TECHNOLOGY, CREATIVITY, IMPLEMENTATION

SAFETY ASSESSMENT OF EMERGENCY SYSTEMS

Mykhailo Donchenko
Candidate of Technical Sciences, Associate Professor at the Department of Intelligent Information Systems, Petro Mohyla Black Sea National University, Ukraine
e-mail: mikhaildon@mksat.net, orcid.org/0000-0002-4084-3112

Summary

The issue of a technical system safety assessment is very important and at the same time is very difficult, since safety is one of the main criteria for the quality of any object as well as reliability and efficiency. Unfortunately, in most cases, safety is assessed only by compliance with specific standards or regulations. The presence of a quantitative assessment, and even better, the distribution of the assessment criterion, opens up a number of possibilities for its provision at all stages of the system life cycle: setting the optimal safety level at the design and manufacturing stages and keeping it at a sufficient level during the operation. At the same time, it is important to evaluate both the safety of the system itself and its negative impact on people and the environment. The paper proposes an attempt to assess the safety of the system, taking into account its reliability and the impact of external and internal factors on the system itself, on human health and the environment. The possibility of taking into account constructive, organizational and information safety systems is considered. It is proposed to determine the probability of a dangerous situation non-occurrence under the influence of hazardous factors and the presence of safety systems.

Keywords: safety, reliability, impact factors, emergency situation, systems protection.

DOI https://doi.org/10.23856/5327

1. Introduction

The functioning of any system is closely connected with the functioning of other surrounding systems. The interaction of such systems generates influences and causes certain changes, both physical and functional. If such changes lead to the forced threats to surrounding systems, people, environment, then the question of assessing how safe such a system is and how you can reduce the risks of its use arises. In any case, this problem must be considered comprehensively, taking into account the threatening effects on the system of its environment and, as a result, possible negative physical consequences for the system itself and efficiency of its functioning, as well as for people and the environment.

The vast majority of systems do not pose significant threats, therefore we will consider only those ones that can cause them or get into emergency situations. Since, because of the specifics of operation, it is impossible to avoid accidents completely, it is important to determine

the causes of their occurrence, to analyze their consequences and take into account while designing and operation in order to reduce or avoid them. In order to do this, it is necessary to analyze all possible interactions, destructive changes and consequences, evaluate them and search the ways to reduce them.

There is a large variety of different systems in the world: environmental, social, global, technical, etc., which is why we will consider only technical systems (TS), but a conceptual approach can be useful for other systems, taking into account their specifics.

2. System security assessment

Let us clarify the definition of safety and normal operation of TS. Security means the absence of unacceptable influences and changes that threaten the integrity of the system itself, human health or life, other systems and negative environmental changes. In fact, it is achieved during the normal operation of the TS.

To assess the level of security, it is necessary to take into account all possible risks in the operation of the system under conditions of multifactorial impact. In the most general case, the state of the system can be described with the following events:

A – there are no any threats and the system is functioning properly;

B – the internal state is normal, but there are external influences on the system, which can lead to system failures and even emergency situations (ES);

C – the internal state is normal, but there are external influences (in this case critical changes in operating conditions can be included), which can disable the system through physical action;

D – the internal condition is normal, but improper management or maintenance can lead to critical situations;

The occurrence of at least one or more of these events describes the state of the system. The described events can be considered as incompatible with a high probability. In this case the state of the system can be described by the sum of these events:

$$S=A+B+C+D$$

And the probability of the sum of events will be equal to the sum of their probabilities:

$$P\{S\} = P\{A\}+ P\{B\}+ P\{C\}+ P\{D\}.$$

Moreover, with a high probability we can assume that events A, B, C, D form a complete group of incompatible events. In this case, the sum of their probabilities is 1.

$$1= P\{A\}+ P\{B\}+ P\{C\}+ P\{D\}.$$

So, the probability that the system will function properly will be equal to:

$$P\{A\}=1- (P\{B\}+ P\{C\}+ P\{D\}),$$

in case when $P\{A\} = S(t)$ – is a distribution of the safety function;

$P\{B\} = F(t)$ – is a distribution of the probability of failure on (0, t);

$P\{C\}$; $P\{D\}$ – is a probability of critical situations in the event of the emergence of the appropriate threats.

Let us consider event B in more detail. For its implementing, the joint occurrence of two events are necessary:

- M – TS is functioning normally;
- H – a threat occurs which can lead to failure and an emergency.

Thus, event B will be equal to the product of events M and H: B = MH, and the probability P{B} will be equal to the product of the probabilities P{B} = P{M} * P{H}. Let us denote the probability of an emergency at (0, t) for event B as $V_b(t)$.The probability P{M} is a function of reliability TS by (0,t)–P(t)=[1-F(t)],and the probability P{H} – is a function of the distribution of the type B threat at (0, t): $Z_b(t)$. In this case the probability of a type B emergency will be equal to:

$$V_b(t)= P(t)*Z_b(t).$$

By analogy, let us write the distribution expression for events of type D

$$Vg(t)= P(t)*Zg(t).$$

Thus, the security function will take the form:

$$S(t)=1-[F(t)+V_b(t)+V_g(t)].$$

Let's plug the value

$$S(t)=1-\{F(t) + [\{1-(F(t)\}*Z_b(t)] + [\{1-(F(t)\}*Z_g(t)]\}.$$

The functioning of any system is closely connected with the functioning of other surrounding systems. The interaction of such systems generates influences and causes certain changes, both physical and functional. If such changes lead to the forced threats to surrounding systems, people, environment, the question of assessing how safe such a system is and how the risks of its use can be reduced arises. In any case, this problem must be considered comprehensively, taking into account threatening effects on the system of its environment and, as a result, possible negative physical consequences for the system itself and its efficiency, as well as for people and the environment.

Two options for assessing the safety of TS can be considered:

- without a system of protection against harmful influences (threats);
- taking into account protection systems.

Humanity has appreciated the need to protect TS long ago. Conventionally, they can be divided into:

- constructive and technological;
- organizational;
- informational.

Structural and technological measures are the development of such a design and manufacturing technology to counteract the main negative impacts that reduce safety. Such measures are used to ensure reliability, only for specified operating conditions. In fact, increasing reliability helps to increase security, but for the general conditions of TS using. However, constructive protection is aimed at counteracting the most dangerous factors which can cause an emergency. These factors are random and, by their nature, they can be both internal and external, and practically do not occur during normal functioning. And their action is extreme.

However, it should be noted that the constructive providing of security has its own characteristics, which depend on factors leading to dangerous situations and their consequences. Besides, it should be considered the specifics of the factors influence and the probability of their occurrence in operating conditions.

Since, as a rule,such a providing is usually associated with additional investments, taking into account the priorities of people protection, the product itself and everything related to it, as well as the environment, the best solution based on how severe the consequences of a possible emergency are should be searched.

Organizational protection is, first of all, the prevention of accidents for such reasons:

- unsatisfactory technical condition of products;
- getting into dangerous situations;
- reducing the impact of the "human factor".

Unsatisfactory technical condition of the product often leads to an emergency situation, such as a failure of the vehicle's braking system or inability to perform important functions in critical situations (loss of the vessel speed, especially during the storm or during the vessel's progress in bottlenecks).

Operation of the product may also be associated (due to specificity) with the possibility of getting into a situation that could provoke an accident. Such situations are accidental, but the probability of their occurrence, in many cases, can be predicted, and it can provide an opportunity to avoid a critical situation or prepare for it accordingly, which will significantly reduce its negative consequences. Information protection plays an important role in this aspect. With the advent of information systems, especially geographic information ones, there is a powerful opportunity for analyzing the operation of vehicles in a dynamic spatial information field, predicting changes, modeling emergencies, quick providing optimal solutions to such situations, providing urgently needed current information, warning of possible critical situations, etc. The combination of organizational and information protection can significantly reduce the negative impact of the "human factor" on the occurrence of emergencies.

In the presence of protection systems against adverse impacts it is necessary to take into account the extent to which they can counteract the threats in case of the adverse impact arises. In this case, it is important to assess the extent to which such a system is able to counteract the adverse factor when it occurs.

In the context of the emergence of constructive and organizational protection, safety is improved by counteracting negative factors, and the description of the states of the TS can be represented in this way:

- A – there are no threats and the system is functioning properly;
- B – the internal state is normal, but there are external influences that can lead to failures and critical situations;
- C – the internal state is normal, but there are external influences that can disable the system through a physical action;
- K – there is a powerful harmful external influence, which constructive protection does not cope with;
- L – there is a powerful harmful external influence of the "human factor" such that organizational protection does not work;

The events K and L emerged because the defense worked without no doubt, but to some extent. Failure of protection is real because of the fact that 100% protection is impossible, and even before that, its level is chosen optimally. Then the security function will take such a form:

$$P\{A\}=1-(P\{B\}+P\{C\}+P\{K\}+P\{L\}), \quad (1)$$

where $P\{A\} = S(t)$ – is a distribution of the safety function;

$P\{B\} = F(t)$ – is a distribution of the probability of failure;

$P\{C\}$ – is the probability of the occurrence of critical situations in case of threats;

$P\{K\}$; $P\{L\}$; –are the probability of protection failure in the event of strong threats.

Let's plug in (1) the corresponding probabilities, and then the security function will take the form:

$$S(t)=1-\{F(t) + [\{1-(F(t)\}*Z_{в}(t)] + [\{1-(F(t)\}*Z_{k}(t)*Z_{kmax}(t)] + \{1-(F(t)\}*Z_{l}(t)*Z_{lmax}(t)*\},$$

where F(t) – is the distribution of the probability of failure;

$Z_b(t)$ – is the probability distribution of the B type threat;

$Z_k(t)$ – is the probability distribution of the K type threat;

$Z_{kmax}(t)$ – is the probability distribution that the K type threat will be higher than the constructive protection;

$Z_l(t)$ – is the probability distribution of the L type threat;

$Z_{lmax}(t)$ – is the probability distribution that the L type threat will be higher than the organizational protection;

Reliability indicators are known and their definition is elaborated in detail. The probabilities of the threats occurrence and critical situations can be determined by simulation modeling, statistics of the occurrence of threats and accidents, or by the method of accelerated tests.

3. Conclusions

It is proposed the possibility of taking into account the reliability and protection systems when determining the safety assessment. The directions of assessment and possibilities of increasing the safety of the TS use are defined. A method for determining the distribution of the security function is proposed.

References

1. Aleksandrov M.N. (1983) Bezopasnost cheloveka na more [Human safety at sea]. L: Shipbuilding. (in Russian)

2. Venttsel E. S. (1972) Issledovanie operatsii [Operations research]. Moscow: Soviet radio. (in Russian)

3. Donchenko M. V., Kazariezov A. Ya. (2017) Pidvyshchennia bezpeky suden na bazi heoinformatsiinykh system [Ships safety improving based on the geographic information systems]. Naukovi pratsi [Scientific studies] (scientific journal), vol. 295, no. 307, pp. 36-41. Mykolaiv: BNU named after Petro Mohyla publication. (in Ukrainian)

4. Donchenko M. V., Kazariezov A. Ya. (2018) Vykorystannia heoinformatsiinykh system dlia rannoho vyiavlennia nadzvychainykh sytuatsii [Use of geographic information systems for early detection of emergencies]. Naukovi pratsi [Scientific studies] (scientific journal), vol. 308, no. 320 Kompiuterni tekhnolohii, pp. 31-37. Mykolaiv: BNU named after Petro Mohyla publication. (in Ukrainian)

5. Polovko A.M., Hurov S.V. (2006) Osnovy teorii nadezhnosti [Fundamentals of reliability theory]. Petersburg, 2 ed. (in Russian)