Gapanovich V.A., Rozenberg E.N., Shubinsky I.B.

SOME CONCEPTS OF FAIL-SAFETY AND CYBER PROTECTION OF CONTROL SYSTEMS

The paper provides some definition of a hazardous failure and fail-safety, discusses relations and principal differences between functional reliability and functional safety, and analyzes alternatives for ensuring fail-safety of control systems.
The paper considers major threats to cyber protection, ways of implementing cyber attacks, offers a concept of ensuring a guaranteed cyber protection level of control systems.

Keywords: *reliability, failure, hazardous failure, functional safety, fail-safety, cyber attack, cyber space, cyber protection.*

1. Fail-safety

According to [1], “a hazardous event is a situation potentially causing damage for a human being”. Of course, it applies not only to a human being but also to damages that can be caused for material assets or environment. Not every hazard always brings a threat. For that to happen, a causing event should take place. Afterward a threat can result in a chain of undesirable events that ultimately will lead to a hazardous event, to an accident. A hazardous state (event) is failed state of IT system objects when there occur unacceptably high risks of damages for the life and health of citizens, assets of persons and companies, state and municipal assets, environment, the life and health of animals and vegetation.

Therefore, safety is an absence of unacceptable risk. The risk is a combination of damage and probability of occurrence [2]. With consequences taken into account, we can separately consider:

a) functional reliability of a system if it performs its function (i.e. does not lose certain properties) in a chain of all those systems that are involved in implementing that function;

b) functional safety if consequences will not lead to unacceptable risks.

Fig. 1 shows that in terms of consequences functional reliability smoothly transits into functional safety if criticality of consequences increases. Hence it is clear that IT control systems whose failure rate in implementation of a function should not be higher than 10^{-6} 1 / hour can be treated in terms of functional safety [3]. Such systems are often called potentially hazardous systems. For such systems *a hazardous failure* is defined as an event resulting in transit of a system from good, operating or partially operating state into hazardous state.

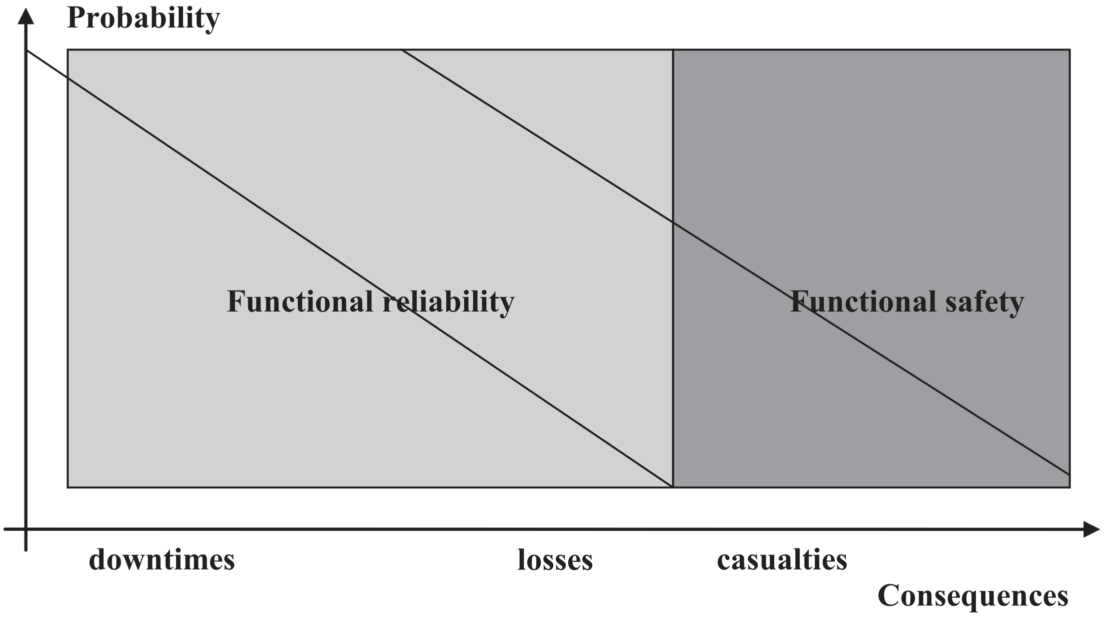

Fig. 1. Functional reliability and functional safety

Fail-safety is a control system’s ability to retain safe state and (or) to ensure the safety of controlling subordinate objects in case of hazardous failures of a system itself or its components.

The issue of ensuring the functional safety of control systems consists in eliminating the influence of their failures and faults on controlled objects and environment, i.e. eliminating the so-called hazardous failures (Fig. 2). Giving wrong commands can bring train crashes, tank leakage, explosions etc. It results to economical and ecological damages, casualties and even disasters.

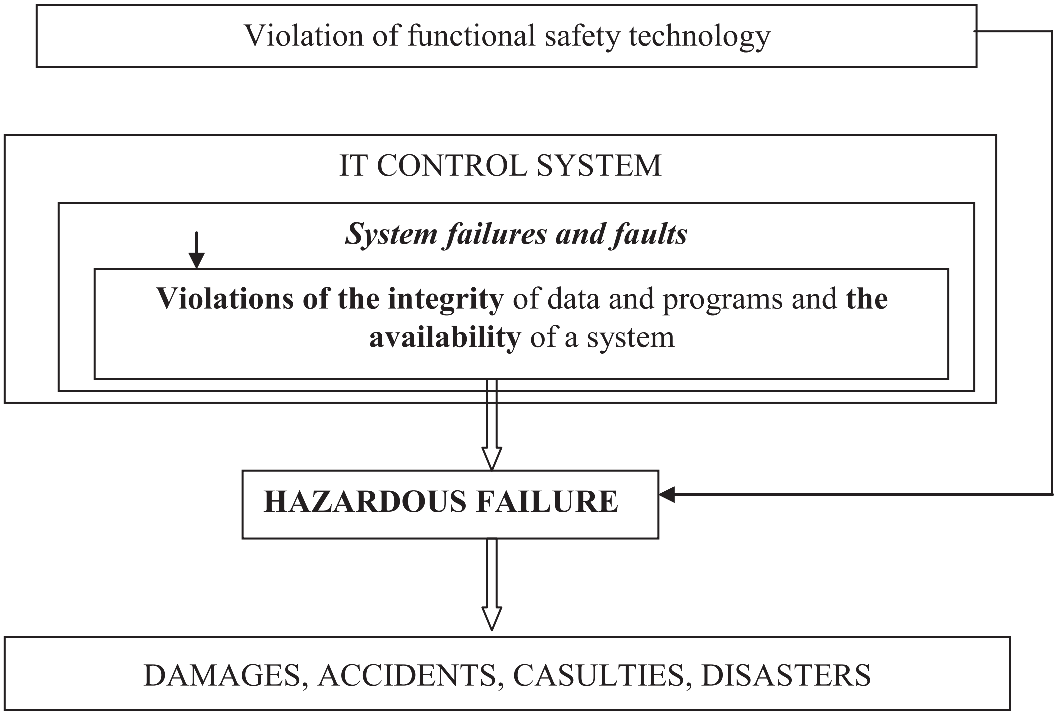
Violation of functional safety technology
IT CONTROL SYSTEM
System failures and faults
Violations of the integrity of data and programs and the availability of a system
HAZARDOUS FAILURE
DAMAGES, ACCIDENTS, CASULTIES, DISASTERS

Fig. 2. Threats to safety of IT control systems

In principle, we cannot entirely rule out the influence if failures and faults of systems on the environment since there is always some probability of such events happening. Our task is to achieve minimum values of such probabilities. One of the ways to achieve them is to ensure a high level of system reliability. However, the possibilities of radically increasing the reliability by means of technological, algorithmical, structural and other methods are limited, mainly due to unacceptable economical losses.

In terms of safety, there can be no other alternative than to stop a system's functioning or to decrease its capacity to predefined levels in case of unacceptable probabilities of a hazardous failure occurring in it. Hence, it is necessary to develop technologies of guaranteed and confident detection of system failures. If functional safety is ensured in a right way, then system hazardous states are duly identified and eliminated.

Hazardous states are effectively identified in IT systems by using detection technologies based on development of two, three and more control channels working in parallel. Parallel generation and comparison of commands secure detection of hazardous states provided that there are safe algorithms or comparing devices (so-called comparator circuits), independence of channels and data, unsymmetrical failures of channels ensured and other conditions satisfied. Yet, to implement this technology of failure detection, it is required to introduce an extra considerable amount of HW and SW into systems, thus reducing its reliability.

The above said leads to the following:

– the safety and the reliability of systems have principal differences: if unreliability leads to unaccepted levels of availability, maintenance, non-failure operation and maintenance costs, then insufficient safety leads to accidents and casualties;

– the objectives of ensuring the reliability and the functional safety of systems have contradictions that can be eliminated on the basis of some compromise, so the requirements for reliability and functional safety should be well balanced together;

– in safety critical, potentially hazardous objects, or objects presenting increased hazards, the tasks of safety ensuring are prioritized, while required level of reliability should specified with cost limits taken into account, after safety requirements have been implemented.

In order to ensure system fail-safety, we should go the same way that we go to ensure fault-tolerance, i.e. create conditions when a system is observable and controllable. Based on the principle of acceptability of a residual risk with existing financial limits taken into account, it is necessary to fully realize the possibilities of ensuring fault-tolerance and functional safety.

2. Cyber protection

The issue of fail-safety in control systems is closely related to the issues of their IT protection, above all, against cyber attacks. The term *cyber* is defined as "bearing a relation to IT technologies" [4]. IT technologies are implemented in the so-called *cyber space* that is understood as "environment created by means of physical and nonphysical components characterized by use of personal computers and electromagnetic band to store, change and exchange data via computer networks" [4]. Use of cybernetic capabilities aiming to implement some goals in cyber space or by means of cyber space is defined as *cyber operation*. Now we have come close to the definition of the term cyber attack. This is *cyber operation*, either offensive or defensive one that causes human damages or casualties, or damage to or destruction of objects.

Based on the above definitions, we can define **cyber protection as the ability of a system to successfully perform specified tasks under the conditions of cyber attacks aiming to make damage to safety critical or potentially hazardous objects, or objects presenting an increased threat for the life and health of citizens, assets of persons and companies, economy, environment.**

The main threats to cyber protection in IT control systems are as follows (Fig. 3):

- IT attacks (cyber attacks in the first place);
- Undocumented features of SW/HW;
- Failures and faults, including HW/SW errors and glitches, operator mistakes, data errors.

Fig. 2 shows that a system's cyber protection depends on unauthorized access capabilities of a potential attacker as well as on undocumented features that occur in HW and SW means. Unauthorized access is realized by means of information attacks (cyber attacks) at a system.

In theory, full elimination of hazardous failures in control systems is possible but in practice, it is not feasible as it will take expenditures much higher than expected damages due to hazardous failures. The most realistic way is to define an acceptable level of risks due to cyber attacks and to develop efficient protection against hazardous failures.

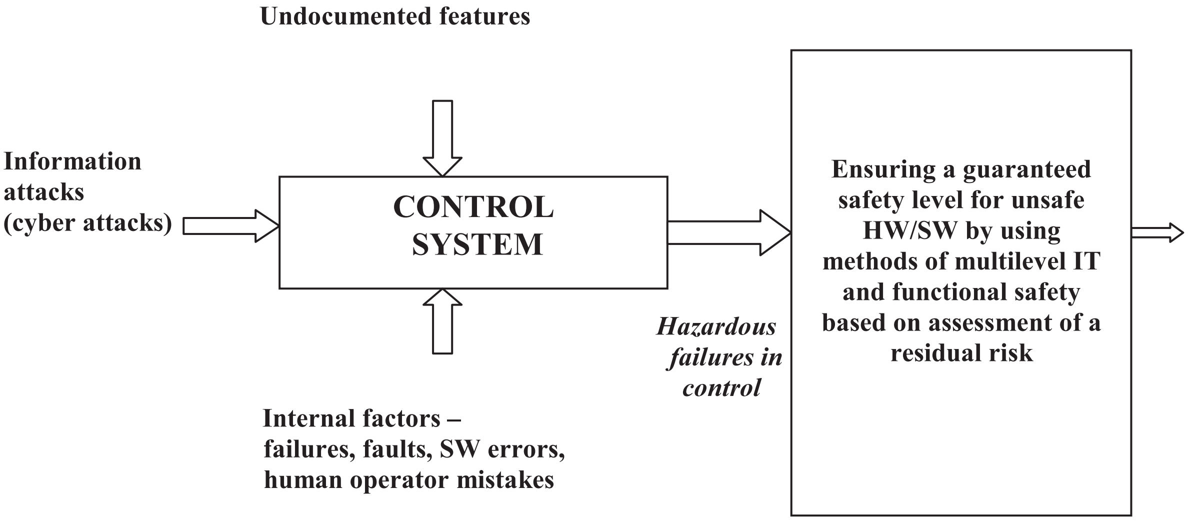
Undocumented features
Information attacks (cyber attacks)
CONTROL SYSTEM
Ensuring a guaranteed safety level for unsafe HW/SW by using methods of multilevel IT and functional safety based on assessment of a residual risk
Hazardous failures in control
Internal factors – failures, faults, SW errors, human operator mistakes

Fig. 3. The Concept of ensuring a guaranteed safety level of control systems

Let us consider the above listed threats in more detail.

A successful cyber attack can result in violations of information integrity or availability. An attack can target servers, personal. For implementation of cyber attacks, intruders often use specialized SW that provides automation for actions performed at different stages of an attack.

Generally, four stages can be identified in any cyber attack:

Reconnaissance. At this stage an introduer attempts to get as much information as possible about an attack object in order to plan further stages of intrusion on its basis. To this end he can target, for example, information about the type and version of an operating system, a list of users registered in the system, data about applied SW used in the system etc.

Intrusion. At this stage an intruder get an unauthorized access to those resources that are under attack.

Attack perpetration. At this stage an intruder realizes the goals that motivated the attacker, for example, violation of IT system operation, deletion or change of data etc. while doing this, an intruder often performs actions aiming at deletion of the traces of his presence in the system. Each attack is based on the fact that a control system has some vulnerabilities, and the "right" use of at least one of them opens the door for an intruder to the system.

Attack progression. After attack perpetration, an intruder aims to go to the stage of its further progression. To that end, he usually implants into a system some malicious program that helps to arrange an attack at some other nodes of an IT system. Major threats for IT system cyber protection are presented by the following groups of malicious programs: ***DoS attack*** (Denial of Service) that is an attack at an

IT system aiming at its failure, i.e. creating such conditions when legitimate (authorized) users cannot get an access to resources (servers) provided by the system or this access gets complicated. An “enemy” system’s failure can be one of the steps to get hold of a system (if SW generates some critical information in emergency – for example, version, part of a program code etc.); ***Trojan programs*** *when implemented into a system disrupt the integrity of information and programs or generate viruses in the system*. They can also collect information about user profiles stored on a PC, passwords and other confidential data with further sending it to intruders; ***programs of unauthorized control of information system PCs (****boot viruses, SW viruses, network viruses etc.)*

Undocumented features are HW and SW functional features not specified or not compliant with those described in specifications, whose application can cause violation of availability, integrity as well as confidentiality of processed information. For example, SW and HW bugs belong to undocumented features.

Implementation of the above listed threats results in hazardous failures that lead to unacceptable damages of objects, which in terms of an operating company belong to the category of objects with increased hazards or to the category of potentially hazardous objects, and in terms of state or regional authorities hazardous failures can cause unacceptable damages for critical infrastructure. The latter is explained by the fact that responsibility for critical infrastructure protection is put on state or regional authorities.

Threats of cyber protection violations are similar to threats of fail-safety violations. A principal difference is that cyber attacks are a specific class of information attacks aiming at damaging or destructing a control object that belong to one of the three groups of critical objects.

When dealing with the issues of cyber protection, as well as fail-safety and fault-tolerance, it is reasonable to rely on the following **postulates**:

1. There is no absolute cyber protection (fail-tolerance, fail-safety) of control systems.
2. The more complicated a system is, the more number of tasks it performs, the lower its cyber protection is.
3. A prerequisite for enhancing the cyber protection of a system is redundancy in combination with organization of efficient control.
4. The cyber protection of a control system should be ensured at all stages of its life cycle.
5. The level of cyber protection is restricted by economical risks of a customer and operating company.

Absolute cyber protection cannot be reached since elimination of vulnerabilities of one type does not rule out the possibility of new vulnerabilities appearing. The problem of ensuring cyber protection is the problem of improving a shield against a sword’s attacks. Along with the increase of a protection level, attack means are improved, and one cannot guarantee that the efficiency of protection means at certain times is much higher than the efficiency of attack means.

The radical solution of the task consists in **ensuring a guaranteed level of cyber protection for unsafe HW/SW by using multilevel IT and functional safety based on assessment of residual risk** (Fig. 3).

The implementation of multilevel safety principles on railway transport can be exemplified as follows:

Multilevel safety ensuring for each standalone control device. Let this HW/SW complex provide for *several* safety functions. One or several safety functions simultaneously performs the task of switching the device into safe state in case of failure, which can be states of acceptable decreased functionality or states of protection when generation of commands is blocked;

Multichannel safe multilevel system made of devices or systems of different types. The point is that on a certain railway section two or more control devices (systems) perform analogous control functions that are implemented by different ways and algorithms. The results of each controlling action are checked for consistency. If the condition is satisfied, then controlling is realized. Otherwise, an additional check is done and a decision is made on introducing a safe failure of one of the devices or its further operating as part of a multilevel system, but with decreased performance. If at some random moment of time control functions are not contradictory, then a multilevel system keeps on performing control functions with predefined efficiency.

System of choosing a more restrictive aspect. A decision making device is introduced into a multilevel system. This device realizes the following rule: if control functions are not contradictory, then a less hazardous control is chosen. For example, if the output of the first device of railway signalling and remote control generates "at danger" light signal, and the output of the second one generates "red and yellow" signal, then the output of the system generates "at danger" control signal.

Development of system functions of safety in developing multilevel systems. A developing multilevel system is a system that has possibilities and abilities to generate new controlling properties and/or new safety functions. Further on we'll consider a developing system that only generates new safety functions. The essence of the principle is as follows: a decision making support subsystem is introduced into a system along with (or instead of) a decision making device. Also, for each composite device or composite system of railway signalling and remote control, an additional logical control of safety states is introduced. This control is realized by means of memorization, analysis, correlation with indication of composite devices of logical consequences as regards changes of states of trackside signalling and remote control equipment. By jointly processing control commands from the outputs of these devices or systems and data of logical control in decision making support systems, their additional safety functions are generated.

3. Conclusion

In order to ensure the fail-safety of control systems, it is necessary to create conditions when a system is observable and controllable.

Based on the principle of acceptability of a residual risk under the existing limits of financial resources, it is needed to fully realize possibilities in ensuring fail-safety and functional safety.

To ensure the cyber protection of a control system, a complex of measures for ensuring IT protection, reliability and, in particular, functional safety should be implemented. A radical solution of the task is in ensuring a guaranteed cyber protection level for unsafe HW/SW by using multilevel IT and functional safety based on assessment of residual risk.

References

1. ISO 9126 GOST R ISO/IEC 9126-93 Information technology. Software product evaluation. Quality characteristics and guidelines for their use, 28.12.93

2. GOST R/IEC 61508. Functional safety of electrical, electronic, programmable electronic safety-related systems, 2010.

3. **Shubinsky I., Schäbe H.** On the definition of functional reliability. Dependability, 2012. – №4, pp. 74-84.

4. Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013.

5. **Rozenberg E.N., Shubinskiy I.B.** Functional Safety of RailwayAutomation Systems: Methods and Models. Moscow: VNIIAS MPS UIC, 2005.- 155 p.