Scientific Journals
Maritime University of Szczecin

Zeszyty Naukowe
Akademia Morska w Szczecinie

2012, 29(101) pp. 76–80

2012, 29(101) s. 76–80

Calculation of dangerous technical objects' safety level

Określanie poziomu bezpieczeństwa niebezpiecznych obiektów technicznych

Jurii Korostil

Maritime University of Szczecin, Institute of Marine Technology
Akademia Morska w Szczecinie, Instytut Technologii Morskich
70-500 Szczecin, ul. Wały Chrobrego 1/2, e-mail: j.korostil@am.szczecin.pl

Key words: risk, model, genetic, resource, danger, threat

Abstract

Research of problem of general safety level determination of complicated technical object, affected by a number of negative factors of different nature, decreasing the safety level technological object were conducted. The general model for calculation current values safety level consists of basis genetic conversions. Due to use of genetic models to determine come components of safety value of technical object it is possible to calculate impact of various factors which determine change of main components of safety value. Due to use of service functions the relevant influence of factors of different nature can be described according to logic of those factors.

Słowa kluczowe: ryzyko, model, genetyczne, resurs, bezpieczeństwo, zagrożenie

Abstrakt

W artykule przeprowadzono badania poziomu bezpieczeństwa skomplikowanych technicznych obiektów, na które działają negatywne czynniki różnej natury, zmniejszające poziom ich bezpieczeństwa technicznego. Ogólny model obliczeń bieżącego poziomu bezpieczeństwa bazuje na genetycznych przekształceniach. Dzięki wykorzystaniu genetycznych modeli służących do określania składników bezpiecznej wartości obiektu technicznego, możliwe jest skalkulowanie różnych czynników, określających zmianę komponentów głównych czynników wartości bezpiecznej. Wykorzystując funkcje serwisowe, można określić relatywny wpływ różnych czynników w stosunku do logiki tych czynników.

Introduction

The size of dangerous technical object (TO) safety is preconditioned by a number of factors and relative to objects can only decrease during its functioning. Therefore, in technical diagnostic, to measure the amount of safety level decrease, the conception of TO performance resource is used [1, 2]. The TO resource, is generally defined by dominating components and proper parameters of those components, that describe their suitability for calculation the resources size. Domination, in that case, can be determined by functional load of TO components, or by its relative value. In that case, the size of resource Pr_i is considered to be the function time, during which the corresponding component and whole TO are affected by factors, decreasing the resources level. Such factors directly affect physical parameters, during TO function, that can be recorded as:

$$Pr(t) = f\ \{[pr_1(x_1), ..., pr_n(x_n)], t\} \tag{1}$$

Among factors x_i, which affect TO parameters, are factors caused by TO functioning process, and therefore are themselves periodical factors, completely defined by technological processes (TP). Therefore, resource amount can be represented as a periodical function from integral factor, distributed on dominating TO components:

$$Pr(t) = f\ [x, \varphi(t)] \tag{2}$$

where $\varphi(t)$ – relevant periodical function, period of which is determined by changes of amount of influence of x_i factors in determined time intervals Δt_i. Because TP, realized in TO is known, the relevant function $\varphi(t)$ and current meanings of x_i are also known. So, the value of TO safety level change, caused by the known technology factors influence, not only can be calculated, but also modeled.

Besides $Pr(t)$ resource to determine safety level, concept of R risk is used [3, 4]. This parameter is orientated on TO deterioration effects, when it is affected by accidental factors. Such factors are mostly external, and are mainly natural, or factors, supposed to be accidental. In this case, calculation of risk value consists of calculation of probability of safety level decrease depending on influence of relevant factors on TO. In case of complicated TO such accidental factors can be internal factors, arising in TO framework, particularly when service staff takes part in TP realization. For the objects, characterized by accidental factors domination, the example of risk calculation model can be known model [5]:

$$R(t) = r + ct - \sum_{i=1}^{N(t)} y_i \tag{3}$$

where $R(t)$ – current risk level, τ – initial risk level, c – coefficient, which characterize functioning of protection and restore measures, $N(t)$ – spot process of negative effect moments, y_i (i = 1,2,...) – value of risk increase in i moment of accidental negative factor influence. In further author will consider risk, as amount of relevant danger type. An example of objects, for which influence of accidental negative factors and negative influence of technologic factors are on close domination levels could be sea transport.

For objects, which characterized by functional distribution, for example, digital information systems, the approach to determine a value of functioning safety level is based on existing international standards, which determine a number of specific concepts [6, 7]. One of the key concepts is a safety profile, which determine a list of necessary means to counteract negative factors, which we will further call threats, implemented in attack form. This approach differs from previous because it has structured process of negative influence of relevant factor on TO. Structuring consists in extraction of following components that together implement negative action on TO, which are:

– danger,
– attack,
– threat,
– attack counteraction,
– attack effect.

Danger is a source of possible attacks, targeted on TO safety level decrease.

Attack is a process, implemented in framework of external means, directly connected to TO and also internal means of object, implementation of which brings to TO safety level decrease.

Threat is a mean, which is a component TO, or a functional possibility, that characterizes TO, using which by attack process allows changing TO safety level.

Attack counteraction is a process, implemented in TO framework, including relevant protection means, aimed to create conditions, prohibiting events of attack process.

Attack effect on TO is an amount of TO safety level decrease.

In framework of this approach, safety level is defined basing on determination of amount of adequate number and quality of protection means, included into TO, to relevant threats and their abilities. Defining safety level decrease in that case can be described as difference between losses caused by some protection mean absence, recommended by defined safety profile and full value of those means. As a full value author mean market value together with service value of the mean. In general, safety level, provided by use of some protection mean types can be represented in following way:

$$B = \sum_{i=1}^{n} \left(V_i^D - V_i^Z\right) k_i \tag{4}$$

where: V_i^D – data value, V_i^Z – relevant safety means value, k_i – correction coefficient.

In the framework of this safety type, decrease of which is caused by accidental factors, which are activated by threats in a way of system attacks. This circumstance is a key from the point of view of optimization of safety means use. Therefore, conditions of the standards can be used as starting data for protection system construction. Its further modification should be based on taking into account real attacks on relevant TO.

Resource parameters are considered regarding complex TO. The complex objects differ from simple objects, not depending on their size, number of components which is not less then determined threshold. If the dependence of their components will be taken in consideration, arising in functioning process, then it can accept that general for the whole TO resource parameter can be calculated more precisely basing on suggestion that meaning of factors, determining decrease of resource, are random.

The general model for calculation

Let's take that general indicator of TO safety decreases, but on some functioning periods this value can be restored to some level due to repairs, during which substitution of some parts takes place.

Lets extract three danger indicators: B^A, determined by quantity of successful attacks, B^Φ – determined by quantity of possible losses, measured relevant costs, B^R, measured by resources amount reserve. Let's take, that B^Φ depends of B^A and B^R. The amount of generalized current value of danger will be determined as generalized value of different danger types B^A, B^Φ and B^R.

$$B^I = \left(\alpha_1 B^A, \alpha_2 B^\Phi, \alpha_3 B^R\right)/3 \qquad (5)$$

where α_1, α_2, α_3 – coefficient of current importance of separate danger types. In process of functioning of safety system, importance coefficients change depending on speed of separate dangers changing according to correlation:

$$[v(B_i) > 0] \rightarrow \left[\alpha_i = \beta \cdot \frac{B_i(t+1) - B_i(t)}{\Delta t_i}\right] \qquad (6)$$

$$[v(B_i) \leq 0] \rightarrow \left[\alpha_i = \frac{B_i(t+1) - B_i(t)}{\beta\, \Delta t_i}\right] \qquad (7)$$

The general schema of genetic algorithm (GA) for calculation current values B^A, B^Φ and B^R is the same and consists of basis genetic conversions and general functions [8, 9]. For each separate case of GA implementation different types of organization of service functions will be used, as they are mostly dependent on peculiarities of the task objective field. As far as general schema of GA is linear with general reverse connection, so GA will be written as a consecutive points used in GA general schema.

GA general schema

1.1. Service function of selection of chromosome hr_i in population p_i is activated:

$$hr_{ij} = f_{1i}^M(p_i)$$

1.2. Mutation gene is selected from chromosome hr_i:

$$gn_{ij} = f_{2i}^M(hr_{ij})$$

1.3. Necessity to perform mutation $M(hr_{ij})$ is analyzed and in case of its confirmation is implemented $M(hr_{ij})$.

2.1. For operation of crossing $ch\left(hr_{ij}^1, hr_{ik}^1\right) \Rightarrow \left(hr_{ij}^2, hr_{ik}^2\right)$ are selected pair of chromosomes hr_{ij} and hr_{ik}:

$$cr_{ij}^2 = f_{1i}^{ch}(p_i); \quad cr_{ik}^2 = f_{1k}^{ch}(p_i)$$

2.2. Braking point hr_{ij} and hr_{ik} is selected:

$$k\left(hr_{ij} \,\&\, hr_{ik}\right) = hr^*\left(gn_{ij}, gn_{ij+1}\right)$$

2.3. Necessity of crossing $ch\left(hr_{ij}^1, hr_{ik}^1\right)$ is analyzed and in case of its confirmation $ch\left(hr_{ij}^1, hr_{ik}^1\right)$ is realized.

3.1. Signs λ of selection hr_{ij} from population p_i are determined.

3.2. Values: $\varphi(hr_{i1},...,hr_{in}) = \lambda_1,...,\lambda_n$ are calculated.

3.3. hr_{ij} are chosen for which $\lambda(hr_{ij}) \geq \lambda_{pr}$.

3.4. Forming:

$$p_{i+1} = \\ = \left[hr_{i+1,1},...,\lambda(hr_{ij}),...,\lambda(hr_{ik}),...,hr_{i+1,k+1},...,hr_{i+1,n}\right]$$

4.1. With the help of service function is determined amount of interval Δt_i between cycles, for which functioning of GA is delayed.

4.2. Control is transferred to point 1.1.

Let's consider interpretation of separate genes and chromosomes for each of tree systems.

Let's consider a case, when it talks about TO, relatively to which the existing dangers form attacks and TO is equipped with protection means. In the framework of hr_{ij} such number of genes is implemented, that correlates with number of attacks, which is defined by the following correlation:

$$\left\{At_i = \sum\nolimits_{k=0}^n At_{ik} - \sum\nolimits_{j=0}^m At_{ij}\right\} \rightarrow \left(At_i = gn_{ij}\right)$$

where At_{ij} –attack that was detected and eliminated by protection means, n – general number of attacks of type i, m – number of detected and eliminated attacks. Such interpretation of danger size takes into account results of the attacks made on TO. This means that the higher the number of successful attacks on TO, the higher is danger. Number of such genes can increase with detection of new types of attacks. This function is an extension of GA^A, formed basing on analysis of known attacks and new attacks on its basis. In current case author will not consider such subsystem. Every chromosome in population p_i represent number attacks and their state on some definite time lap τ. All chromosomes of single population p_i represent attacks on selected time lap, which is mainly determined by selected cycle of TO functioning. Such cycle with time lap Δt_i is determined basing on implementation interpretation of technology process TO.

In case, when representation of danger is taken from the point of view of losses, which may be caused by accident, when technological process (TP) can not be used or TP is used with lower performance for users of TO, so with participation of the user the amount of possible losses in the cas of use by them such TP is determined, or value V^{ui} is determined. If TP allows to service *m* users, let's take, that for one particle of time τ_i of implementation of TP *m* users can suffer losses, determined by following correlation:

$$V^u = \sum\nolimits_{i=1}^{m} V^{ui}$$

Value V^u is influenced not only by attacks, which are counted in GA^A, but also by quality systems user service internal integral characteristics TP and TO, for example, by reliability of TO components and other factors. Therefore, GA^A that takes into account such factors is not duplicating GA^A.

For user protection in TP framework protection means are used, which beside protection from external threats N_Z, in form of attacks, also used means protecting from internal factors, for example appropriate software and hardware protection means (Z_Z). Each of those means has its own value V_Z, which may vary depending on various factors, for example it can increase or decrease with time. Therefore, it makes sense to consider following correlation:

$$V^u \le V^Z \quad \text{and} \quad V^u > V^Z$$

It is evident, that protection means are used efficiently, if $V^u = V^Z$, but it is hard to reach. If $V^u < V^Z$ system suffers losses, as far as value of use Z_z is baseless. If $V^u > V^Z$ then user is under risk and can suffer losses due to insufficient user or his values protection level. Current values of genes gn_{ij} for GA^A can be determined in following way:

$$\left[\left(V_i^u - V_i^Z\right) \le 0\right] \to (gn = 0) \vee$$

$$\left[\left(V^u > V^Z\right) > 0\right] \to \left(gn = V_i^u - V_i^Z\right)$$

Number of genes in chromosome is equal to the number of users during one time lap τ_i. Number of chromosomes hr_{ij} in population p_i is equal to the number of time laps τ_i, in defined period Δt_i of TP functioning.

If safety concept is connected to user risk determined by resource amount, left in TO component, then the value of one gene can be determined in following way. If in TO the value of resource left for current time period is equal p_i, than it can suppose that user risk value is reciprocally proportional to the value resources left. This means that with increase of value of resources left the value of risk decreases. For value of resource of every TO is set threshold value d_i, which is taken as critical value of the resource. The critical value of the resource is set in such a way, that after TO reaches this threshold, there still exists possibility to safely finish the current routine cycle of TP. The value of relevant gene is set by the following correlation:

$$\left[(Pr > D) \to (gn = 0)\right] \vee \left[(Pr \le D) \to (gn = D - Z)\right]$$

where: *Pr* – current resource value, *D* – allowable threshold of resource value.

One chromosome looses as much genes, as much dedicated key components is in TO. Depending on component's value for safe TP implementation, the value of threshold, taking into account that value, is set. The higher is value of the component, the higher is threshold relatively to value of absolute minimum resource value [10].

Number of chromosomes is equal to number of elements of time laps τ_i to which period of cycle Δt_i of TP realization is broken. Separate populations p_i describe state of TO resource during time interval Δt_i.

According to accepted approximation, current safety level can be determined with formula (5). Coefficient of importance α_i increases if relevant risk increases and α_i decreases, if relevant risk decreases.

Conclusion

In the framework of the work experiments with the model were conducted, which describe processes of aging of boiler walls of power unit, which determine changes of its resource. As factors which play the key role in activation of aging process of boiler walls thermal loads, appearing in boiler walls and also tension of wall material were taken.

Processes of aging of boiler walls material where determined basing on analysis of metal structure change on the boiler surface and thermal loads were determined basing on temperature change dynamics of the boiler walls during one technological period of its use. Relevant experimental data received in work were compared to data, received from genetic model. Variance between data is 10% average, which can be caused by the fact that during experiment other factors influencing the material's resource, such as influence of environment, changes in fireproof internal covers of boiler construction etc. were not counted.

References

1. CHOLEWA W., KISIŃSKI J.: Diagnostyka techniczna. Odwrotne modele diagnostyczne. Wyd. Politechniki Śląskiej, Gliwice 1997.
2. CHIANG L.H., RUSSEL E.L., BRATA R.D.: Fault Detection and Diagnosis in Industrial System. Springer Verlag, London 2001.
3. BENING N.E.: Introduction in mathematic theory risk. M.: МАКС – Pres, 2000.
4. BEARD R.E., PENTIKAINEN I., PESSONEN E.: Risk Theory. Chapman and Hall, London 1978.
5. EMBRECHT P., KLUPPERBERG K.: Some aspects of insurance mathematics. Theory probability and her application. V. 38, (2), 1993, p. 375–416.
6. ISO/IEC 15 408 (1999) Information technology – Security techniques – Evaluation criteria for IT security.
7. ISO/IEC 9797-1:1999, Information technology – Security techniques – Message authentication codes (MACs) – Put 1: Mechanisms using a block cipher.
8. GOLDBERG D.E., KUO C.H.: Genetic algorithms in pipeline optimization. Journal of Computers in Civil Engineering, 1987, I(2), 128–141.
9. HOLLAND J.H.: Genetic algorithms and classifier systems: Foundations and future directions. Genetic algorithms and applications Proceeding of the Second International Conference on Genetic Algorithms, 1987, 82–89.
10. ARABAS J.: Wykłady z algorytmów ewolucyjnych. WNT, Warszawa 2001.

Other

11. CHIANG L.H., RUSSEL E.L., BRATZ R.P.: Fault Detection and Diagnosis in Industrial Systems. Springer Verlag, London 2001.