Оригинальная статья
https://doi.org/10.21683/1729-2646-2021-21-2-24-27

Ошибки, неисправности и отказы

Игорь Б.Шубинский[1]*, Хендрик Шебе[2]
[1]АО «НИИАС», Москва, Российская Федерация, [2]TÜV Rheinland, Кельн, Германия
**igor-shubinsky@yandex.ru*

Игорь Б. Шубинский

Хендрик Шебе

Резюме. Цель. *Гармонизация русскоязычных и англоязычных определений ошибок, неисправностей, отказов. Объект статьи – одни из наиболее важных предметов изучения теории надежности и функциональной безопасности. Предмет статьи – понятия и определения отказов, ошибок, неисправностей.* **Результаты исследования.** *Проанализированы определения понятий, описывающих нарушения надежности и функциональной безопасности объектов в русскоязычных и международных стандартах, таких как ГОСТ 27.002-2015, ГОСТ Р/МЭК 61508-2012, IEC 60050, DIN 40041, а также в публикациях ряда авторов. Анализ показывает, что отказ всегда связан с потерей функции, то есть с возможностью выполнять работу так, как требуется по всем стандартам. Нужно отметить, что здесь неверное ожидание пользователя не подпадает под определение отказа. Отказ следует отличать от вводимых непреднамеренно функций. Неисправность определяется как неспособность системы в полной мере выполнять требуемую работу, которая может при определенных условиях перерасти в отказ. Ошибка – как несоответствие между вычисленным, наблюдаемым или измеренным значением или условием и истинным, заданным или теоретически правильным значением или условием – это отклонение, которое присутствует, но превратится, возможно, при определенных условиях в отказ. Типичный пример – некритичные ошибки программного обеспечения. Так называемые систематические отказы на самом деле являются ошибками, которые могут превратиться в критичные ошибки (отказы). Отметим, что определения в международном электротехническом словаре IEC 60050 могут быть использованы как демонстрирующие общее согласие, что не удивительно для международного стандарта.*

Ключевые слова: *отказ, неисправность, ошибка, сбой, повреждение, стандарт, термин, надежность, функциональная безопасность, событие, работа.*

Для цитирования: *Шубинский И.Б., Шебе Х. Ошибки, неисправности и отказы // Надежность. 2021. №2. С. 24-27. https://doi.org/10.21683/1729-2646-2021-21-2-24-27*

Поступила *20.10.2020 г. /* **После доработки** *10.04.2021 г. /* **К печати** *21.06.2021 г.*

1. Введение

Развитию терминологии в области надежности и безопасности уделено большое внимание (см., например, работы Нетеса, Похабова, Плотникова, Михайлова [1-5]. Не всегда эти термины достаточно хорошо отражаются в разных языках. В данной статье мы попытаемся дать представление о возможных определениях терминов *ошибка, неисправность, отказ*. Мы попытаемся сделать это параллельно на двух языках: английском и русском. Эта задача не из легких, так как не так много статей или книг существует в хороших двуязычных версиях. Во всяком случае, авторы попытаются в этой статье описать свой взгляд на терминологию. В разделе 2 приведен обзор ряда существующих определений и концепций. В третьем разделе дается краткий анализ ключевых терминов и предложено их определение в интерпретации авторов. В четвертом разделе приведено заключение.

2. Обзор существующих концепций

Определения терминов *неисправность* (иногда и *сбой*, см. [6]), *отказ и ошибка* можно найти в первую очередь в стандартах, касающихся терминов и определений. В стандарте IEC 60050 [7] рекомендуется использовать следующие определения:

отказ – потеря способности выполнять работу по мере необходимости;

неисправность – неспособность выполнить требуемое, обусловленное внутренним состоянием;

ошибка – расхождение между вычисленным, наблюдаемым или измеренным значением или условием и истинным, заданным или теоретически правильным значением или условием.

В межгосударственном стандарте ГОСТ 27.002 [8] имеет место следующее определение:

отказ – событие, заключающееся в нарушении работоспособного состояния объекта.

Эта интерпретация основывается на монографии – основной книге по надежности, написанной в 1965 г. Б.В. Гнеденко, Ю.К. Беляевым, Ю.Д. Соловьевым [9].

Отказ – это частичная или полная утрата или изменение таких свойств изделия, которые существенно ухудшают работоспособность или приводят к потере работоспособности.

Здесь можно отметить, что это определение данное в работе [9] также смогло определить неисправность. Но нужно признать, что за последние 55 лет произошла определенная эволюция терминологии, которую авторы не могли предвидеть. Это касается, в частности, определение термина *ошибка*.

В межгосударственном стандарте ГОСТ 27.002 [7] отсутствует определение ошибки, однако неисправность и дефект определены следующим образом:

неисправность – состояние объекта, при котором оно не соответствует хотя бы одному из требований, предъявляемых в документации на него;

дефект – каждое отдельное отклонение объекта от требований, определенных в документации.

Различия между этими определениями незначительны. Если неисправность – любое несоответствие заданным требованиям, то дефект – каждое конкретное несоответствие. В стандарте ГОСТ 27.002 определено понятие

повреждение как событие, заключающееся в нарушении исправного состояния объекта, при сохранении работоспособного состояния.

Это определение повреждения очень близко к определению неисправности согласно словарю IEC 60050 [7].

В качестве третьего источника используем статью Gayen & Schäbe [10, 11], которая была опубликована на двух языках, и поэтому терминология синхронизирована. Авторы частично заимствовали терминологию из DIN 40041 [12], которая, хотя и остается в силе, но устарела и больше не поддерживается. Это объясняет некоторые недостатки.

Отказ: физический определенный функциональный модуль прекращает выполнение функции в пределах указанной загрузки и условий окружающей среды.

Это определение связано с потерей предполагаемой функции и соответствует приведенным выше определениям. Однако сфера применения данного термина ограничивается элементом. Такое применение этого понятия на уровне системы может привести к недоразумениям, поскольку не обязательно характеризует отказ систем – на уровне системы это может быть связано с неисправностью. Однако определение неисправности, данное в той же статье, проясняет это.

Неисправность: потерянная или ошибочная функция, или неполное предоставление желательной функции модулем.

Важной частью обсуждения является различие между неисправностей и отказом. С одной стороны, неисправность – это частичная потеря функциональной способности или полная потеря функциональной способности, связанной с блоком или подсистемой, не обязательно приводящая к отказу системы. С другой стороны, неисправность может также возникнуть на системном уровне и ухудшить производительность системы. Поэтому важно различать систему и подсистему или блок. Мы должны отметить, что событие, которое может быть отказом подсистемы, может быть просто неисправностью на системном уровне, поскольку другие подсистемы могут, по крайней мере частично, компенсировать этот отказ подсистемы, чтобы сделать его просто неисправностью на системном уровне.

Chillarege [13] рассматривает отказ / сбой программного обеспечения как событие, когда ожидания клиента не оправдались. Фактически это следует из интерпретации отказа как полной или частичной потери функции системы, в данном случае вызванной программным обеспечением. Шубинский [14] отмечает, что само программное обеспечение в этом случае не вышло из строя, отказ происходит на системном уровне. Активируются только те части программного обеспечения, которые являются ошибочными, или активируется та часть

программного обеспечения, которая не в состоянии предоставить правильный ответ на команду системы.

Рэнделл [15] предлагает целую цепочку в виде

Отказ → Неисправность → Ошибка → Отказ и т. д.

Здесь термины повторяются, только связаны с более высоким уровнем в системе. Рэнделл использует следующие определения:

отказ системы происходит, когда поставляемая услуга отклоняется от выполнения функции системы, причем последняя является тем, на что нацелена система.

Это соответствует определению отказа, данному другими авторами.

Ошибка – это та часть состояния системы, которая может привести к последующему отказу. Ошибка, влияющая на услугу, является признаком того, что сбой уже произошел. Признанной или предполагаемой причиной этого является ошибка.

Итак, для Рэнделла *ошибка* – это отклонение как составная часть состояния системы. Кроме того, он видит в этом признак неисправности и определяет неисправность как причину ошибки. Такой подход представляется неоднозначным. В понимании авторов Рэнделл скорее описывает неисправность, когда объясняет, что такое ошибка. Риис [16] также поддерживает точку зрения, что

отказ – это потеря функции, т. е. элемент не работает, если он не сделал то, что мы хотим, и находится в исправном состоянии, если сделал, что мы хотели. Более точно, это функция, которая отказывает.

Обратите внимание, что речь не идет о том, является ли система физически неповрежденной или нет – отказавшая система может быть физически неповрежденной. Физически неповрежденная система также может выйти из строя из-за скрытой (нежелательной или неправильно спроектированной функции, см., например, Deckers & Schäbe [17]) или недекларированных функций, которые были вовлечены в систему непреднамеренно или намеренно.

Пархами [18] вводит список из 7 состояний: *идеальное*, *дефектное*, *неисправное*, *ошибочное*, *плохо функционирующий*, *деградированное*, *состояние отказа*. Система движется от состояния к состоянию, начиная от идеального и заканчивая отказом. По мнению авторов, некоторые обозначения состояний неоднозначны. Дефект может также означать неисправность, деградацию или отказ. Кроме того, вопрос заключается в том, как интерпретировать ошибочное состояние. Должен ли этот термин использоваться только для характеристики системы с ошибкой, где ошибка описывает отклонение от спецификации, встроенной в систему с самого начала, т.е. отклонение? По мнению авторов, количество состояний должно быть сокращено. Говоря об отказах, следует также упомянуть о разграничении, сделанном в МЭК 61508 [6] и других стандартах функциональной безопасности между понятиями «Случайные отказы аппаратных средств» и «Систематические отказы». Прежде всего, приведем определение отказа, неисправности (здесь употребляется сбой в переводе) и ошибки согласно МЭК 61508 [6] часть 4:

3.6.4: «отказ – прекращение способности функционального блока обеспечивать требуемую функцию или работу функционального блока любым иным способом, кроме требуемого»;

3.6.1: «сбой – ненормальное состояние, которое может привести к снижению или потере способности функционального блока выполнять требуемую функцию»;

3.6.11: «ошибка – расхождение между вычисленным, наблюдаемым или измеренным значением или условием и истинным, заданным или теоретически правильным значением или условием».

Сравнивая эти определения с определениями из других источников, можно увидеть, что отказы также рассматриваются как событие, при котором система или ее составная единица не обеспечивают желаемую функцию. Кроме того, сбой определяется как предвестник отказа – здесь как ненормальное состояние, то есть отклонение. Тем не менее, последствия будут отличаться на системном уровне. Это может быть частичная потеря способности. Поскольку используется термин «может», также возможно, что на системном уровне не происходит никаких последствий – только необходимость ремонта избыточного блока.

3.6.5: «случайный отказ аппаратных средств – отказ, возникающий в случайный момент времени, который является результатом одного или нескольких возможных механизмов ухудшения характеристик в аппаратных средствах»;

3.6.6: «систематический отказ – отказ, связанный детерминированным образом с какой-либо причиной, которая может быть исключена только путем модификации проекта либо производственного процесса, операций, документации, либо других факторов».

В этих двух определениях отказы различаются в зависимости от механизма, который их вызвал. Случайный отказ аппаратных средств связан с процессами старения и деградации. Напротив, систематический отказ связан с ошибками в процессах проектирования и т.д. Однако и эти отказы проявляются стохастическим образом [19], когда срабатывает механизм отказа, поэтому они детерминированы только в том смысле, что может быть указана одна четко определенная причина. Время возникновения во многих случаях является случайным. Эта случайность вызвана окружающей средой, которая вызывает случайное влияние. Чтобы быть точным, здесь следует различать два подвида:

а) система содержит ошибку, например программную ошибку. Другим примером может быть система, которая не способна выдерживать определенные высокие или низкие температуры, хотя они требованы. Нет никакого старения. Как только влияние активирует эту ошибку, система отказывает в произвольное время. Случайность обусловлена случайностью внешнего воздействия;

б) из-за ошибочных процессов система имеет узкое слабое место. Этим слабым местом является, например, снижение устойчивости к нагрузкам, воздействию окружающей среды и т.д. Примером могут служить механические детали с заниженными параметрами,

которые отказывают из-за усталости. Здесь фактически активируется механизм случайного отказа, вызванный ошибкой проектирования, которая была бы исключена в противном случае с помощью конструктивных решений, если бы компонент был достаточно прочным.

3. Анализ и выводы

Анализ ясно показывает, как следует интерпретировать неисправность, отказ и ошибку.

Отказ всегда связан с потерей функции, то есть с функцией как возможностью выполнять работу так, как требуется, во всех стандартах. Следует отметить, что это требование также может быть неявным, т.е. система функционирует не так, как ожидалось. Нужно отметить, что здесь неверное ожидание пользователя не подпадает под определение отказа. Отказ следует отличать от вводимых непреднамеренно функций (sneaks), (см., например, [17]).

Неисправность определяется как неспособность системы выполнять в полной мере требуемую работу, которая может при определенных условиях перерасти в отказ. Термин „fault“ допускает два разных перевода на русский язык (отказ, неисправность), которые используются параллельно в зависимости от документа.

Ошибка как несоответствие между вычисленным, наблюдаемым или измеренным значением или условием и истинным, заданным или теоретически правильным значением или условием – это отклонение, которое присутствует, но может превратится в отказ при определенных условиях. Типичный пример – некритичные ошибки программного обеспечения. Так называемые систематические отказы на самом деле являются ошибками, которые могут превратиться в критичные ошибки (отказы). Отметим, что определения в [6] могут быть использованы как демонстрирующие общее согласие, что не удивительно для международного стандарта.

Библиографический список

1. Нетес В.А. Объект в надежности: определение и содержание понятия // Надежность. 2019. Том 19. № 4. С. 3-7.

2. Нетес В.А., Тарасьев Ю.И., Шпер В.Л. Как нам определить что такое «надежность» // Надежность. 2014. Том 14. № 4. С. 3-14

3. Плотников Н.И. Разработка альтернативной терминологии надежности // Надежность. 2020. Том 20. № 3. С. 21-26.

4. Похабов Ю.П. О дефиниции термина «надежность» // Надежность. 2017. Том 17. № 1. С. 4-10.

5. Михайлов В.С. О терминах надежности // Надежность. 2020. Том 20. № 2. С. 24-27.

6. ГОСТ Р МЭК 61508. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. М.: Стандартинформ, 2014.

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

8. ГОСТ 27.002-2015. Надежность в технике. Термины и определения. М.: Стандартинформ, 2016. IV, 23 с.

9. Гнеденко Б.В., Беляев Ю.К., Соловьев Ю.Д. Математические методы в теории надежности. М.: Наука, 1965. 524 с.

10. Gayen J.-T., Schäbe H. (Mis-)conceptions of safety principles, // ESREL 2008, Proceedings Safety, Reliability and Risk analysis. 2008. Vol. 2. P. 1283-1291.

11. Гайен Й.Т., Шебе Х. Правильное и неправильное понимание принципов обеспечения функциональной безопасности // Надежность. 2009. № 3. С. 63-74.

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

13. Chillaregge R. What is Software Failure / Commentary in IEEE Transactions on Reliability, 45, no. 3, 1996.

14. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: Журнал Надежность, 2012. 296 с.

15. Randall B. On Failures and Faults // Conference Paper in 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. Vol. 46. No. 2. P. 163.

17. Deckers J., Schäbe H. Using Sneak Circuit Analysis in Aerospace Product Assurance // Qual. Rel. Eng. Int. 1993. Vol. 9. P. 137-142.

18. Parhami B. Defect, Fault, Error,…., Failure // IEEE Transaction on Reliability. 1997. Vol. 46. No. 4. P. 450-451.

19. Braband J., Schäbe H. Individual Risk, Collective Risk, and F–N Curves for Railway Risk Acceptance. /In: Handbook of RAMS in Railway systems – Theory and Practice, Qamar Mahboob, Enrico Zio (Eds.), 2018, Boca Raton, Taylor and Francis, chapter 8, p. 119-128.

Сведения об авторах

Игорь Борисович Шубинский – доктор технических наук, профессор, заместитель руководителя НТК АО «НИИАС», ул. Нижегородская, д. 27, стр.1, Москва, Российская Федерация, 109029, тел. +7 (495) 786-68-57; e-mail: igor-shubinsky@yandex.ru

Хендрик Шебе – доктор физико-математических наук, заведующий отделом анализа рисков и опасностей, TÜV Rheinland InterTraffic, Кельн, Германия, e-mail: schaebe@de.tuv.com

Вклад авторов в статью

Вклад авторов заключается в анализе терминологии отказ, неисправность / сбой и ошибка и их использование на русском и английском языках. Вклад авторов равный.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.