IS(CTO_i)$. and so on (Rash et. al., 2005). When a danger Nb_i is a system of a physical influence on CTO_i, an example of Nb_i can be a tool system that can use the corresponding tools to physically affect CTO_i. A similar situation takes place when Nb_i is an object of a natural type.

Condition 2. When activating $Pr_i(At_i)$, fragments are used in CTO_i from $Pr_i(CTO_i) = \{pr_{i1}(k_{i1}) \rightarrow \ldots \rightarrow pr_{im}(k_{im})\}$ which lead to an increasing number of threats.

When predicting Vp_i^N and, respectively, At_i^N the following additional information should be considered:

- Information regarding an CTO_i object that a danger Nb_i possesses;
- Information regarding the attack goal $C_i(At_i^N)$, which is defined more accurately at each implementation step $C_i(At_i^N)$;
- Each random event Vp_i^N is characterized by a set of parameters $H(Vp_i) = \{h_{i1},\ldots,h_{ik}\}$, that are used at various implementation steps of $Pr_i(At_i)$.

Prediction systems and implementation of affecting the prediction parameters

One or more attacks on CTO_i are dangerous when CTO_i is vulnerable to an influence of Vp_i^N. This vulnerability means that in CTO_i there are certain threats $Zg_i(CTO_i)$ that allow an event Vp_i^N to activate the corresponding processes of attack implementation $Pr_i(At_i)$ in CTO_i. Threats Zg_i in CTO_i can exist since the building an object functional operation of an object. In the last case, threats as a result of incomplete and unsuccessful attacks and a decrease in the object's resource value.

It is only reasonable to perform an analysis on events that can have a negative influence on the CTO_i. Thus, it is natural to extend the prediction process by defining a degree of negativity of a possible Vp_i. The Vp_i and its respective At_i of this type belong to the class of unexpected Vp_i^N and At_i^N.

Since an attack, At_i^N, represents the last stage of activating the processes of a negative influence on CTO_i, we will discuss At_i^N. The first stage of a negative influence is an activation stage Vp_i^N that occurs in Nb_i. Information in Nb_i is formed as a result of implementing the procedures of data analysis regarding an CTO_i object. The data in most cases is outside of the object but can be obtained from the object itself. A danger Nb_i regarding CTO_i is an autonomous object. Thus, data about CTO_i stored in Nb_i can only be defined on the basis of analyzing parameters that characterize Vp_i^N. Considering this, besides identifying the moment of occurrence of the Vp_i^N, that is defined by a model $M(PG_i)$, it is reasonable to recognize an information image Im_i, that is implemented by a model $M(RIm_i)$. Implementation of a model $M(RIm_i)$ depends on Vp_i^N type. For example, if Vp_i^N is an information package that is transferred via Internet, then $H_i(Vp_i^N)$ is text and numeric information in single packages. In this case, $M(RIm_i)$ implements recognition of texts and numbers. If Vp_i^N is a weather change, the parameters $h_{ij} \in H_i$ can be changes in pressure, wind force, environment temperature and so on. The model $M(RIm_i)$, in this case, is a system of tools used to analyze the given parameters. For example, to determine the estimation of a storm weather value (Wiszniewski, 1989). So, the first extension of $M(PG_i)$ is a model $M(RIm_i)$. The next stage of implementing the influence of Nb_i on CTO_i is an activation of an attack At_i^N by the event Vp_i^N incorporating a threat Zg_i. This activation leads to the development of the process $Pr_i(At_i^N)$. This process is called an intrusion in information systems (Dudek, 2005). So, the next extension of the prediction model is a model of detecting intrusions $M(VIn_i)$ in the corresponding environment.

In this case, prediction lies not only in detecting a certain event Vp_i^N, but, aso in detecting a possible negative influence on CTO_i performed by an attack At_i^N. Based on the given extensions of the prediction model $M(PG_i)$ by models $M(RIm_i)$ and $M(VIn_i)$, some general prediction system is created:

$$SPG = F[M(PG_i), M(RIm_i), M(VIn_i)] \qquad (6)$$

There can be situations when *SPG* will consist of a larger number of components or other extensions that can be used in *SPG*. This means that the system *SPG* is different from a single prediction model $M(PG_i)$ because in *SPG*, besides the direct prediction, a set of processes is implemented that are related to the attacks At_i^N occurring and influencing the object. The prediction model by its very nature functions as an informer regarding the events Vp_i^N. The prediction system *SPG*, in addition to the functions of $M(PG_i)$, implement processes oriented towards determining the possibilities of a specific Vp_i^N on their influence on CTO_i and determining the possible counter-actions to the influence of attacks At_i^N, activated by events Vp_i^N. These factors extend the interpretation of determining the possibility of a negative influence of random events Vp_i^N and a danger Nb_i, as a whole, on the CTO_i object. Another aspect of interpretation of the given extensions regarding prediction concepts lies in the fact that, thanks to using the given extensions, the time interval of predicting Δt_i on the occurrence of a negative influence on CTO_i shortens. This change of the key prediction parameter occurs due to the fact that events of Vp_i^N type lose the status of a dangerous event that could become critical for CTO_i if $SB(CTO_i)$ neutralized the corresponding influence. Because of this, the following definition is introduced:

Definition 4. A functional prediction is a prediction within which a prediction model $M(PG_i)$ is

linked to other models that solve tasks closely related to predicting random events.

In the given case, the model used to detect threats Zg_i allows for the decrease in the number of events, including Vp_i^K, that are critical for the given CTO_i. The result of using $M(PG_i)$, that is the value Δt_i, is used to determine the period of monitoring the vulnerable elements of CTO_i. The model of recognizing an information image $M(RIm_i)$ that is formed on the basis of data about predicted events Vp_i^N and, respectively, about At_i^N that are described by parameters $H_i(Vp_i^N \vee At_i^N)$. This allows the model to make decisions regarding the need to check a single vulnerable component or a threat Zg_i during the process of CTO_i monitoring.

Additionally, in the *SPG* system a model of calculating the value of the current object resource $M(VR)$ is included. This can be considered a model of determining the functioning time of an object that still exists in CTO_i (Kolowrocki, 2004). This model is aimed at detecting new occurring vulnerable elements in CTO_i, that is caused by natural decrease of the value of an object resource and is caused by influence of attacks on CTO_i that occur during the operation process of CTO_i and influence of other factors that can lead to decrease of the resource value. Vulnerable elements of CTO_i that are detected can be turned into threats Zg_i. So, the model $M(VR)$ detects vulnerable elements that have to be modified in order to avoid turning this element into a new threat. It is known that extending the resource of CTO_i is ensured by the corresponding repair service. Thus, the results of the model $M(VR)$ are used to determine the extent of maintenance and system down time. Thanks to this, it is possible to avoid initializing the work that is performed when the corresponding CTO_i components fail.

Conclusions

A processes of predicting random events that are critical towards the CTO_i objects is researched. Analysis of critical events is performed and a set of features that define the corresponding events as critical status is reviewed.

To extend the possibilities of process of predicting critical events, research of a method of extending the prediction with processes that interact with the prediction is discussed. The recognition processes or the identification of a random event that is predicted, the process of detecting the possible implementation of a random event influencing CTO_i, and, a process of detecting changes of values of CTO_i resource is also reviewed. These processes, together with the prediction process, make up a prediction system that not only defines a random event related to CTO_i, but detects among them a critical event for CTO_i. This, in general, allows an interpretation of possibilities of a prediction system as a tool for predicting random critical events.

References

1. Andersen, T. (1976) *Statistic analysis of time series*. Moscow: Mir.
2. Anderson, J.A. (1982) Logistic discrimination. In: Krishnainh P.R., Kanal L.N. (eds), *Handbook of Statistics. Vol. II. Classification, Pattern Recognition and Reduction of Dimension*. North-Holland, pp. 169–191.
3. Bidyuk, P.I., Romanenko V.D. & Timoshchuk, O.L. (2003) *Analysis of numerical series*. Kyiv: NTTU "KPI".
4. Dudek, A. (2005) *Nie tylko wirusy. Haking, cracking, bezpieczeństwo Internet*. Gliwice: HELION.
5. Kolowrocki, K. (2004) *Reliability of Large System*. Amsterdam: Elsevier.
6. Korolyov, V.Y. (1998) About convergence of distributions of generalized Cox processes to stable laws. *Probability theory and its application* 43, 4, pp. 786–792.
7. Korostil, J. (2016) Features of protection of technical objects against negative exposure. *Measurement Automation Monitoring* 62, 7, pp. 234–237.
8. Rash, M., Orebaugh, A., Clark, G., Pinkard, B. & Babbin, J. (2005) *Zapobieganie i aktywne przeciwdziałanie intruzom*. Warszawa: MIKOM.
9. Vazirani, V.V. (2004) *Algorytmy aproksymacyjne*. Warszawa: WNT.
10. Wiszniewski, B. (1989) *Pogodowe prowadzenie statków przez ośrodki lądowe*. Szczecin: WSM.