New international standard for dependability

Viktor A. Netes, *Moscow Technical University of Communication and Informatics, Moscow, Russia, e-mail: vicnet@yandex.ru*

Viktor A. Netes

Abstract. *In 2015 International Electrotechnical Commission adopted a new international standard IEC 60050-192 that specifies the main terms in the field of dependability with their definitions. It was developed by IEC/TC 56 "Dependability" under control of TC 1 "Terminology" and forms Part 192 of International electrotechnical vocabulary. This standard substituted the previous similar standard IEC 60050-191 adopted in 1990. This article is dedicated to IEC 60050-192, acquaintance with which is required for all specialists in the field of dependability. The new standard is compared with the previous IEC 60050-191, and with the similar Russian GOST 27.002–89. In comparison with IEC 60050-191 the new standard contains the modified content and scope, with exclusion of the sections containing the terms related to the quality of services of telecommunication and electric power systems. Based on that, IEC 60050-192 is entitled just with one word "Dependability". Therefore, now it totally corresponds to its status of a horizontal (i.e. inter-industrial, basic) standard. Terminology in the field of dependability is given in respect to a technical item, with analysis of the definitions of this notion, probable structure of the item and the number of terms specifying the types of items. IEC 60050-192 gives a new definition for "dependability": the ability of an item to perform as and when required. This definition was discussed actively, among the IEC experts who took part in the standard development, and among Russian specialists as well. The cluster of features of dependability has also changed: availability, reliability, recoverability, maintainability and maintenance support performance, and in some cases durability, safety and security. A new notion here is "recoverability" defined as ability of an item to recover from a failure, without corrective maintenance. This paper describes the standard's sections dedicated to an item's states and time notions, failures and faults, maintenance and repair, dependability indices, testing, design or engineering, analysis and improvement of dependability. It introduces and explains the most important terms, specifies new terms that were added to the standard, and those excluded from it. The article pays attention to the fact that certain terms have no adequate Russian equivalents. Though the Russian and international dependability terminologies have much in common, there are still significant differences between them. It is explained by the fact that the standardization of dependability terminology in our country that started half a century ago developed for a long time in isolation form similar work world-wide. Due to such differences the creation of a new GOST to be harmonized with IEC 60050-192 is currently not possible. But nevertheless it is necessary to seek to a maximum possible convergence of the Russian and international terminologies.*

Keywords: *dependability, terms and definitions, international standard, International electrotechnical commission.*

Citation format: *Netes V.A. New international standard for dependability // Dependability. 2016. No.3. P. 54-58. DOI: 10.21683/1729-2646-2016-16-3-54-58*

Early in 2015 the International Electrotechnical Commission (IEC) adopted a new international standard (IS) 60050-192, that specifies main terms in the field of dependability with their definitions. It forms Part 192 of International Electrotechnical Vocabulary (IEV). This standard substituted the previous similar standard IEC 60050-191 adopted in 1990, as well as amendments thereto of 1999 and 2002. At first the new standard was supposed to be the second revision of IS 60050-191, but then it was given another number (the reason will be explained later).

IS 60050-192 was prepared by Technical committee (TC) IEC 56 "Dependability" under control of TC 1 "Terminology". The development took quite a long time, progress of this work was reflected in several publications in Russian [1–3], but main purposes of these articles were different and

this standard was described in them briefly. This article is especially dedicated to IEC 60050-192, acquaintance with which is required for all specialists in the field of dependability. It should also be mentioned that some notions of this IS are used for the development of the new interstate standard which shall replace GOST 27.002–89, and the work under which is now in well progress.

Of course, one article cannot cover the whole content of IS 60050-192, that is why here we shall consider the most important moments only. The new standard will be compared with the previous IEC 60050-191, and with the similar Russian GOST 27.002–89. In the course of presentation, after first mention of terms we shall give their English equivalents from IS 60050-192 in brackets.

One could get acquainted with IS 60050-192, as well as with other parts of IEV using online version of this

vocabulary which is called "Electropedia" (www.electro-pedia.org/). Access to this Internet resource is free. Terms of dependability and their definitions are given there in English and French, and only terms (without definitions) are also given in Arabic, German, Spanish, Japanese, Polish, Portuguese and Chinese. Unfortunately, there is no Russian version (for IS 60050-191 there was the Russian version, though it was not provided in"Electropedia"). The complete text of IS in English and in French in electronic form or on paper can be bought through the IEC website (price is 310 CHF).

In comparison with IS 60050-191 the new standard contains the modified content and scope, with exclusion of the sections containing the terms related to the quality of services of telecommunication and electric power systems. Terminology for the quality of telecommunication services is listed in Recommendation E.800 of the International telecommunication union [4], and the terms on reliability and quality of electric power systems shall be described in the special IS 60050-692, which is currently under development. Based on that, IEC 60050-192 is entitled just with one word "Dependability", whereas IS 60050-191 was called "dependability and quality of service" It was the reason why the standard's number was changed. Therefore, now IS 60050-192 totally corresponds to its status of a horizontal (i.e. inter-industrial, basic) standard, that should be used by all standardization TCs.

Terminology in the field of dependability is given in respect to a technical item. In IS 60050-191 the definition of this terms just gives different types of items: an individual part, component, device, functional unit, equipment, subsystem, or system that can be considered separately. However, it is hardly a complete list of all possible types of items. That is why the new IS defines an item объект as a subject matter, and the types of items are listed in a note. Then the terms sub item, system and subsystem are defined.

Another note indicates that an item may consist of hardware, software, people or any combination of them. Further the terms "hardware" and "software" are defined. The standard also includes the number of terms specifying different types of software (SW): system software, application software, computer program, firmware, embedded software.

The terms "repaired / non-repaired item" used in the previous IS, are substituted with more precise term "repairable / non-repairable item". The fact is that a word combination "repaired item" may be understood in two ways: as an item the repair of which is possible, or as an item the repair of which is being carried out at this moment. To exclude the second incorrect meaning the terms were replaced.

In IS 60050-191 the definition of a key term "dependability" is actually reduced to the enumeration of its properties: availability, reliability, maintainability and maintenance support performance. IS 60050-192 gives the new definition of dependability: ability of an item to perform as and when required. This definition was discussed actively, among the IEC experts who took part in the standard development, and among Russian specialists as well. This definition, as well as other definitions of dependability were analyzed in a special article [3] that is why this issue is not described here.

This definition has a note that specifies the properties of dependability. They are availability, reliability, recoverability, maintainability and maintenance support performance, and in some cases durability, safety and security. As it has already been mentioned, availability, reliability, maintainability and maintenance support performance were listed in IS 60050-191. The term "durability" was also mentioned in IS 60050-191, but its relation to dependability was unclear there. Although safety and security are also mentioned in the note as individual terms that have definitions, none of them is mentioned in IS 60050-192.

New term "recoverability" is defined as ability of an item to recover from a failure, without corrective maintenance. Really, recovery is often carried out, for instance, by means of backup switching or SW reloading. These actions cannot be referred to repair, that is why the ability to such recovery is not covered by "maintainability", and it required the introduction of a new term. A particular case of recovery is self-recoverability when an item has the ability to recover from a failure, without external action to an item. These terms are certainly closely associated with the notion "recovery" that shall be described below.

Speaking about the properties that are the part of dependability let remind that according to GOST 27.002–89 dependability is a complex property which, depending to an item's designation and terms of application, may include reliability, durability, maintainability and storability, or certain combinations of these properties. There is no well-defined term "availability" in our standard, but there are the factors specifying this property quantitatively: availability factor and operational availability factor. On the other hand, there is no storability in IS.

IS 60050-192 contains no general terms "effectiveness" and "capability" mentioned in the previous IS, because they are considered as not directly referring to dependability.

The new standard, as the previous IS, has a section dedicated to an item's states. GOST 27.002–89 defines two pairs of states: good – faulty, upstate – down state (a good item is always in the up state, faulty item may be both in the up and down states; an item in the up state may be good and faulty, an item if the down state is always faulty). IS contains no equivalents to good and faulty states, but it has a number of other terms specifying different states of an item. Particularly, there are operating and non-operating states. Being in the first one an item performs a certain required function, being in the second one it does not perform any required function.

For each state the time of being in this state is defined. Then the times related to maintenance and repair

of an item are defined. This intricacy of times could be understood with the help of two figures provided in the standard. Notions of time include useful life, as well as early life failure period, infant mortality period, constant failure intensity period and wear-out failure period. The last three notions are specific to the items with U failure rate curve.

Some terms were excluded from the section about failures. For example, such types of failures as critical and non-critical, sudden and gradual, relevant and non-relevant, degradation, etc. At the same time the following types of failures are kept: complete and partial, primary and secondary, systematic and etc., software failure was added.

Terms "failure cause", "failure mechanism", "common cause failures", "common mode failures" also remain. The first two are quite clear, let us give the definitions for the last two of them. Common cause failures – failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause. Common mode failures – failures of different items characterized by the same failure mode. This term could be understood better with introducing the notion "failure mode" which is defined as manner in which failure occurs. The terms "failure effect" – consequence of a failure, within or beyond the boundary of the failed item and "criticality" – severity of effect with respect to specified evaluation criteria, were also introduced

One of the IS sections is dedicated to the notion that has no direct analogue in the Russian terminology for dependability. In English it is expressed by the term "fault" and defined as follows: inability to perform as required, due to an internal state.

In the Russian version of IS 60050-191 fault is translated as "znachitelnaya neispravnost (Rus.)", in GOST R 27.002–2011 (originally GOST R 53480–2009) – just "neispravnost (Rus.)". But this translation can hardly be admitted a good translation, because by many years of tradition kept in several standards one of which is GOST 27.002–89, "neispravnost (Rus.)" is a short form of the term "neispravnoe sostoyanie (Rus.)". Meanwhile, as per its definition, fault is not a state. By the way, such rendering of the notion "neispravnost (Rus.)" in GOST R 27.002–2011 was criticized hardly by experts [5, 6], because according to our standards "neispravnost (Rus.)" does not at always lead to an inability of an item to perform (that is why when IS 60050-191 was translated into Russian a word "znachitelnaya (Rus.)" was added). We cannot translate "fault" as "otkaz (Rus.)", though these two notions are closely connected as it will be clear from the subsequent. A word "disturbance narushenie (Rus.)" is used in the Russian version of this article as a working Russian equivalent (author will consider other suggestions on this topic with appreciation).

The definition of a fault is supplemented by several notes. The first note says that a fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life cycle, such as specification, design, manufacture or maintenance. The respective words can be used to indicate the cause of a fault: due to the errors occurred at the stage of specification development, design or engineering, manufacturing. Another note says that The type of fault may be associated with the type of associated failure, e.g. wear-out fault and wear-out failure. It is also noted that an item may have one or more faults.

Some terms specifying the types of faults were excluded from this section: critical and non-critical, major and minor, complete and partial and some other terms. The following terms remain though: intermittent, latent, systematic, programme-sensitive. Software and data-sensitive faults were added.

One more IS term having no direct Russian equivalent in GOST 27.002–89, is "maintenance". It can be translated as a word combination "tekhnicheskoe obsluzhivanie i remont" that includes two notions which are separate in the Russian terminology. The word combination "tekhnicheskoe soderzhanie" is proposed in the Russian version of this article as the Russian equivalent to the English "maintenance". This word combination was already mentioned in GOST 32192–2013 Dependability in Railway Techniques – General Concepts – Terms and Definitions.

Maintenance operations are divided into preventive and corrective. The first type operations are carried out to mitigate degradation and reduce the probability of failure, operations of the second type are carried out after fault detection to effect restoration. There are also such types of maintenance as scheduled and unscheduled, deferred; by a state – condition-based, automatic, remote, etc.

A term "Condition monitoring" was added. It deals with obtaining information about physical state or operational parameters of an item. It is used to define the necessity in preventive maintenance operations.

"Repair" is referred to corrective maintenance and is defined as direct action taken to effect restoration. It includes fault localization, fault diagnosis, fault correction and function checkout. During repair there are no technical, administrative and logistics delays.

"Restoration" is defined in IS as event at which the up state is re-established after failure. That is why the duration of the period when an item is in a down state after failure is called "time to restore". GOST 27.002–89 restoration (recovery) is defined as a process when an item is transferred from down state to upstate, which is why a term "restoration time" is used. Each rendering whether it is an event or a process has its pluses and minuses. In particular, IS approach gives a convenient twoness of terms: failure – restoration (both are events), time to failure – time to restore.

In IS 60050-191 a word "restoration" had a synonym word "recovery". But in IS 60050-192 it is introduced as an individual term with somewhat different sense:

restoration without corrective maintenance. It has a special case "self-recovery", a recovery without external intervention.

"Software maintenance" is also a new notion. It is modification for the purposes of software fault removal, adaptation to a new environment, or improvement of performance. It may be corrective, adaptive or perfective.

The sections related to "measures" have not changed significantly. We shall note that in contrast with GOST 27.002–89, IS gives a deeper differentiation for some measures. For instance, there is no general term "availability factor", but there is separate instantaneous availability, mean availability, steady state availability. Three factors of unavailability are defined in the same way.

Inherent availability and operational availability are also distinguished. Inherent availability is provided by the design under ideal conditions of operation and maintenance. Delays associated with maintenance, such as logistic and administrative delays, are excluded. Operational availability is experienced under actual conditions of operation and maintenance. Operational availability is determined considering down time due to failures and associated delays, but excluding external causes.

The sections about "tests: has been extended by supplementing with some new terms. They are: screening test – test carried out to detect and remove non-conforming items, or those susceptible to early life failure; black-box testing – testing in which test cases are chosen using only knowledge of the functional specification of the item under test; white-box testing – testing in which test cases are chosen using knowledge of the internal structure of the item under test; censoring – excluding from a particular assessment, data obtained either after a given duration or a given number of events, etc. Some special terms related to SW tests were added: software alpha test, software beta test, etc. But several terms were excluded. For instance a term "compliance test" remained but "determination test" was excluded.

The section about "design" has also been extended. It contains the remained terms: redundancy, active redundancy, standby redundancy, fail-safe, fault tolerance, fault masking. Some of them were given more exact definitions.

Several terms related to "redundancy", were added, for instance, diverse redundancy and m out of n redundancy. Some general terms were included: system reconfiguration, fault avoidance, self-checking, self-testing, as well as the terms specific to software: N-version programming, backward recovery, forward recovery. The last two terms mean error recovery in which a system is restored to a previous state, and in which a system is restored to a new state, respectively.

But the section related to the dependability analysis has been reduced. There are no more terms whose sense is clear without definitions, as well as some individual terms. Among the remained terms are prediction, failure modes and effects analysis; failure modes, effects and criticality analysis; fault tree; fault tree analysis; reliability block diagram; state-transition diagram. We shall note that the first two terms had a word "fault" instead of "failure" in the previous IS. The following terms were added into this section: allocation <of dependability requirements>, event tree analysis, life cycle costing.

The section about dependability improvement concepts was also revised in the similar way. Most terms of these sections that were mentioned in the previous IS have been excluded from the new one. Important terms included again: failure reporting, analysis and corrective action system – closed loop process used to improve dependability of current and future designs by feedback of testing, modification and use experience; root cause analysis – systematic process to identify the cause of a fault, failure or undesired event, so that it can be removed by design, process or procedure changes.

In conclusion it should be noted that although the Russian and international terminologies on dependability have much in common, there is still a big difference between them. It is explained by the fact that the standardization of dependability terminology in our country that started half a century ago developed for a long time in isolation form similar work world-wide. Unfortunately, there are still many experts who do not understand the importance of harmonization of the Russian and international standards. Due to such differences the creation of a new GOST to be harmonized with IEC 60050-192 is currently not possible. But nevertheless it is necessary to strive for a maximum possible convergence of the Russian and international terminologies.

To achieve this goal it is necessary not only to make the Russian standards most approximate to international ones, but also to work on the introduction of the accepted Russian terms and notions to IS. It required active participation of the Russian experts in the IS development, that should be not only remote (by correspondence), but also with attendance of meetings and sessions. However, we have to state once again that the contribution of the Russian experts to the development of IS 60050-192 was very low. The Russian experts, in particular the authors of [1], took part in the early stages of this work, but during the last five years there has been no participation, mainly due to the lack of financing.

References

1. Bogdanova G.A., Netes V.A. IEC/TC 56: standardization for dependability // Quality management methods. 2009. No. 5. P. 44–47.

2. Netes V.A., Tarasyev Y.I., Shper V.L. Topical issues of terminology standardization in dependability // Dependability. 2014. No. 2. P. 116–119.

3. Netes V.A., Tarasyev Y.I., Shper V.L. How we should define what "dependability" is // Dependability. 2014. No. 4. P. 3–14.

4. ITU-T Recommendation E.800 (09/08). Definitions of terms related to quality of service.

5. Netes V.A, Rezinovsky A.Y., Tarasyev Y.I., Ushakov I.A., Fishbein F.I., Shper V.L. Деградация вместо гармонизации // Standards and quality. 2011. No. 5.

6. Ushakov I.A. uncalled GOST // Quality management methods. 2011. No. 5.

About the author

Viktor A. Netes, Dr.Sci., Professor of the Moscow Technical University of Communication and Informatics, deputy chairman of Standardization technical committee No.119 "Industrial product dependability", Moscow, Russia, postal address: Aviamotornaya Str., 8a, Moscow, Russia, 111024, e-mail: vicnet@yandex.ru