Original article
https://doi.org/10.21683/1729-2646-2021-21-2-24-27

# Errors, faults and failures

**Igor B. Shubinsky[1]*, Hendrik Schäbe[2]**
*[1]JSC NIIAS, Moscow, Russian Federation, [2]TÜV Rheinland, Cologne, Germany*
**igor-shubinsky@yandex.ru*


*Igor B. Shubinsky*


*Hendrik Schäbe*

**Abstract. Aim**. *To harmonize the definitions of errors, faults, failures in the Russian and English languages. The Object of the paper is one of the most important subject matters of the dependability theory and functional safety. The Subject of the paper is the concepts and definitions of failures, errors, faults.* **Results of the research:** *analysis of the definitions of the concepts describing the dependability and functional safety of items in the Russian and international standards, such as GOST 27.002-2015, GOST R/IEC 61508-2012, IEC 60050, DIN 40041, as well as in publications by a number of authors. The analysis shows that failure is always associated with the loss of function, i.e., the ability to perform as required by all standards. It should be noted that wrong user expectation does qualify as failure. A failure should be distinguished from unintended functions. A fault is defined as a system's inability to perform the required operation to the full extent that, under certain conditions, may escalate into a failure. An error as a discrepancy between a calculated, observed or measured value or condition and a true, specified or theoretically correct value or condition is a deviation that is present and, under certain conditions, would probably turn into a failure. A typical example is non-critical software errors. The so-called systematic failures are actually errors that can turn into critical errors (failures). Let us note that the definitions in the IEC 60050 international electrotechnical vocabulary can be used, as they show general agreement, which is not surprising for an international standard.*

**Keywords:** *failure, malfunction, error, fault, damage, standard, term, dependability, functional safety, event, work.*

**For citation:** *Shubinsky I.B, Schäbe H. Errors, faults and failures. Dependability 2021; 2: 24-27. https://doi.org/10.21683/1729-2646-2021-21-2-24-27*

**Received on:** *20.10.2020* / **Revised on:** *10.04.2021* / **For printing:** *21.06.2021.*

## 1. Introduction

The development of dependability and safety-related terminology is at the focus of attention of many researchers (e.g., see works by Netes, Pokhabov, Plotnikov, Mikhailov [1-5]). Such terms are not always represented equally well in different languages. In this paper, we will attempt to examine possible definitions of the terms *error, fault, failure*. We will try to do that simultaneously in the English and Russian languages. That is not an easy task, since there are not so many well-translated papers or books. In any case, in this article the authors will attempt to describe their view of the terminology. Section 2 overviews a number of existing definitions and concepts. Section 3 provides a brief analysis of key terms and proposes definitions devised by the authors. Section 4 draws the conclusion.

## 2. Review of the existing concepts

Definitions of the terms *fault, failure* and *error* can primarily be found in the standards dealing with terminology and definitions. In IEC 60050 [7], the following definitions are recommended:

*failure*, loss of ability to perform as required,

*fault*, inability to perform the required function due to the internal state,

*error,* a discrepancy between the calculated, observed or measured value or condition and the true, specified or theoretically correct value or condition.

The GOST 27.002 interstate standard [8] sets forth the following definition:

*failure*, an event consisting in the disruption of an item's up state.

This interpretation is based on a monograph, the fundamental book on dependability written in 1965 by B.V. Gnedenko, Yu.K. Beliaev, Yu.D. Soloviev [9].

*Failure* is a partial or total loss or alteration of such properties of an item that significantly reduce the performance or cause the loss of operability.

It can be noted that this definition set forth in [9] may also define a fault. However, we must admit that over the past 55 years the terminology has somewhat evolved in a way the authors could not have anticipated. That is particularly the case with the definition of *error*.

The GOST 27.002 interstate standard [7] lacks the definition of error, but fault and defect are defined as follows:

*fault* is a state of an entity, in which it does not comply with at least one of the requirements specified in the respective documentation,

*defect* is each individual deviation of an entity from the requirements defined in the documentation.

The differences between the definitions are minor. Whereas a fault is any inconsistency with the requirements, a defect is each particular inconsistency. GOST 27.002 defines *damage* as an event consisting in the disruption of an entity's good state under condition of retained up state.

This definition of damage is very similar to that of fault according to the IEC 60050 dictionary [7].

As a third source, let us use the article by Gayen and Schäbe [10, 11] that was published in two languages, thus the terminology is coordinated. The authors partially borrowed the terminology from DIN 40041 [12] that, although still valid, is outdated and no longer supported. That explains some of the drawbacks.

*Failure*: a specific physical functional module stops performing a function within the specified load and environmental conditions.

This definition is associated with the loss of the expected function and corresponds to the above definitions. However, the application of the term does not go beyond the element. Such application of this concept at the system level can lead to confusion, as it does not necessarily characterize system failure. At the system level, it can be associated with a fault. However, the definition of fault in the same article explains that.

*Fault* is a lost or erroneous function or incomplete delivery of the desired function by module.

An important aspect of the discussion is the distinction between faults and failures. On the one hand, a fault is a partial loss of functional capacity or a complete loss of functional capacity associated with a module or subsystem not necessarily resulting in a system failure. On the other hand, a fault can also occur at the system level and reduce system performance. Therefore, it is important to distinguish between a system and a subsystem/unit. We must note that an event that may consist in a subsystem failure may be just a fault at the system level, as other subsystems can – at least partially – compensate for such subsystem failure to make it just a system-level fault.

Chillarege [13] considers a software failure/fault to be an event where the customer's expectations have not been met. In fact, that follows from the interpretation of failure as a complete or partial loss of system function, in this particular case caused by the software. Shubinsky [14] notes that in this case the software itself did not fail; the failure occurs at the system level. Only those parts of the software that are faulty are activated, or the part of the software unable to respond correctly to the system command is activated.

Randall [15] suggests a whole sequence as follows:

Failure → Fault → Error → Failure, etc.

Here, terms that repeat are associated with higher system levels. Randall uses the following definitions:

A system *failure* occurs when the delivered service deviates from the system's function, the latter being what the system is intended for.

This corresponds to the definition of failure given by other authors.

*Error* is the part of the system state that can cause a subsequent failure. An error affecting the service is an indication that the failure has already occurred. The known or assumed cause is an error.

So, for Randall, an *error* is a deviation as a component of a system's state. Additionally, he interprets it as a fault symptom and defines a fault as the cause of an error. This approach appears to be ambiguous. The author's understanding is that Randall rather describes a fault when he explains what an error is. Rees [16] also maintains that

*failure* is a loss of function, i.e., an element does not work if it has not done what we want and is in a good state if it has done what we wanted. More precisely, it is the function that fails.

Note that it is not a matter of whether a system is physically intact or otherwise. A failed system may be physically intact. A physically intact system may also fail due to hidden (unwanted or poorly designed functions, see, e.g., Deckers and Schäbe [17]) or undocumented functions that were integrated in the system unintentionally or intentionally.

Parhami [18] introduces a list of 7 states: *ideal*, *defective*, *faulty, error*, *poorly functioning*, *degraded*, *failure*. A system passes from state to state, from ideal to failure. In the authors' opinion, the designations of some of the states are ambiguous. A defect can also mean a fault, degradation or failure. Additionally, the question is how to interpret an error state. Is this term supposed to be used only to characterise a system affected by an error, where the error describes a deviation from the specifications, that was built into the system at the very beginning, i.e., a deviation? The authors believe that the number of states is to be reduced. While on the subject of failures, we should also mention the distinction made in IEC 61508 [6] and other functional safety standards between the concepts of "Accidental hardware failures" and "Systematic failures". First of all, let us define failure, fault and error according to IEC 61508 [6] part 4:

3.6.4: "a failure is the termination of a functional unit's ability to ensure the required function or the operation of such functional unit in any other way than the required one.

3.6.1: "a fault is an abnormal state that may cause a functional unit to completely or partially lose be ability to perform the required function".

3.6.11: "an error is a discrepancy between the calculated, observed or measured value or condition and the true, specified or theoretically correct value or condition".

By comparing these definitions with the definitions from other sources, it can be seen that failures are also regarded as events in which a system or its component unit does not ensure the performance of the desired function. Additionally, a fault is defined as a precursor of failure, i.e., an abnormal state, or a deviation, in this case. Nevertheless, the consequences will differ at the system level. That may include a partial loss of ability. Since the term "may" is used, it is also possible that, at the system level, there are no consequences, while there is only the requirement to repair the redundant unit.

3.6.5: "a random hardware failure is a failure that occurs at a random point in time that is the result of one or more possible hardware degradation mechanisms";

3.6.6: "a systematic failure is a failure deterministically associated with a certain cause that can only be eliminated by modifying the design or the process, operations, documentation, or other factors".

In these above two definitions, failures are distinguished depending on the mechanism that caused them. Accidental hardware failures are associated with the processes of ageing and degradation. Systematic failures are associated with design errors, etc. However, these failures also manifest themselves stochastically [19] when the failure mechanism is triggered, therefore they are deterministic only in the sense that one cause can be clearly defined. The time of occurrence is in many cases random. This randomness is caused by the environment that produces random external effects. To be precise, two sub-types should be distinguished:

a) the system contains an error, e.g., a software error. Another example could be a system that is unable to withstand certain high or low temperatures, although that is required. There is no ageing. Once an effect triggers such error, the system fails at a random time. The randomness is caused by the randomness of the external effect.

Due to erroneous processes, the system has a weakness. This weakness, for instance, consists in reduced resistance to loads, environmental effects, etc. An example is degraded mechanical parts that fail due to fatigue. Here, we can observe the triggering of the accidental failure mechanism caused by a design error that would otherwise have been eliminated through design solutions if the component was strong enough.

## 3. Analysis and conclusions

The analysis clearly shows how fault, failure and error should be interpreted.

*Failure* is always associated with a loss of function, i.e., a function as the ability to perform as required by all standards. It should be noted that this requirement may also be implicit, i.e., the system does not operate as expected. It should be noted that wrong user expectation does qualify as failure. Failures should be distinguished from sneaks (see, e.g., [17]).

*Fault* is defined as a system's inability to perform the required operation to the full extent that, under certain conditions, may escalate into a failure. The term "fault" may be translated into Russian in two different ways (failure, malfunction) that are used in parallel to each other depending on the document.

*Error* as a discrepancy between a calculated, observed or measured value or condition and a true, specified or theoretically correct value or condition, a deviation that is present and, under certain conditions, could turn into a failure. A typical example is non-critical software errors. The so-called systematic failures are actually errors that can turn into critical errors (failures). Let us note that the definitions in [6] can be used, as they show general agreement, which is not surprising for an international standard.

## References

1. Netes V.A. Item in dependability: definition and content of the concept. Dependability 2019;19(4):3-7.

2. Netes V.A., Tarasyev Yu.I., Shper V.L. How we should define what "dependability" is. *Dependability* 2014;4:15-26.

3. Plotnikov N.I. Development of an alternative dependability terminology. *Dependability* 2020;3:21-26.

4. Pokhabov Yu.P. On the definition of the term "dependability". *Dependability* 2017;17(1):4-10.

5. Mikhailov V.S. On the terminology of dependability. *Dependability* 2020;2:24-27.

6. GOST R IEC 61508. Functional safety of electrical, electronic, programmable electronic safety-related systems. Moscow: Standartinform; 2014. (in Russ.)

7. IEC 60050 International Electrotechnical Vocabulary; 2015-02.

8. GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

9. Gnedenko B.V., Beliaev Yu.K., Soloviev A.D. [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965. (in Russ.)

10. Gayen J.-T., Schäbe H. (Mis-)conceptions of safety principles. *Proceedings of ESREL 2008, Safety, Reliability and Risk Analysis* 2008;2:1283-1291.

11. Gayen J.-T., Shäbe H. [Correct and incorrect understanding of the principles of functional safety]. *Dependability* 3;3:63-74. (in Russ).

12. DIN 40041, Zuverlässigkeit; Begriffe (Reliability, terms). 1990-12 (outdated).

13. Chillaregge R. What is software failure. Commentary in IEEE Transactions on Reliability 1996;45(3).

14. Shubinsky I.B. [Functional dependability of information systems. Analysis methods] Moscow: Dependability Journal; 2012. (in Russ.)

15. Randall B. On failures and faults. Lecture notes in computer science. September 2003. DOI: 10.1007/978-3-540-45236-2_3.

16. Rees R. What is a failure. *IEEE Transactions on reliability* 1997;46(2):163.

17. Deckers J., Schäbe H. Using sneak circuit analysis in aerospace product assurance. *Qual. Rel. Eng. Int.* 1999;9:137-142.

18. Parhami B. Defect, fault, error,…., failure. *IEEE Transaction on Reliability* 1997;46(4):450-451.

19. Braband J., Schäbe H. Individual risk, collective risk, and F–N curves for railway risk acceptance. In: Mahboob Q., Zio E., editors. Handbook of RAMS in Railway systems – Theory and Practice. Boca Raton, Taylor and Francis; 2018. P.119-128.

## About the authors

**Igor B. Shubinsky,** Doctor of Engineering, Professor, Deputy Director of Integrated Research and Development Unit, JSC NIIAS. Address: 27, bldg 1 Nizhegorodskaya St., 109029, Moscow, Russian Federation, phone: +7 (495) 786 68 57, e-mail: igor-shubinsky@yandex.ru.

**Hendrik Schäbe**, Dr. rer. nat. habil., Head of Risk and Hazard Analysis, TÜV Rheinland InterTraffic, Cologne, Germany; e-mail: schaebe@de.tuv.com.

## The authors' contribution

The authors' contribution consists in the analysis of the terms failure, fault and error and their use in the Russian and English languages. The authors' contributions are equal.

## Conflict of interests

The authors declare the absence of a conflict of interests.