ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61069-5– 2012

Измерение и управление промышленным процессом Определение свойств системы с целью ее оценки Часть 5 Оценка надежности системы

IEC 61069-5:1994

Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability

(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации – ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Некоммерческим образовательным частным учреждением «Новая Инженерная Школа» (НОЧУ «НИШ») на основе аутентичного перевода на русский язык стандарта, указанного в пункте 4, который выполнен Российской комиссией экспертов МЭК/ТК 65

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 306 «Измерение и управление промышленными процессами»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2012 г. №1048-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61069-5:1994 «Измерение и управление промышленным процессом. Определение свойств системы с целью ее оценки. Часть 5. Оценка надежности системы» (IEC 61069-5:1994, «Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (пункт 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок – в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2013

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область назначения
2 Нормативные ссылки
3 Термины и определения
4 Свойства надежности
4.1 Общие положения
4.2 Надежность
4.3 Готовность
4.4 Безотказность
4.5 Ремонтопригодность
4.6 Достоверность
4.7 Защищенность
4.8 Целостность
5 Обзор документа «Требования к системе»
6 Обзор документа «Спецификация системы»
7 Процедура оценки
7.1 Общие положения
7.2 Анализ документов «Требования к системе» и «Спецификация системы»
7.3 Разработка программы проведения оценки
7.4 Программа проведения оценки
8 Методы определения свойств
8.1 Общие положения
8.2 Методы определения качественных характеристик свойств
8.3 Методы количественного определения свойств
9 Выполнение оценки и отчет об оценке
Приложение А (справочное) Пример требуемой информации и формата документации для задачи управления «ведущий – ведомый» в документе «Требования к системе»
Приложение В (справочное) Пример требуемой информации и формата документации для задачи управления «ведущий – ведомый» в документе «Спецификация системы»
Приложение С (справочное) Испытания достоверности

Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации .....

Библиография .....

Введение

МЭК 61069 состоит из серии публикаций, в которых данная публикация является пятой.

Часть 1 представляет собой общее руководство и в таком качестве является самостоятельной публикацией.

Часть 2 детализирует методологию оценки.

Части 3 – 8 представляют руководства по оценке определенных групп свойств.

Распределение свойств по частям от 3 до 8 было выбрано так, чтобы сгруппировать вместе связанные между собой свойства.

Полный набор документов всей серии стандартов включает в себя:

Часть 1. Общие подходы и методология.

Часть 2. Методология оценки.

Часть 3. Оценка функциональности системы.

Часть 4. Оценка производительности системы.

Часть 5. Оценка надежности системы.

Часть 6. Оценка эксплуатабильности системы.

Часть 7. Оценка безопасности системы.

Часть 8. Оценка свойств системы, не связанных с ее основным назначением.

Приложения А, В и С даны только для информации.

В настоящей части МЭК 61069 рассмотрен метод, который следует применять для оценивания надежности систем измерения и управления промышленным процессом.

Оценка системы является основанным на доказательстве суждением о пригодности системы для конкретного целевого назначения (миссии) или класса целевых назначений.

Для получения полного итогового доказательства потребовалось бы полное (т. е. при всех влияющих условиях) определение пригодности всех свойств системы для конкретного целевого назначения или класса целевых назначений.

Так как практически это требуется редко, то для оценки системы более рационально:

– определить критичность каждого из соответствующих свойств системы;

– спланировать определение соответствующих свойств системы с учетом критерия «цена – эффективность» для усилий по реализации этих свойств.

При проведении оценки системы следует стремиться к получению максимальной обоснованности пригодности системы с учетом целесообразной стоимости и ограничений по времени

Оценка может быть выполнена только в том случае, если целевое назначение (миссия) сформулировано (или задано) или если оно может быть определено или представлено гипотетически. В случае отсутствия миссии, оценка не может быть выполнена (как определено в МЭК 61069-1), тем не менее, определение свойств системы может быть выполнено для применения в оценках, выполняемых по-другому.

В таких случаях стандарт может быть использован как руководство для планирования и обеспечения процедурами определения свойств системы, которое представляет собой неотъемлемую часть оценки.

Взаимосвязь настоящей части с другими частями МЭК 61069 и ее место в составе серии МЭК 61069 показаны на рисунке 1.

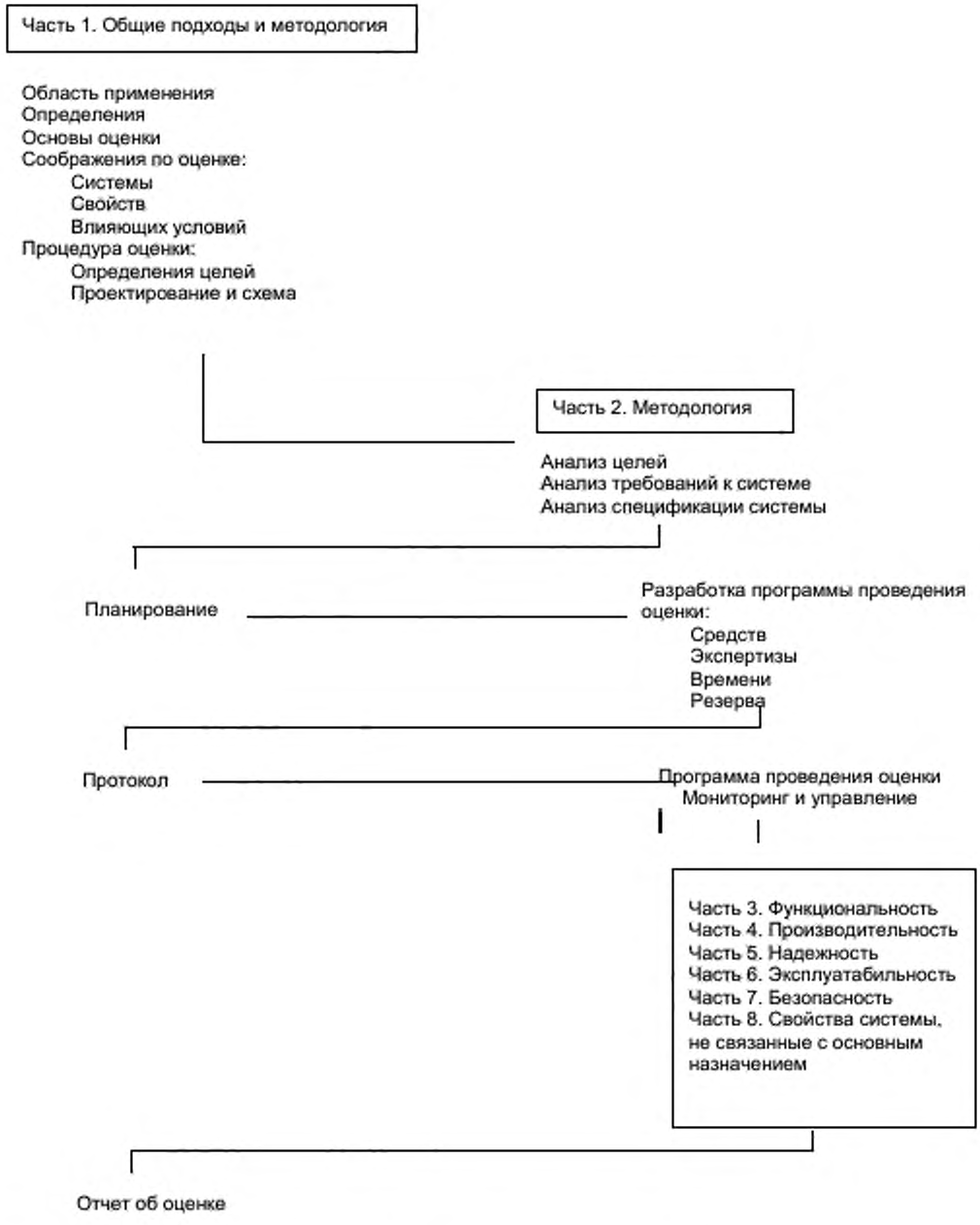


Рисунок 1 — Общий состав МЭК 61069

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Измерение и управление промышленным процессом Определение свойств системы с целью ее оценки Часть 5 Оценка надежности системы

Industrial-process measurement and control.
Evaluation of system properties for the purpose of system assessment.
Part 5: Assessment of system dependability

Дата введения – 2014–07–01

1 Область назначения

В настоящем стандарте изложен метод, используемый для систематической оценки характеристик систем измерения и управления промышленным процессом.

Детальная оценка методологии, представленная в МЭК 61069-2, применима для разработки программы оценки надежности.

В настоящем стандарте анализируют вспомогательные свойства надежности и описывают критерии, принимаемые во внимание при оценке надежности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Если указана дата публикации, то именно данное издание следует использовать. При отсутствии даты публикации используют последнее издание указанного документа, включая любые изменения.

МЭК 60050 (191):1990 Международный Электротехнический Словарь (МЭС). Глава 191: Надежность и качество обслуживания [IEC 60050 (191): 1990, International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service]

МЭК 60068 Испытание на воздействие внешних факторов (IEC 60068, Environmental testing)

МЭК 60300-3-2:1993 Управление надежностью. Часть 3. Руководство по применению. Раздел 1. Методики анализа для определения надежности. Руководство по методологии (IEC 60300-3-2:1993, Dependability management

Издание официальное

– Part 3: Application guide – Section 2: Collection of dependability data from the field)

МЭК 60706-4:1992 Электрооборудование. Руководство по ремонтопригодности. Часть 4. Раздел 8. Планирование технического обслуживания и его обеспечения (IEC 60706-4:1992, Guide on maintainability of equipment – Part 4 – Section 8: Maintenance and maintenance support planning)

МЭК 60801 Электромагнитная совместимость средств (оборудования) измерения и управления промышленным процессом (IEC 60801: Electromagnetic compatibility for industrial-process measurement and control equipment)

МЭК 60812:1985 Методы анализа надежности системы. Процедура для режима отказа и анализа воздействий (FMEA) [EC 60812:1985, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)]

МЭК 60863:1986 Представление надежности, ремонтопригодности и предсказаний пригодности (готовности) (IEC 60863:1986, Presentation of reliability and availability predictions)

МЭК 61000 Электромагнитная совместимость (EMC) [IEC 61000, Electromagnetic compatibility (EMC)]

МЭК 61025:1990 Анализ дерева ошибок (FTA) [IEC 61025:1990, Fault tree analysis (FTA)]

МЭК 61069-1:1991 Измерение и управление производственными процессами. Определение характеристик системы для ее оценки. Часть 1. Общие аспекты и методология (IEC 61069-1:1991, Industrial-process measurement and control – Evolution of system properties for the purpose of system assessment – Part 1: General considerations and methodology)

МЭК 61069-2:1993 Измерение и управление производственными процессами. Определение характеристик системы для ее оценки. Часть 2. Методология оценки (IEC 61069-2:1993, Industrial-process measurement and control – Evolution of system properties for the purpose of system assessment – Part 2: Assessment methodology)

МЭК 61070:1991 Сравнение процедур проверки на установленную готовность (IEC 61070:1991, Compliance test procedures for steady-state availability)

МЭК 61078:1991 Методы анализа надежности. Метод блок диаграмм безотказности (IEC 61078:1991, Analysis techniques for dependability – Reliability block diagram method)

МЭК 61132:199x Предсказание наступления отказа изделий, имеющих серийную структуру ряда [IEC 61132:199x, Failure rate prediction of items having a series structure (in preparation)]

МЭК 61165:1995 Применение методики Маркова для анализа общей надежности [IEC 61165:1995, Application of Markov techniques (in preparation)]

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

Определения, отмеченные * являются идентичными тем, которые приведены в МЭК 60050 (191). Чтобы определения были поняты правильно во всех частях МЭК 61069, к этим определениям приведены комментарии в примечании в конце этого раздела.

3.1 **надежность** (dependability): Степень, с которой на систему можно полагаться в части полного и правильного выполнения задачи в данных условиях в данный момент времени или на данном интервале времени, в предположении доступности необходимых внешних ресурсов.

3.2 **безотказность** (reliability)*: Свойство изделия выполнять требуемую функцию при данных условиях на данном интервале времени.

3.3 **ремонтопригодность** (maintainability)*: Свойство изделия в данных условиях использования, оставаться исправным или восстанавливаться в состояние, в котором оно может выполнять требуемую функцию, при выполнении в данных условиях обслуживания и обеспечении установленных процедур и ресурсов.

3.4 **готовность** (availability)*: Свойство изделия выполнить требуемую функцию в данных условиях в данный момент или на данном интервале времени, в предположении, что требуемые внешние ресурсы обеспечиваются.

3.5 **целостность** (integrity): Гарантия того, что задачи, решаемые системой, будут выполнены правильно, если не поступит уведомления о том,

что система находится в состоянии, которое может привести к обратному (т.е. к невыполнению).

3.6 **защищенность** (security): Гарантия того, что в систему не будет подан неправильный входной сигнал или осуществлен неправомочный доступ к системе.

3.7 **достоверность** (credibility): Степень, с которой система обладает свойством распознать отклонения в состоянии системы и сигнализировать об этом, а также противостоять ошибочным входным сигналам или неправомочному доступу.

Примечание — Для настоящего стандарта принимается что:
- изделие является системой измерения и управления промышленным процессом;
- требуемая функция является задачей. В случае определения свойства, задачу следует понимать как задача системы. Задача и функция определены в 2.2.4 и 2.2.5 МЭК 61069-1.

4 Свойства надежности

4.1 Общие положения

Для того чтобы система была надежной, необходимо чтобы она была готова выполнить свои функции. В общее понятие готовности входят зависимость от интенсивности отказов системы (безотказность) и время, необходимое для восстановления системы (ремонтопригодность).

Однако практически это не означает, что когда система готова выполнить свою функцию, то есть уверенность в том, что функция будет выполнена правильно.

Этот аспект достоверности зависит:

– от способности системы обеспечить предупредительную сигнализацию в случае, когда она находится в состоянии, в котором не может выполнить некоторые или все свои функции правильно (целостность);

– от способности системы отклонить любые неправомерные входные сигналы или предотвратить несанкционированный доступ к системе (защищенность).

Для того чтобы оценить надежность системы, необходимо, прежде всего идентифицировать и оценить дополнительные составляющие свойства, которые определяют надежность.

Отношение между надежностью и ее составляющими свойствами показано на рисунке 2.



Рисунок 2 — Составляющие свойства надежности

4.2 Надежность

Надежность не может быть оценена непосредственно. Необходимо оценить каждое составляющее свойство отдельно.

Каждое составляющее свойство зависит от архитектуры расположения модулей системы и свойств этих модулей.

Отношение составляющих свойств надежности этих модулей к надежности системы может быть очень сложным.

Каждое составляющее свойство на уровне системы может зависеть от нескольких составляющих свойств на уровне модуля.

Например:

– если архитектура системы включает избыточность, то готовность системы зависит от свойства целостности избыточных модулей;

– если архитектура содержит механизмы защищенности системы, то защищенность системы зависит от свойства готовности модулей, которые реализуют механизм защиты;

– если архитектура содержит модули, которые проверяют данные, передаваемые от других частей системы, то целостность системы зависит от свойств защищенности этих модулей.

Надежность не может быть описана просто количественно (числом). Некоторые из ее свойств могут быть выражены как вероятности, другие свойства детерминированы; некоторые могут быть определены количественно, другие аспекты могут быть выражены только в качественном виде.

Когда система выполняет несколько системных задач, ее надежность может очень сильно влиять на решение этих задач. Поэтому для каждой из этих задач требуется отдельный анализ.

4.3 Готовность

Готовность системы зависит от готовности отдельных частей системы и способа, которым эти части взаимодействуют при выполнении задач системы. Способ, которым обеспечивается взаимодействие частей, может включать функциональную избыточность (гомогенную или разнообразную), функциональные отступления и деградацию. Готовность практически зависит от используемых процедур и ресурсов, доступных для поддержания системы. Готовность системы может отличаться для каждой из ее задач. Готовность системы для каждой задачи может быть определена количественно двумя способами.

4.3.1 Прогнозируемое значение готовности системы, может быть рассчитано так:

$$\text{Готовность} = \frac{\text{среднее время до отказа}}{\text{среднее время до отказа} + \text{среднее время восстановления}}$$

где:

– «готовность» – готовность системы для выполнения данной задачи;

– «среднее время до отказа» – среднее время с момента перехода системы в состояние готовности выполнения данной задачи до момента времени, когда система будет не в состоянии ее выполнять (до отказа);

– «среднее время восстановления» – среднее время, требующееся для восстановления системы в состояние готовности выполнения заданной задачи с момента времени, когда система не смогла выполнять задачу.

4.3.2 Для системы, находящейся в эксплуатации, готовность может быть рассчитана так:

$$\text{Готовность} = \frac{\text{время, за которое система в состоянии выполнить задачу}}{\text{время, за которое система, как ожидалось, выполнит задачу}}$$

4.4 Безотказность

Безотказность системы зависит от безотказности отдельных частей системы и способа, которым эти части взаимодействуют при выполнении задачи системы. Способом, взаимодействия частей может быть функциональное дублирование (однородное или многообразное), функциональное резервирование и снижение эффективности.

Безотказность системы может быть различной для каждой из ее задач. Безотказность может быть определена количественно для отдельных задач с различными степенями доверительности.

Безотказность отдельных частей вычислительных средств системы может быть предсказана методом расчета безотказности составных частей данной системы. В этом случае, безотказность системы может быть предсказана синтезом. Следует отметить, что для модулей программного обеспечения систем нет доступных методов предсказания безотказности, которые обеспечивают высокий уровень доверительности.

4.5 Ремонтопригодность

Ремонтопригодность системы зависит от ремонтопригодности отдельных частей, физической и функциональной структур системы. Физическая структура определяет легкость доступа, заменяемость и т. д. Функциональная структура определяет простоту диагностики и т. д.

При количественном определении ремонтопригодности системы, должны быть учтены все действия, требуемые для восстановления состояния системы, в котором она способна полностью выполнять задачи. Также должны быть учтены затраты времени, которые необходимы для обнаружения ошибки, подготовки к техобслуживанию и ремонту, проведения диагностики и исправления причины отказа, настройки и проверки, и т. д.

Количественное определение ремонтопригодности следует дополнять описательными заключениями по проверке обеспечения, и учета следующих моментов:

– оповещение о возникновении отказов: световая сигнализация, аварийные сообщения, отчеты и т. д.;

– доступ: простота доступа для персонала и для подключения измерительных приборов, модулей, и т. д.;

– диагностика: прямая идентификация ошибки, диагностические инструменты, которые не оказывают никакого влияния на систему, удаленные средства поддержки обслуживания, статистическая ошибка проверки и передачи сообщений;

– ремонтопригодность/заменяемость: модульность, однозначная идентификация модулей и элементов, минимальная потребность в специальных инструментах, минимальные последствия от других элементов или модулей, когда элементы или модули заменены;

– контроль: инструкции по процедурам обслуживания, минимальные требования контроля.

4.6 Достоверность

Достоверность системы зависит от целостности и механизмов защищенности, реализуемых как функции, выполняемые элементами системы.

Механизм целостности осуществляется элементом, проверяющим выходы других элементов.

Механизм защищенности осуществляется элементом, проверяющим входы к другим элементам.

Механизмы достоверности содержат:

a) проверка:

– правильности выполнения функций (например, устройством обеспечения безопасности, используя известные данные); и/или

– корректности данных (например, проверка правильности, контроль по четности и т. д.):

b) операции типа:

– самонастройка;

– защита данных;

– извещение об операции и т. д.

Эти механизмы могут быть использованы для обеспечения целостности и/или защищенности.

Для анализа механизмов достоверности могут использоваться методы внесения ошибки, описанные в 8.3.2.2.

Достоверность детерминирована, и поэтому некоторые аспекты могут быть определены количественно.

4.7 Защищенность

Защищенность системы зависит от механизмов, применяемых на границе системы, чтобы обнаружить и предотвратить некорректные входные сигналы и несанкционированный доступ.

Защищенность детерминирована, и некоторые аспекты могут быть определены количественно.

4.8 Целостность

Целостность зависит от механизмов, применяемых в выходных элементах системы, чтобы проверить корректность выходных сигналов. Она также зависит от механизмов, действующих в пределах системы для обнаружения и предотвращения некорректных передач сигналов или данных между частями системы. Эти внутренние механизмы определяют целостность или механизмы защищенности для зависимых частей, каждая из которых может рассматриваться как отдельная система.

Целостность детерминирована, и поэтому некоторые аспекты могут быть определены количественно.

5 Обзор документа «Требования к системе»

Документ «Требования к системе» (далее – ДТС) следует использовать для контроля за тем, что все задачи, которые должна выполнять система, и соответствующие требования к надежности представлены и документированы в соответствии с МЭК 61069-2.

Если целью является обеспечение безопасности процесса и требуется система для выполнения задач, связанных с безопасностью, то необходимо проверить требования к системе на соответствие МЭК 61508 (приложение D).

Эффективность оценки надежности зависит от полноты установленных требований и результатов рассмотрения отказов.

По этой причине ДТС должен быть рассмотрен для проверки того, что для каждой из задач системы установлены:

- относительная важность задачи;
- определение того, как рассматривается отказ задачи;
- критерии отказа в терминах свойств надежности;
- эксплуатационная и операционная среда.

Там, где характеристика надежности зависит от человеческого фактора, ее следует описывать должным образом и определять количественно (если это возможно), чтобы определить надлежащую оценку его влияния.

Чтобы установить обеспечение необходимой информацией, требования надежности должны рассматриваться для конкретных задач и относительно полного целевого назначения системы.

В приложении А приведено руководство, регламентирующее тип информации и форму изложения документа ДТС, которое позволяет оценить свойства надежности.

6 Обзор документа «Спецификация системы»

Документ «Спецификация системы» (далее – ДСС) следует использовать для контроля за тем, что свойства надежности для каждой требуемой задачи внесены в перечень в соответствии с МЭК 61069-2.

Особенное внимание следует уделить проверке наличия информации по следующим аспектам:

- функции системы, поддерживающие каждую задачу, модули, элементы, технические средства и программное обеспечение, обеспечивающие реализацию каждой из этих функций;
- альтернативные маршруты, поддерживаемые системой, для выполнения каждой задачи, и способы их активации;
- механизмы обеспечения достоверности (защищенности и целостности) и способы их поддержки;
- безотказность и готовность каждой задачи, также как функций поддержки, модулей и элементов;
- характеристикам ремонтопригодности;

– эксплуатационные характеристики, свойствам окружающей среды и границы применения модулей и элементов.

В приложении В приведено руководство, регламентирующее тип информации и форму изложения ДСС, которое позволяет оценить свойства надежности.

7 Процедура оценки

7.1 Общие положения

Оценку следует выполнять в соответствии с процедурой, изложенной в МЭК 61069-2 (раздел 7).

Цель оценки должна быть четко сформулирована руководствуясь положениями МЭК 61069-1 (пункт 4.1).

Информацию в документах ДТС и ДСС следует излагать полно и точно для того, чтобы можно было оценить надежность.

Если на какой-либо стадии оценки выявится, что в информации что-то пропущено или изложено неполно, следует обратиться с соответствующими вопросами к разработчику ДТС и ДСС для того, чтобы откорректированную информацию можно было использовать в дальнейшем.

Перечень вопросов, которые должны быть рассмотрены, приведен в МЭК 60863.

7.2 Анализ документов «Требования к системе» и «Спецификация системы»

7.2.1 Сравнение информации в документах

Для оценки свойств, не связанных с целевым назначением системы, информация, относящаяся к этим свойствам, должна быть выбрана из ДТС и ДСС в соответствии с МЭК 61069-2 (пункт 7.2).

Свойства надежности, требуемые для каждой из задач, а также влияющие условия, при которых эта надежность требуется, должны быть получены из ДТС в количественном и/или качественном виде.

Каждую задачу следует описывать для входов, выходов и операций.

Для каждого входа следует указать:

– допустимые состояния и соответствующие допустимые выходные состояния;

– недопустимые состояния и соответствующие требуемые действия.

Для каждого выхода следует указать:

– допустимые состояния;

– недопустимые состояния и соответствующие требуемые действия.

Для каждой из задач следует четко указать:

– что представляет собой отказ;

– допустимая интенсивность отказов;

– действие, которое должно быть предпринято;

– максимальное допустимое время для возврата задачи в исходное состояние;

– насколько приемлемы влияющие условия, как это определено в МЭК 61069-1.

Всю информацию, касающуюся требований надежности и данных по надежности системы, следует рассматривать вместе и с учетом взаимного влияния, чтобы составить точные и лаконичные заключения относительно:

– функциональных границ системы;

– условий, при которых система не выполняет требования;

– обеспечения, функций, предназначенных для выполнения требуемых задач и альтернативных путей передачи данных, связывающих функции для поддержания требуемых задач;

– распределение функций, связывающих модули системы и элементы с данными их свойств надежности;

– имеющихся знаний и в какой мере следует оценивать свойства надежности.

Анализ должен включать исследование, каким образом альтернативные пути в системе инициируются:

– статическим способом с изменением конфигурации системы; или

– динамически или автоматически, например, механизмами достоверности или вручную, например, через клавиатуру.

7.2.2 Влияющие условия

На надежность системы могут воздействовать следующие факторы, перечисленные в МЭК 61069-1 (пункт4.4):

– задача, выполняемая системой, приводящая, например, к перегрузке системы и т. д.;

– процесс, связанный с системой, создающий, например, электрические помехи;

– внешние системы, связанные с заданной системой, создающие, например, электрические помехи и т. д.;

– средства поддержки (воздух, электроснабжение и т. д.), обслуживающие систему, в результате, например, изменения напряжения;

– окружающая среда, в которой размещена система: влажность, температура, и т. д.

Следующие основные факторы воздействуют на:

a) безотказность:

– средства обеспечения (электроснабжение и т.п.), обслуживания, влияние: использование данных об интенсивности отказов, предназначенных для предсказания надежности компонентов в электронном оборудовании,

– окружающая среда,

– услуги, связанные с техническим обслуживанием, хранением информации и т. д.;

b) ремонтопригодность, которую в настоящем стандарте рассматривают как внутреннее свойство самой системы, подвергающейся воздействию не прямо, а только косвенным образом, например, какие-то опасности внутри системы могут привести к ограничению доступа к некоторым частям системы;

c) готовность, которая:

– связана с зависимостью от деятельности человека по поддержанию системы в рабочем состоянии, когда она может выполнять требуемую задачу(и),

– находится под влиянием поведения человека и условий обслуживания (задержка поставки запасных частей, обучение, документирование и т. д.);

d) достоверность, на свойства защищенности и целостности которой могут воздействовать:

– преднамеренные или неумышленные действия человека, и, если при этом используются обычные средства обслуживания типа шин или многозадачных процессоров, то эти свойства могут находиться под влиянием задач системы, из-за внезапного возрастания активности промышленного процесса (например, при аварийной ситуации) и т. д., а также

– внешние системы.

Любые отклонения от рекомендованных состояний, в которых система, как предполагается, работает, могут сказываться на правильности функционирования системы.

При проведении конкретных испытаний для определения результатов воздействия влияющих условий, следует применять следующие стандарты:

– МЭК 60068;

– МЭК 60801;

– МЭК 61000.

7.2.3 Документирование сравниваемой информации

Сравниваемую информацию, как указано выше, следует документировать по форме, которая может изменяться в процессе разработки программы проведения оценки.

Примеры документирования информации приведены в приложениях А и В.

7.3 Разработка программы проведения оценки

7.3.1 Сравнение документов «Требования к системе» и «Спецификация системы»

Началом в разработке программы проведения оценки является анализ информации, собранной из ДТС и ДСС, как указано в 7.2.

Сравнивая ДТС и ДСС, как это указано в 7.2, строится позадачный перечень всех предложенных функций и средств, для выполнения требований к свойствам, не связанным с целевым назначением.

Каждая позадачная запись в этом перечне является потенциальным компонентом оценки.

Каждый потенциальный компонент оценки должен быть исследован, чтобы определить, в какой степени этот компонент должен быть оценен для получения требуемого увеличения уровня доверительности.

7.3.2 Компоненты оценки

Подготовленный перечень компонентов оценки подвергается сокращению с помощью следующих фильтров:

– важность задачи для целевого назначения;

– существующий уровень доверительности, основанный на знаниях и опыте, полученных при успешной эксплуатации системы с подобной или идентичной задачей, опыте изготовителя, опыте работы потребителей с тем же самым типом системы или с аналогичными системами;

– совершенство системы, основанное на определенной новизне системы, количестве систем, находящихся в эксплуатации, уровне стандартизации устройств, интерфейсов, операционной системы и языка программирования. Такими стандартами могут быть международные стандарты, национальные или корпоративные;

– уровень взаимозависимости различных функций, количество интерфейсов, повторное использование тех же самых функций в различных задачах;

– технические ограничения размера, веса, готовность обслуживания, мониторинг состояния окружающей среды.

7.3.3 Действия по проведению оценки

Перечень действий по проведению оценки для каждого компонента оценки из сокращенного перечня, указанного в 7.3.2, формируют с учетом:

– типа анализов и требуемых испытаний;

– знаний и навыков, требуемых при выполнении каждого анализа и/или испытания;

– ограничений на график проведения оценок, когда испытания других свойств могут повлиять на оценку свойств;

– готовности отобранного персонала;

– оборудования и утилит, требуемых для выполнения анализа и испытаний;

– оценки стоимости и времени для каждого анализа и испытания;

– приоритетности каждого действия оценки.

В зависимости от критериев, указанных в 7.3.1 и 7.3.2, может быть следует рассмотреть несколько методов определения свойств, которые взаимно дополняют друг друга.

Перечень «Действия по проведению оценки» следует применять с подобными перечнями, сформированными для оценки других свойств, с целью выполнения всей программы оценки системы.

7.4 Программа проведения оценки

В окончательной программе проведения оценки следует точно определить и/или перечислить:

– дедуктивный, качественный анализ надежности системы, как это описано в 8.2;

– критерии, которые принимаются во внимание, как это изложено в 7.2;

– действия по оценке приведенные в 7.3.3;

– варианты отказа, которые будут проанализированы и/или оценены, а также их ожидаемые результаты;

– целостность и механизмы защищенности, обеспеченные в системе;

– требуемое увеличение уровня доверительности;

– график проведения оценок, учитывающий постоянные воздействия, которые могут иметь место при испытаниях.

8 Методы определения свойств

8.1 Общие положения

Методы определения свойств, которые нужно использовать, следует выбрать так, чтобы результаты можно было сравнить количественно и/или качественно с данными, определенными в ДТС.

Отобранные методы могут быть аналитическими, использующими только документацию системы, или эмпирическими, требующими доступа к созданной системе.

Результаты определения свойств различными методами могут быть количественными, качественными или их комбинацией.

В настоящем стандарте предложено несколько методов определения свойств. Другие методы также могут применяться, но во всех случаях, в отчете об оценке следует приводить ссылки на документы, описывающие использованные методы.

Перечень аспектов, которые следует рассмотреть для оценивания, приведен в МЭК 60863. Аналитические методы, описанные ниже, основаны на использовании моделей. Такие модели редко могут достаточно точно описывать реальную систему. Даже в случае полного описания, нет уверенности в их 100 % точности. Поэтому результаты, основанные на аналитических методах, следует дополнять данными о степени их доверительности.

Надежность системы зависит также от ошибок на стадиях проектирования, спецификации и производства системы. Это одинаково справедливо для технических средств и программного обеспечения системы. Такие ошибки могут быть обнаружены только при тщательной проверке и надлежащем выполнении каждой функции.

Кроме того, применяют метод внесения гипотетических отказов или ошибок в систему, которые являются методическими, для увеличения степени доверительности при окончательной оценке надежности готовой системы. Такие методы внесения ошибок (с использованием средств автоматизации и/или специально разработанных программ) применяют с

целью выявления последствий от гипотетических отказов или ошибок для задач(и) системы.

Тем не менее увеличение степени доверительности практически ограничено, так как число испытаний, которые могут быть запланированы и выполнены, будет ограничено числом всех возможных отказов и ошибок, которые можно ожидать и, кроме того, ввести дополнительно.

8.2 Методы определения качественных характеристик свойств

Определение качественных характеристик свойств основано на прогнозирующем анализе или на результатах испытаний.

В обоих случаях определение необходимо начинать с анализа функциональной и физической структуры системы и того, как задачи выполняются системой.

Структура системы может быть описана с использованием схем функциональных и физических блоков, схем маршрутов прохождения сигналов, графов состояний, таблиц и т. д.

Режимы отказа рассматривают для всех элементов системы (технических средств и программного обеспечения) и определяют их влияние на надежность выполнения задач системы, а также на требований к ремонтопригодности.

Качественный анализ может быть выполнен с применением одного или комбинации из следующих методов.

8.2.1 Индуктивный анализ

Режимы отказа идентифицируют на уровне компонента или элемента, и для каждого из этих режимов анализируют на более высоком уровне соответствующее влияние на надежность выполнения задач системы. Результирующее воздействие отказа приводит к режимам отказа на следующем более высоком уровне.

Этот подход «снизу-вверх» – трудоемкий метод, который, в конечном счете, заканчивается идентификацией воздействий на всех уровнях системы для всех постулированных режимов отказов.

Соответствующий индуктивный метод анализа описан в МЭК 60812.

8.2.2 Дедуктивный анализ

При дедуктивном анализе рассматривают гипотетический отказ на самом высоком уровне системы, то есть отказ выполнения задачи с последовательным рассмотрением более низких уровней.

Следующий более низкий уровень анализируют для идентификации режимов отказа и связанных отказов, которые привели бы к идентифицированному отказу на самом высоком уровне, то есть на уровне задачи.

Анализ повторяют с прослеживанием обратного прохождения через функциональные и физические части системы до тех пор, пока анализ не приведет к получению достаточной информации для оценки в терминах надежности (включая ремонтопригодность).

Дедуктивный анализ не дает никакой информации относительно режимов отказа, которые не рассматриваются как события. Тем не менее, его применение очень эффективно по временным затратам для сложных систем, для которых более удобно описать то, что называется отказом системы или успешным выполнением задачи, чем рассматривать все возможные режимы отказов составляющих элементов системы.

Соответствующий дедуктивный метод анализа описан в МЭК 61025.

8.3 Методы количественного определения свойств

Количественное определение свойств может быть основано на прогнозирующем анализе, и расчетах или на испытаниях.

В обоих случаях определение необходимо начинать с анализа функциональной и физической структуры системы и того, как задачи выполняются системой.

Структура системы может быть описана с использованием схем функциональных и физических блоков, схем маршрутов прохождения сигналов, графов состояний, таблиц и т. д.

Количественный анализ может быть выполнен с применением одного или комбинации из следующих методов.

8.3.1 Прогнозируемое определение свойства

Прогнозируемое определение свойства основано на анализе качественных характеристик, дополненном определением количественной оценки безотказности (интенсивности отказов) элементов системы. Чтобы определить интенсивность отказов системы при выполнении задач(и), требуется применение прогнозирующего анализа. Соответствующий метод приведен в МЭК 61078.

Схема безотказности блока может быть построена, практически непосредственно исходя из функциональной и физической структур системы. Метод направлен, прежде всего, на анализ успешного выполнения задачи (с двумя устойчивыми состояниями) и не касается влияния ни сложного ремонта, ни стратегий обслуживания, ни других ситуаций с несколькими устойчивыми состояниями.

Различные математические инструменты пригодны для вычисления интенсивности отказов – типа булевой алгебры, таблиц истинности и/или траектории и анализа секущего множества. Для количественного прогноза интенсивности отказов системы при выполнении задачи в ситуации, характеризующейся большим числом состояний, может быть использована методика Маркова, приведенная в МЭК 61165.

Тем не менее, применение методики Маркова становится очень сложным, если нужно рассматривать большое количество состояний системы. В таких случаях более эффективно применить анализ Маркова для расчета данных по безотказности для подгрупп моделей анализа, полученных одним из других методов анализа, например, таким как «анализ дерева неисправностей».

Основные количественные данные по интенсивности отказов модулей и элементов, используемых в вышеупомянутых методах анализа, могут быть получены из опыта эксплуатации или методом «прогнозирования безотказности частей», используя общие данные для компонентов модулей и элементов. Метод прогнозирования безотказности частей приведен в МЭК 61132.

Метод учета частей базируется на условии, что компоненты функционально связаны последовательно (худшая оценка события). Компоненты модулей и элементов системы внесены списком в модуль или элемент, установленный для каждого компонента этого типа,

соответствующий ему поток отказов, факторы, влияющие на интенсивность отказов (качество, окружающая среда и т. д.) и обычно порядковый номер.

Состав данных о каждом компоненте всех модулей и элементов системы содержит тип этого компонента, интенсивность отказов, факторы, влияющие на интенсивность отказов (качество, окружающая среда и т. д.) и использованный порядковый номер.

Для сложных систем типа измерения и управления промышленным процессом практически невозможно сделать точный прогноз оценки свойств надежности.

Однако отдельные точные предсказания безотказности могут быть сделаны для тех частей системы, которые выполняют достаточное количество операций и дают возможность собрать корректные с точки зрения статистики данные об их эксплуатации.

Свойства системы – ремонтопригодность, защищенность, и целостность зависят, главным образом, от особенностей проектируемой системы, и, следовательно, степень их осуществления не может быть рассчитана на основе вероятностного подхода. Должна быть рассмотрена безотказность элементов, используемых для оценивания защищенности и целостности. Методы, которыми обычно оценивалась надежность этих элементов, могут быть теми же, поскольку они применялись для элементов и модулей, поддерживающих основные функции системы.

8.3.2 Тестирование свойств надежности

8.3.2.1 Введение

Оценка безотказности и готовности сложной системы исключительно на основании результатов этапа испытаний, практически ни корректна, ни рентабельна. В общем, каждая сложная система является уникальной (особенно когда образец существует в единственном экземпляре). Кроме того, объем таких испытаний будет ограничен по обеспечению и строго ограничен по времени, отводимому для испытаний. Однако, для систем, которые уже эксплуатируются, такие испытания представляют ценную информацию.

Полученные при этом фактические данные могут быть полезными для:

– совершенствования будущих проектов, структуры системы, модернизации или замены устаревшего оборудования и программного обеспечения;

– сравнения с ожидаемыми или заданными характеристиками;

– использоваться для прогнозирования показателей надежности.

Руководство по процедурам, которым нужно следовать при определении метода испытаний приведено в МЭК 61070 и МЭК 60300-3-2.

Главная цель проведения испытаний систем состоит в том, чтобы определить поведение системы (технических средств и программного обеспечения) при возникновении ошибки, или несанкционированного или неправильного доступа (защищенность и целостность).

Для того чтобы наблюдать поведение системы должны быть определены типовая задача или конкретный набор задач и для каждой задачи установлены состояния системы, которые рассматриваются как отказ [например, состояние выхода(ов)]. Руководство по проведению таких испытаний приведено в МЭК 60706-4.

8.3.2.2 Испытания методами внесения ошибки

До испытания методами внесения ошибки, спецификация системы должна быть исследована, чтобы определить:

– мероприятия по обеспечению целостности, предотвращающие распространение ошибок внутри систем;

– мероприятия по защищенности, предотвращающие ошибочные или несанкционированные вхождения в систему;

– наличие диагностических возможностей.

Для эффективного по времени проведения испытаний, проект испытаний системы должен быть основан на анализе качественных характеристик и, насколько возможно, должен использовать диагностические возможности, предусмотренные в самой системе и пригодные для системы. Когда диагностические возможности необходимы для обеспечения надежности системы, должна быть проявлена осторожность, и сами эти возможности должны пройти отдельную проверку.

Для проверки целостности ошибки могут быть внесены в модуль(и), элемент(ы) и/или компоненты, и проведены наблюдения за тем действительно ли:

- отказывают выходы системы; и/или
- имеется сообщение об ошибке.

Чтобы проверить защищенность, в систему могут быть внесены ошибки или несанкционированная информация, то есть поступили некорректные входные данные, совершена ошибка в действиях человека при эксплуатации и/или обслуживании.

При проверке целостности и защищенности должна быть проявлена осторожность при проведении некоторых одновременных испытаний. Единственным действием по предотвращению ошибки в пределах системы может быть обнаружение ошибки на входе. В приложении С приведен ряд ошибок, которые могут быть обнаружены при проведении этих испытаний.

8.3.2.3 Испытания влияния окружающей среды

Некоторые воздействия влияющих условий могут вызывать срабатывание механизмов обеспечения защищенности.

Поэтому выбранные влияющие условия должны быть различными относительно их нормальных значений для того, чтобы проверить механизмы защищенности.

Выбор влияющих условий в соответствии с 7.2.2.

9 Выполнение оценки и отчет об оценке

Выполнение оценки и подготовку отчета об оценке следует проводить в соответствии с МЭК 61069-1 (пункты 5.5 и 5.6).

В отчет об оценке следует включить:

a) план оценки, вместе с необходимыми отклонениями;

b) сопоставление данных из ДТС и ДСС таких, как задачи системы, требования надежности, окружающей среды, условии эксплуатации и обслуживания и т. д.;

c) анализ системы:

– физическая и функциональная структура системы, нагрузки, модулей системы, элементов и компонентов, обоснование выбора модели (ей) для различных аспектов оценки надежности;

d) адаптация моделей:

– (если необходимо) для прогнозирования надежности, принимая во внимание требуемую точность;

e) сбор данных, например исходных материалов, используемых для математических моделей;

f) расчеты с согласованной точностью результатов;

g) проведенные испытания:

– описание испытаний и обоснование выбора видов испытаний,

– методы моделирования отказов,

– ожидаемые характеристики качественного анализа,

– ожидаемая интенсивность отказов, полученная из количественного анализа,

– тип ошибок, внесенных в систему для проверки целостности и защищенности для моделирования отказов модуля, элемента или компонента;

– тип ошибок, определяемых через элементы входа/выхода; отказы из-за ошибок человека (например, в результате действий по обслуживанию);

– ошибки, возникающих в результате некорректных действий (например, использование недействительных кодов),

– характер и уровень влияющих условий, возможных в границах системы,

– объем ошибок,

– время распознавания ошибки,

– локализация ошибки (разрешение проблемы),

– время локализации ошибки,

– проверка правильности диалоговой диагностики, например, действительно ли аварийная сигнализация ложная, ошибка системы, имеющая отношение к функционированию промышленного процесса и т. д. выявлена верно, и/или идентифицированы неправильно;

h) перечень действий по оценке, рекомендуемых для дальнейшего анализа и/или испытаний.

Приложение А
(справочное)

Пример требуемой информации и формата документации для задачи управления «ведущий – ведомый» в документе «Требования к системе»

А.1 Схема задачи



А.2 Граничные состояния

Возможные состояния входов:

- измеренное значение 1: > высокое, нормальное < низкое
- измеренное значение 1: > высокое, нормальное < низкое
- уставка > высокое, нормальное < низкое

Возможные состояния выхода(ов):

- выход: полностью открытый, замороженный, плавающий, полностью закрытый

Таблица А.1 — Надежность

Задача		Режим	Отказ		
			Ожидаемая интенсивность	Действие, которое будет принято	Время восстановления, ч
Ведущий – ведомый	ВХОД	Измерение 1			
		> высокий,	1 в год	сообщите/остановите выход	*
		нормальный	NA	_____	-
		< низкий	1 в год		*
				сообщите/остановите выход	
		Измерение 2			
		> высокий,	1 в год	сообщите/остановите выход	*
		нормальный	NA	_____	-
		< низкий	1 в год	сообщите/остановите выход	*
		Уставка			
		> высокий,	1 в год	сообщите/остановите последнее значение	2
		нормальный	NA	_____	-
		< низкий	1 в год	сообщите/остановите последнее значение	2
	ВЫХОД	Выход		сообщите/остановите	2
		> высокий	1 в год	последнее значение	-
		нормальный	NA	_____	2
		< низкий	1 в год	сообщите/остановите последнее значение	

Примечание 1 — В зависимости от границы системы согласно оценке, входные измерения могут быть или не быть под управлением системы. В рассматриваемом примере, измерения – вне границы и следует отметить, что термин «ожидаемая» интенсивность отказа эквивалентен «времени восстановления» – вне рассмотрения системы. Набор уставок управляется с клавиатуры, если система находится в работе.

Примечание 2 — NA – не применяется.

Примечание 3 — * – данная величина – не свойство системы.

Приложение В
(справочное)

Пример требуемой информации и формата документации для задачи управления «ведущий – ведомый» в документе «Спецификация системы»

Задача	Поддерживаемые			Свойства надежности				
	Функция	Модуль	Элемент	Безотказность	Готовность	Ремонтопригодность	Защищенность	Целостность
Ведущий–ведомый	Ввод/вывод	Ввод/вывод	I-карта Барьер	[1]	[1]	[1]	[2]	[2]
	монитор	модуль	I-карта Барьер O-карта Барьер PS-i/o					
	Управление	Процесс модуль 1	CPU-PM FBusC DIA PS-PM SysBusC					
		или						
		Процесс модуль 2	CPU-PM FbusC DIA PS-PM SysBusC					
	Интерфей человек/машина	Оператор станция 1	CPU-OPS Mem-карта GrO-карта SysBusC					
		или						
		Оператор станция 2	CPU-OPS Mem-карта Grd-карта SysBusC[3]					

[1] использовать формат, приведенный в проекте комитета МЭК 56 (Секретариат) 318: Руководство по определению надежности характеристик (на рассмотрении), (приложение D)

[2] заполняется на основания документа «Спецификация системы».

[3] показанные сокращения заимствованы из списка изготовителя и используются здесь только для целей иллюстрации

Приложение С
(справочное)

Испытания достоверности

С.1 Введение

Испытание методами внесения ошибки в систему обеспечивает полезный вклад в оценку достоверности систем (технических средств и программного обеспечения).

Эти методы требуют от персонала, проводящего испытания, глубоких знаний функционирования системы, ее физической и функциональной структуры, и часто делают необходимым получение физического доступа к системе.

Концепция этих испытаний состоит в следующем: достоверная система не должна выполнять задачи неправильно, несмотря на отказ элемента системы или попытки проникнуть в систему через ее границу.

Чтобы проверить данную концепцию, создаются ошибки (чтобы проверить целостность) и/или альтернативное несанкционированное или неправильное действие (чтобы проверить защищенность) и наблюдается результирующее поведение системы (состояние выхода(ов) и/или оповещающее выходное сообщение).

Ниже приводятся примеры вопросов, на которые должны быть получены ответы относительно поведения системы когда:

– происходит ошибка, доводится ли выход системы до предопределенного состояния или замораживания?;

– экран не работает правильно, блокируется ли клавиатура автоматически?;

– связь перегружена, как ведет себя система?;

– ошибка внесена, срабатывает ли сигнализация, например, включается «сторожевое устройство», звучит сигнал тревоги, начинают работать соответствующие средства печати?

Чтобы избежать ненужной работы следует на основе аналитического изучения принять согласованный подход к испытаниям, начиная с уровня печатной платы с постепенным переходом на уровень интегральной схемы.

В общем случае вводится единичная неизменяемая ошибка.

Тип вводимых в систему ошибок может быть, например, таким:

– удаление платы или модуля;

– разрыв связей платы (большинство отказов системы из-за плохих связей);

– нарушение контактов микросхем или принудительное воздействие на них для получения логических 0 или 1.

Для проведения испытания могут потребоваться специальные средства типа:

– расширитель платы с выключателями;

– зажимы;

– специальные программы для испытаний.

В зависимости от глубины оценки, метод может отнимать много времени, но имеет преимущество, связанное с простотой осуществления и относительно недорогими средствами проведения испытаний.

Примечание — Следует соблюдать осторожность и предусмотрительность при проведении этих испытаний, чтобы избежать повреждения каких-либо элементов системы.

С.2 Вводимые ошибки

Потенциальные виды отказа систем классифицируются в МЭК 60812 (пункт 3.6).

Далее приведены примеры ошибок, которые могут привести к отказу системы и использоваться для моделирования.

С.2.1 Отказы системы из-за дефектного модуля, элемента или компонента:

– потеря энергоснабжения от единственного источника энергоснабжения;

– потеря энергоснабжения от резервного источника энергоснабжения (как активного, так и пассивного);

– потеря энергоснабжения резервных модулей с первичной также как и с вторичной стороны модуля энергоснабжения;

– потеря энергоснабжения отдельных модулей и элементов;

– потеря модулями и элементами, отдельными и резервными, связи с коммуникационной шиной;

– потеря модуля или элемента;

– потеря энергоснабжения периферийного оборудования (экранов, клавиатур, принтеров, двигателей диска и т. д.;

– потеря связи с периферийным оборудованием;

– обрывы и короткие замыкания в контурах энергоснабжения, шинах связи, адресных линиях, линиях вход /выход.

С.2.2 Отказы системы из-за ошибок человека

Отказы системы могут происходить из-за ошибок, вызванных неправильными действиями персонала при обслуживании, реконфигурации, модернизации программного обеспечения системы, например, таких как:

– перемещение резервных кабелей шины;

– набор неправильного адреса модулей, элементов и т. д.;

– установка печатных плат в неправильном положении;

– установка печатных плат в перевернутом положении;

– установка соединителей в неправильном или обратном положении;

– установка соединителей в неправильном положении;

– непрочные контакты соединителей после ремонта;

– изменение полярности энергоснабжения;

– отказ выполнения полной или корректной инициализации или процедуры запуска;

– использование того же самого адреса дважды и т. д.

С.2.3 Отказы системы, вызванные неправильными или несанкционированными входами в систему через человеко-машинный интерфейс:

– вызов или использование несуществующих или неправильных отображений, кодов, программ или периферийных устройств;

– перегрузка клавиатуры или сенсорной панели вызовом большого числа команд в течение короткого промежутка времени (поворот n-ключей);

–

– использование неполных кодов для вызова отображения, тэгов и т. д.

С.3 Наблюдения

Когда вышеупомянутые ошибки введены, регистрируются следующие вопросы и ответы на них.

a) На какие задачи системы и как воздействуют введенные ошибки?

– Изменяются ли входные сигналы, пока детектируются все соответствующие модули?

– Соответствуют ли выходные сигналы всех модулей правильным сигналам на входе?

– Корректируется ли еще представление данных операторам?

– Правильно ли выполняются команды оператора?

– Правильно ли функционирует связь между самостоятельными узлами, с ведущим компьютером, с пунктом управления системы, печатающими устройствами и т. д.?

– Есть ли задержки (потери времени) действий в каком-либо модуле?

b) Система сообщает об ошибке?

– Автоматически или в течение некоторого промежутка времени?

– Автоматически, после периодического испытания?

– На каком уровне системы ошибка была сообщена (пункт управления системы, элемент системы)?

c) Обеспечена ли система защитными средствами, чтобы избежать возникновения отказа?

– Предотвращается ли распространение ошибки?

– Продолжается ли действие через резервную связь?

– Деградирует ли выполение задачи системы?

– Продолжается ли выполнение операций резервными средствами; ухушается ли при этом выполнение задач(и) системы?

– Достигает ли выход системы установленного уровня в случае неспособности системы продолжать правильное действие?

d) Действительно ли ремонт в оперативном режиме возможен без воздействия на задачу(и) системы?

– Имеется ли сообщение об ошибке, обеспечивается ли однозначная информация относительно отказавшей части системы?

– Может ли осуществляться ремонт в оперативном режиме без воздействия или прерывания действия других модулей или элементов системы?

– Может ли восстановленный или запасной модуль или элемент автоматически запуститься и правильно функционировать после установки в систему?

С.4 Интерпретация результатов

Для того, чтобы облегчить интерпретацию результатов, рассчитывается процент вводимых ошибок, при которых:

– продолжается правильное функционирование;

– срабатывает штатная сигнализация.

Хотя данные не могут использоваться в абсолютном виде, тем не менее, они ценны в сравнительных ситуациях.

Подобный подход применяется для оценки готовности, когда степень компенсации самоконтроля рассчитывается как процент ошибок, обнаруженных самоконтролем.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60050 (191):1990	–	*
МЭК 60068	–	*
МЭК 60300-3-2:1993	–	*
МЭК 60706-4:1992	–	*
МЭК 60801	–	*
МЭК 60812:1985	–	*
МЭК 60863:1986	–	*
МЭК 61000	–	*
МЭК 61025:1990	–	*
МЭК 61069-1:1991	IDT	ГОСТ Р МЭК 61069-1-2012 «Измерение и управление промышленным процессом. Определение свойств системы с целью ее оценки. Часть 1. Общие подходы и методология»
МЭК 61069-2:1993	IDT	ГОСТ Р МЭК 61069-2-2012 «Измерение и управление промышленным процессом. Определение свойств системы с целью ее оценки. Часть 2. Методология оценки»

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 61070: 1991	–	*
МЭК 61078: 1991	–	*
МЭК 61132	–	*
МЭК 61165	–	*

*Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

IDT – идентичные стандарты;

Библиография

МЭК 60300-3-1: 1991 (IEC 60300-3-1: 1991)	Управление общей надежностью. Часть 3. Руководство по применению. Раздел 1. Методики анализа для определения общей надежности. Руководство по методологии (Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology)
МЭК 60605-1: 1978 (IEC 60605-1: 1978)	Испытание аппаратуры на надежность. Часть 1. Общие требования (Equipment reliability testing – Part 1: General requirements)
МЭК 60605-2: 1994 (IEC60605-2: 1994)	Испытание аппаратуры на надежность. Часть 2. Разработка испытательных циклов(Equipment reliability testing – Part 2: Design of test cycles)
МЭК 60605-3 (IEC 60605-3)	Испытание аппаратуры на надежность. Часть 3. Предпочтительные условия испытаний аппаратуры на надежность. (Equipment reliability testing – Part 3: Preferred test conditions)
МЭК 60605-4: 1986 (IEC 60605-4: 1986)	Испытание аппаратуры на надежность. Часть 4: Методика определения точечных оценок и пределов достоверности по результатам испытаний аппаратуры на надежность (Equipment reliability testing – Part 4: Procedures for determining point estimates and confidence limits from equipment reliability determination tests)
МЭК 60605-6: 1986 (IEC 60605-6: 1986)	Испытание аппаратуры на надежность. Часть 6. Испытания на достоверность предложения о постоянной частоте отказов (Equipment reliability testing – Part 6: Tests for the validity of a constant failure rate assumption)
МЭК 60605-7: 1978 (IEC 60605-7: 1978)	Испытание надежности оборудования. Часть 7. Планы проведения испытаний на установление

	интенсивности отказов и среднего времени работы на отказ допускающего постоянную интенсивность отказов (Equipment reliability testing – Part 7: Compliance test plants for failure rate and mean time between failures assuming constant failure rate)
МЭК 61123 (IEC 61123)	Испытания на надежность. Планы проверки соответствия техническим требованиям для определения нормы успешного исхода (Reliability testing – Compliance test plans for success ratio)
IEC committee draft 56 (Secretariat) 307	Software test methods (under consideration)
IEC committee draft 56 (Secretariat) 318	Guide on specifying dependability characteristics
IEC committee draft 56 (Secretariat) 319	Software reliability and maintainability requirements analysis (under consideration)
IEC committee draft 56 (Secretariat) 383	Use of failure rate data intended per reliability prediction of components in electronic equipment – Reference conditions – Stress models for their conversion (under consideration)
IEC committee draft 65FA (Secretariat) 123	Functional safety of electrical/electronic/programmable electronic systems (under consideration)

USA Military Standardization Handbook MIL-HDBK-217 issues A through F: Reliability prediction of electronic equipment

УДК 658.5.012.7 ОКС 25.040.40

Ключевые слова: промышленный процесс, система измерения и управления, оценка системы, свойства системы, эксплуатабильность системы, анализ свойств системы, методология оценки, задача, функция, модуль, элемент, влияющие факторы

Подписано в печать 30.04.2014. Формат 60x84 1/8.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru