ON THE DEFINITION OF FUNCTIONAL RELIABILITY

I.B. Shubinsky, Doctor of Technical Sciences, professor, director of closed company "IB Trans",
Russia, Moscow tel.: +7 (495) 786-68-57 e-mail: igor-shubinsky@yandex.ru

•

Dr. Hendrik Schäbe, Institute for Software, Electronics, Railroad Technology
TÜV InterTraffic GmbH 51105 Kölne-mail: schaebe@iseb.com

Abstract

The theory of reliability has been developed in order to ensure operability of technical objects (components and systems). However, no thorough explanation of the term "functional reliability" is given by now, although it is used with increasing frequency. We deduce a definition based on the terms property, quality and function.. In this connection, we draw attention on the principal differences between functional and structural reliability. We explain similarities between functional safety and functional reliability and show how they smoothly change one into the other.

Key words: functional reliability, reliability, safety, quality, function

1. Introduction

The theory of reliability has been evolved in order to ensure operability of technical objects (elements and systems). This assumes that the object is reliable, if it provides its intended function. This condition is absolutely necessary - however, is it also sufficient? Let us assume that an object is working and performs its intended function. Performance of the function is connected with output generated by the object. If there is no result - there is no realisation of the function. When considering the result, the latter cannot be considered abstractly – it should be characterized by its quality characteristics. For example, it needs to be defined when correctness, accuracy and efficiency of de delivered result of the function performance are acceptable.

If the object is intended for performance of two or more functions, then it is necessary to consider the reliability of each of the intended functions taking into account the functioning state of the said object. This assumes, firstly having the result of each function, and, secondly, knowing how much these results meet the given requirements.

Thus, functioning of the object is the necessary condition, but it is not sufficient for its reliable functioning. In the standard [1], an attempt has been undertaken to expand the interpretation of reliability by adding the aspect that an object is able to carry out the intended function, in addition to the traditional task of creating a working object. However, there is no explanation of the term "ability to carry out the intended functions" in the given standard and in the subsequent publications connected with it [8,9]. Moreover, it is not clear whether this term includes a judgement whether the function has been performed with sufficient quality. If this aspect is not included, the given definition is nothing else than the definition of the availability of the object. This is the same as the traditional understanding availability of the object as the property to perform any intended task..

If the introduction of the term is accompanied with a quality level with which each of the functions has to be carried out, the question arises, which quality characteristics have to be used und how they are defined? How can the space of working states of the objects be combined with the space of successful performed functions by the objects – and this taking into account possible different quality characteristics? Answers to these questions are extremely problematic as are attempts to analyse the reliability of execution of intended processes by the means of traditional reliability.

2. The tasks of structural and functional reliability

We introduced the term "Structural Reliability" for the definition of that part of the general reliability theory, which is focused on investigation of failure processes and renewal of technical objects, and on solving problems of ensuring their functioning. Earlier these problems were in the center of attention of the traditional reliability theory.

The concept of "Functional Reliability" is used increasingly, both in Russian as well as in the foreign literature [1, 8, 9]. However, we could not find a sufficiently deep interpretation of this concept. Since the role of the general reliability theory for solving tasks of ensuring reliability of modern complex technical systems is difficult to judge, we have decided to express our position in understanding of the subject, research target and problems in the field of functional reliability,

The research targets of structural and functional reliability are presented on fig.1

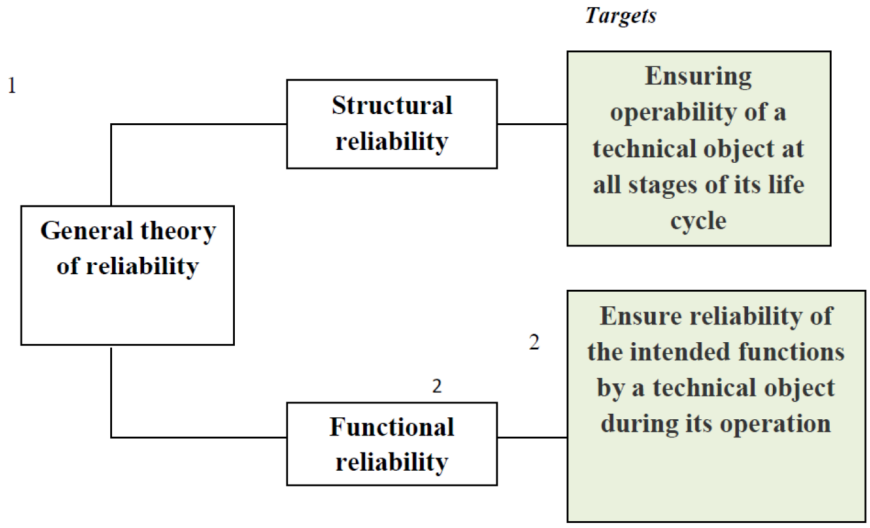

Figure 1. The targets of structural and functional reliability

Structural reliability covers a wide spectrum of tasks ensuring operability of technical objects (elements, systems). It includes the application of various kinds of redundancy, design of reasonable electric loads and climatic modes of operation during development and realisation of effective external and internal monitoring of the function of the object. Problems of maintenance optimisation (maintenance and repair), minimisation of life cycle cost, and prolongation of rated service life of an object (defined by the developer) are solved at operation stage.

The theory and practice of functional reliability are focused on studying functional failure processes, as well as renewal processes and restoration of information processes. A functional failure is a failure to fulfil a functional task caused by a deviation of an information process.

One of the main problems which cause faults of information processes (alongside with faults caused by software errors), operator errors, errors of input information is the problem of transitional failures of digital equipment and IC devices. The frequency of transitional failures exceeds the frequency of hardware failures by several orders of magnitude [2.] Transitional failures are caused by wrong performance of logic functions of discrete hardware components, which then progress into errors in performance of operations, procedures, programs, tasks.

The methodology of structural reliability is rather broad but it is not focused on calculations of reliability of information processes and their constituents - it is dedicated solely to failure processes

and renewal of technical systems. Structural reliability does not deal with the sequence of tasks to be carried out. In addition to that, it does not take into account the influence of software errors, operator errors and errors in the input information on the results of the task algorithms. All these factors (threats) of unreliability serve as a study subject in the theory of functional reliability, as a component of the reliability theory. It is necessary to note, that operator errors are investigated in the theory of human reliability, which is a separate area not belonging to structural reliability.

3. Quality and properties

Each system possesses certain attributes describing it. ***Quality of a system*** is a set of properties defining the system for users according to its functional purpose and requirements. In addition, requirements can be understood in a very broad sense, which leads to many different definitions of the concept. Mostly, the used definition of quality is taken from the standard ISO 9001 [10] according to which "quality is the degree to which a set of inherent characteristics fulfils requirements". System quality of is a relative concept, which makes sense only taking into account real application., Therefore the quality requirements are defined according to conditions and the specific area of application of the system.

According to the standard ISO 9126 properties are attributes defining properties of software which can be considered as quality characteristics. The standard ISO 9126 [3] presents a model of software quality. Quality models can be defined for all technical systems. They are in fact specifications of system properties. A well and logically written requirements specification is close to a quality model as it defines all essential system properties. The structure of system properties should correspond to the system structure. If the system consists of software and hardware, then properties are divided into the two groups for software and hardware, besides a third group of system properties.

For example, information protection can be an important system property. Information protection can be considered as software property, if corresponding measures are implemented in the software. Information protection can also be a hardware property, if corresponding measures are implemented in hardware.

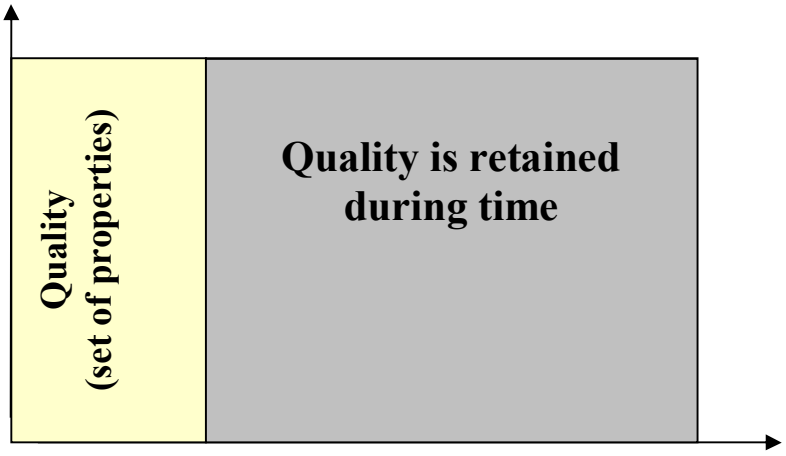

Figure 2. An explanation of functional reliability

It goes without saying, that total or partial loss of a certain property means decrease of system quality.

It is important, that properties are not only present in the object in the beginning of its life cycle, but it is also important that they were kept long enough during its lifetime. Retention of these properties (i.e. quality) is defined as reliability [4]. The second definition of reliability is given in

the standard EN 50126 [5] as the probability that an object can perform the function in a certain time interval. Both the first and the second definitions directly relate to functional reliability.

A functional failure is the loss of the ability to perform the assigned function by the object. [2]. Failure can be caused by malfunction, i.e. functional deviation of a system component from the specification. Not each malfunction will lead to failure.

An intolerable deviation of the characteristics of the object [4] is called an error. Such deviations can be, for example, intolerable values, inadmissible precision, inadmissible time (late, early, too long) or others. The error is introduced into the system during its development, manufacturing, etc.

Failures are divided as systematic and random ones [5]. Systematic failures are often caused by errors. Software failures are always systematic by nature and they are caused by software (SW) errors. Usually, SW failures reveal themselves in a random manner since SW is subject to random influence of an environment, which activates an error and, hence, can lead to a fault or even to a system failure. Further, it is necessary to note, that failures can be partial in cases when only a part of a function fails.

4. Properties and hazards

We start from the obvious fact, that it is impossible to describe functional reliability by any single property. Only the entire set of properties (attributes) allows the system to perform the intended functionals, i.e. to provide qualitative service of inquiries of system users [2]. Properties and hazards regarding functional reliability of the system are shown on fig. 3.

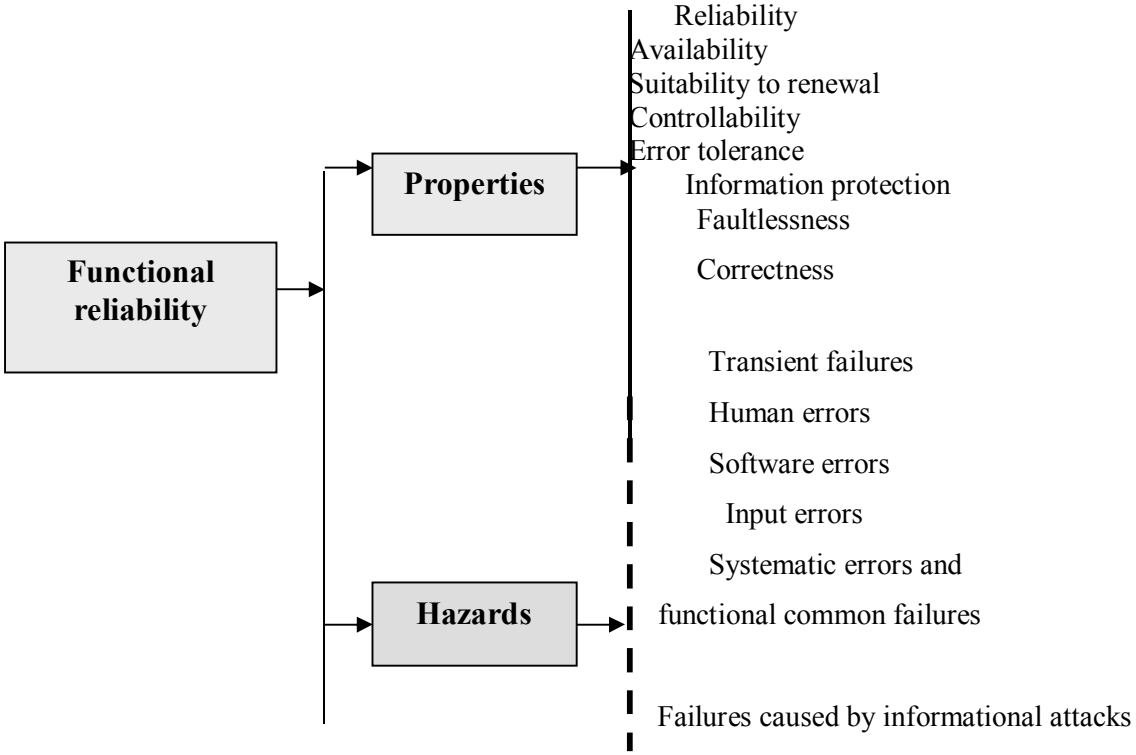

Figure3. Properties and hazards of system functional reliability

Besides the properties of reliability and availability which are typical for structural reliability, for objects studied by functional reliability, properties such as suitability for recovery of the function (analogue of maintainability), but also new properties: protection of information,

monitoring of the quality of the functional performance, stability against errors, and last but not least faultlessness and correctness of the function. In the opinion of the authors, the latter is very important.

Let us consider the hazards connected with functional reliability. According to standard EN 50126 [5] "hazard is a physical situation with a potential for human injury". Certainly, hazard concerns not only harm for an individual, but also harm to material belongings or to the environment. Not each hazard always leads to a threat. For such a threat, it is necessary, that there was an initiating event. Then the chain of undesirable events can evolve from threat, which finally will lead to unfortunate event, i.e. to accident.

Typical groups of threats (hazards) for systems are the following (fig.3):

- *Transient failures* –results of disturbances of digital technical equipment leading to malfunction of the software performance, malfunction of information technologies and malfunction of information process as a whole. These effects reveal themselves in the form of distortions, distortion or loss of data, errors in intermediate and / or in output results.
- *Software errors* – these are essentially errors arising during information processing at various stages of the software process. They are grouped as follows: system errors, algorithmic errors, program errors.
- *Human errors. Human* error is defined as a failure to carry out a required task (or performance of a forbidden operation), which can lead to a deviation of the functional processes in the system or incorrect *performance of at l*ast one function.
- *Input message errors* [6] – *damage of the* integrity of the information flow (more or less messages were received, the order of messages was violated, delay of messa*ges,* message **d**istortion or masquerade).
- *Systematic failures and common mode functional failures* - deviations of system functions caused by typical errors in designing components, operating modes, maintenance of the system, information coding, and also such factors, which cause simultaneous influence on several channels (in multichannel system), or several functions, or redundant devices or subsystems.
- *Errors due to information threats* - set of attacks of an intruder corrupting integrity and availability of the information.

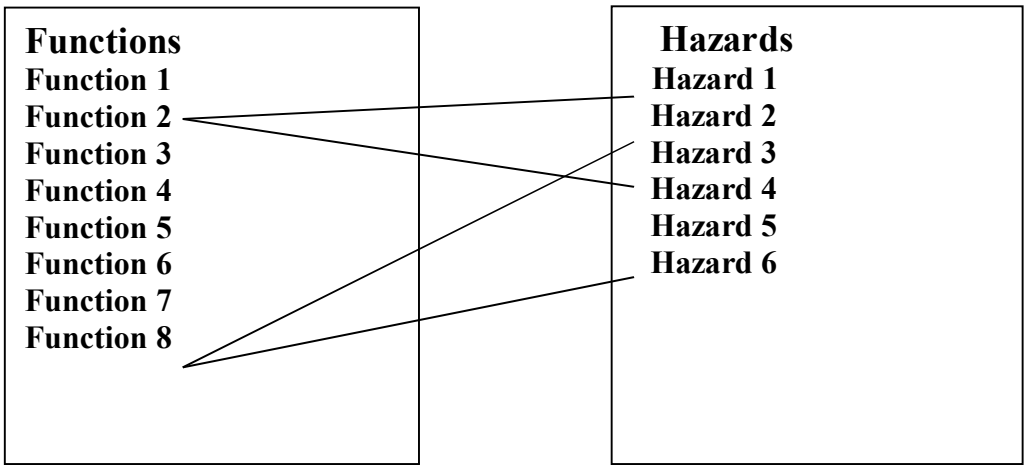

Figure 4. Connection of functions and threats

There is a connection between threats and system functions. This connection can be caused by two reasons:

a) The system function directly generates a threat or a hazard. For example, the function of high voltage generation implemented in a power supply system leads to high voltage, which represents a hazard (threat) and can lead to electrocution.
b) The system function itself is important for control or prevention of hazards. For example, a railway interlocking prevents collisions of trains.

Thus, there is an interrelation of functions and hazards (fig.4).

Not each failure, i.e. degradation or loss of a function, leads to hazard or threat. This depends on the specific properties of the failed function. And on the contrary, not each threat is caused by loss or degradation of some system function.

5. Functional failures

Let us now assume that the system can be described in a space of states. The dimensions of this space are the system properties. The system properties change in time. These changes can be caused both by external influence, and by internal processes, including system ageing. The space of states contains both allowed and not allowed states. If the system is in an inadmissible state, then there is a deviation from the intended functional behaviour, i.e. a partial or full functional failure has occurred.

The admissible part of the space of states is characterized by the fact that the admissible states satisfy the following requirements:

- Accuracy;
- Information output is provided (function);
- Logic admissibility of output data.

The allowed area of system states is shown on fig. 5.

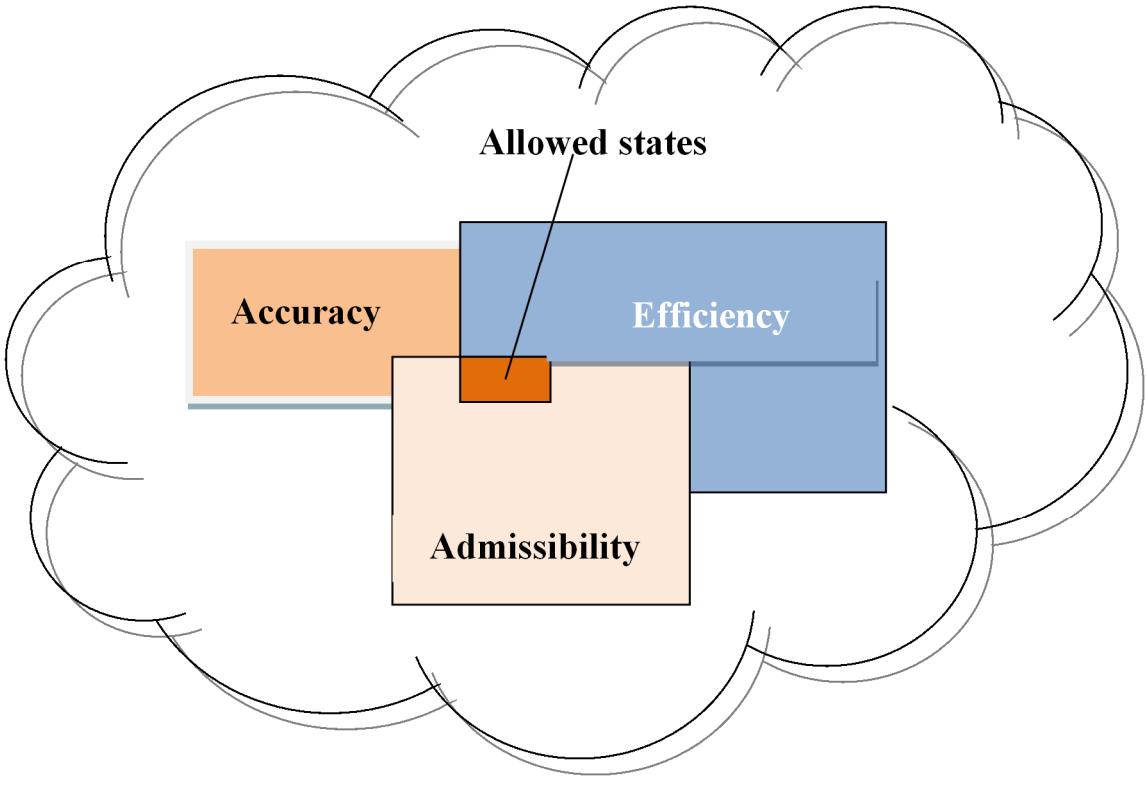

Figure 5. System states

Of course, all the three above mentioned requirements need to be satisfied for all intended functions.
System failure can lead to consequences of different nature, for example:

- Material losses due to non-availability of the system function,
- Material losses due to damages caused by the system to itself or to other systems,
- Material losses due to damages to the environment,
- Loss of life or injury, caused to people.

The consequence, which takes place, depends not only on the system itself, but also on the function, that is performed by system. Hence, it is meaningful to speak about functional reliability.

6. Definition of functional reliability

Based on reasoning presented in the previous chapters we are now ready to give definition of functional reliability.

In the given paper, *functional reliability of a system is defined as the set of its properties, which define the ability of the system to correctly perform the intended tasks with an acceptable level of precision with the output results being in admissible limits.*

Some positions of the definition require an explanation. First of all, the combination of attributes "precision" and "correctness", which have a different meaning, requires an explanation. The term "correctness" means, that information processes are realized according to the specified set of rules and instructions, i.e. in essence according to the algorithms for performance of information processes intended in a system. The term "correctness" of functional reliability is similar to the concept of "failure free function" in structural reliability. Any deviation from the specified rules and instructions leads to deviation *from correct* functioning of the information system. This means the following. If the algorithm for information processing is constructed correctly then it is possible to receive correct results provided program or transitional faults are absent during information processing. We say "it is possible to receive" keeping in mind, that correct results are not solely achieved due to a correctly constructed algorithms of information processing. Wrong results can be obtained caused by deviations in boundary values of data and / or results, boundary values of lengths of keys, admissible number of file records, admissible length of keys, admissible number of search criteria, etc. Transitional failures of digital technical equipment, for example, can cause wrong results, which lead to distortion of separate instructions of the algorithm or falsification of stored boundary values. Thus, the property *of correctness* is one of the important components of system *functional reliability* and it characterizes the credibility of results (for example, code combinations or results are in the allowed region).

Let us assume that the system correctly performs the intended tasks. Does it mean that the system is functionally reliable? The answer is no, because *correct function must be ensured, but it is not sufficient.* For example, an error caused by informational threats and violation of data integrity, intermediate and / or distrortion of output results in failure of control. In this case, the algorithm of the task being performed has been correct. As an example, we consider a graph describing part of an algorithm (fig. 6). The graph shows procedures (nodes) and connections between them (edges). All the defined task procedures (they can be considered as instructions) must be executed according to the defined rules (they can be considered as connection between the nodes). If in the given task all operations are performed strictly according to rules and instructions, then we can assume that information process used for implementation of the function has been realised correctly.

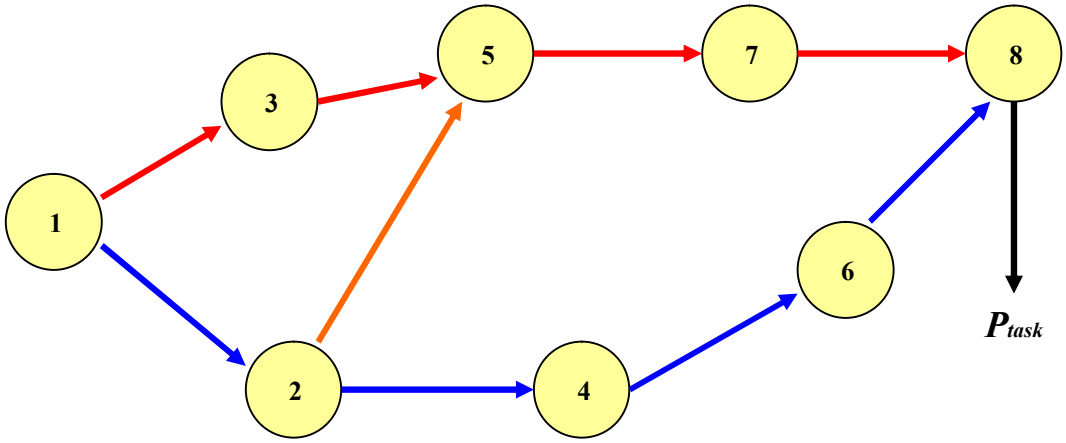

Figure.6. Explaining correctness and faultlessness of system functional reliability

Probabilities of faultless performance of tasks can be related to the nodes of the graph. The resulting probability of faultless performance of all tasks is calculated taking into account the connections between the tasks (edges). The property of faultlessness is a complex one. It is ensured both by faultless execution of each task taken separately and the correct execution of the sequence of the tasks according to the algorithm.

A definition of functional reliability of information system would be incomplete without taking into account the transformation of a possible output error into a functional failure of the information system. It is necessary to understand, that with the help of the intended functions in the system it is possible not only to exclude the progression of an error into a functional failure within the admissible limits, but also to neutralize that error. This is achieved under the following necessary conditions:

a) the system has a qualitatively high means for detection of errors,
b) the system has in its structure means for ensuring error tolerability

Note that, if there is some, even small time interval available for detection and reaction of the system, then there is always a certain probability to efficiently eliminate the detected error, even if the system is not equipped with intrinsic error tolerability. However, with the help of means for error tolerability, there are possibilities to considerably increase the probability of preservation of correct output results and, certainly, to enhance faultlessness of transformation of the initial data into results.

7. Safety

So far, we used the term “safety” without defining it. According to the standard EN 50126 [5], safety is defined as freedom from unacceptable risk. Risk is a combination of damage and probability of its occurrence [7]. The definition of risk given in EN 50126 is somewhat ambiguous. In EN 50126 risk is defined as “The probable rate of occurrence of a hazard causing harm and the degree of severity of the harm.”. One should talk about a specific combination meaning a specific operation, instead of a simple compilation. However, in the sequel the term risk is used correctly in the given standard

Depending on consequences, it is possible to consider separately:

a) functional reliability of the system if it performs its function (i.e. does not lose the defined properties) in a chain of all those systems contribute to functional performance;
b) functional safety if consequences do not lead to unacceptable risks.

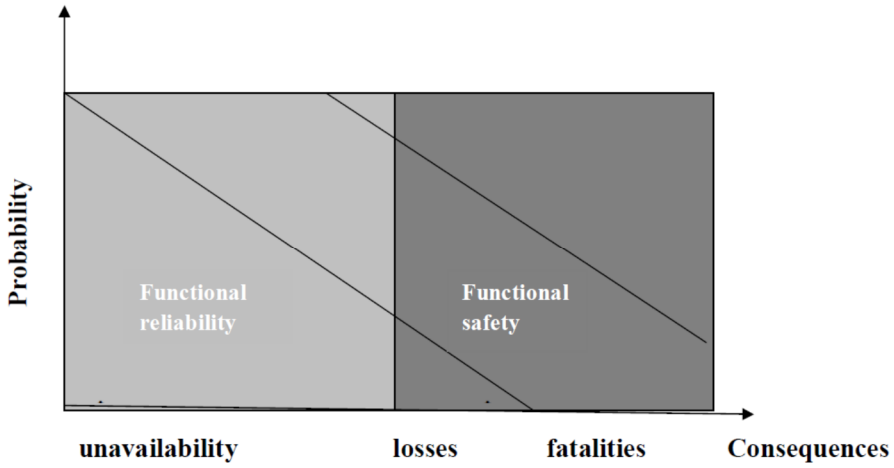

Figure 7. Functional reliability and functional safety.

Figure 7 shows, that as far as consequences are considered, functional reliability smoothly transforms into functional safety if the consequences of functional failures become more and more critical. From this fact it is evident, that systems, which are critical in the area of functional reliability (for example, with a rate of functional failures in the area $10^{-6}...10^{-7}$ 1/h), can handled using the concept of functional safety. Such systems are often called as critical systems.

Finally, from the above considerations we conclude that those methods which are used in functional safety for neutralization of threats, may be used in functional reliability in the same manner.

8. Combining reliability, safety and quality

Functional reliability and safety of a system in its specific application and environment, can be considered as complex properties. However, it is not always logical when recalling the definition of reliability definition.

Thus, we have the following picture (fig.8).

Thus, properties of functional reliability and functional safety are explained through other system properties, and they also transform smoothly into each other. This has already been shown on fig. 7.

It should be noted, that the quality model, i.e. the set of properties as described in figure 8, differs from that, which is presented in section 3. It is larger and cannot be used for an explanation of the terms functional reliability or safety.

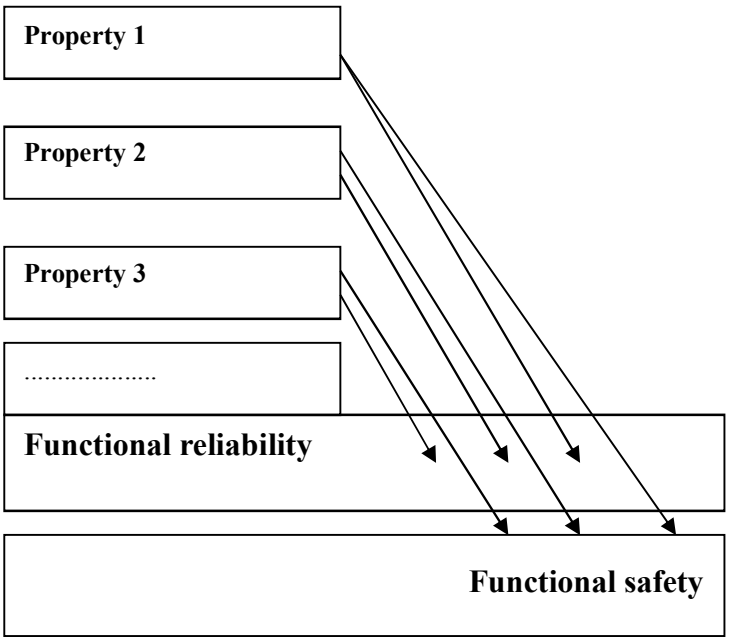

Figure 8. Functional reliability and functional safety as system properties.

9. Conclusions

In this paper, we have defined the concept of functional reliability. Much attention has been paid to the fact that the system is not so much important itself, but functions it performs. We have substantiated this statement considering system functions and the threats caused by them. Our discussion has shown how the concepts of functional reliability and functional safety are connected with each other. On the one hand, they both smoothly transform into each other, on the other hand, they cover a broader spectrum of properties and threats, than the terms “structural reliability” or "simple" safety.

We hope, that systematic interpretation and deeper understanding of functional reliability facilitates the solution of many urgent problems of reliability and safety.

References

1. IEC 60050 (191) : 1990-12. Reliability and quality of service.
2. Shubinsky I. Functional reliability of information systems.- M.: Journal “Dependability”.2012 – 295p.
3. ISO 9126 GOST R ISO/IEC 9126-93, Estimation of program production, characteristic of quality and manuals on their application, 28.12.93.
4. VDI 4001 Blatt 2 (siehe DIN 40041 Teil 1) Begriffsbestimmungen zum gebrauch des VDI Handbuches Technische Zuverlässigkeit. (Definition of concepts for use VDI manual on operational reliability.
5. EN 50126 State standards of Byelorussia, Railways. Requirements and demonstration of RAMS. Part 1 Basic requirements STB/PR_1.
6. CENELEC EN 50159. Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission. Part 2: Part 2: Safety related communication in open transmission systems. - 2000.

7. GOST R/IEC 61508. Functional safety of electrical/electronic/programmable electronic safety systems.-2008.
8. Avizienis A., Laprie J-C. and Randell B. Dependability of computer systems/Fundamental concepts, terminology and examples. Technical report, LAAS - CNRS, October, 2000
9. Rus I., Komi-Sirvio S., Costa P. Computer program with insurance of high reliability. Technical report, IFIP WG-10.4, March, 2008.
10. GOST R ISO 9001 Systems of quality management, requirements, 2008