ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 27.303— 2021 (МЭК 60812:2018)

Надежность в технике

АНАЛИЗ ВИДОВ И ПОСЛЕДСТВИЙ ОТКАЗОВ

(IEC 60812:2018, Failure modes and effects analysis (FMEA and FMECA), MOD)

Издание официальное

Москва
Российский институт стандартизации
2021

Предисловие

1 ПОДГОТОВЛЕН Закрытым акционерным обществом «Научно-исследовательский центр контроля и диагностики технических систем» (ЗАО «НИЦ КД») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 119 «Надежность в технике»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 сентября 2021 г. № 987-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту МЭК 60812:2018 «Анализ видов и последствий отказов (FMEA и FMECA)» (IEC 60812:2018 «Failure modes and effects analysis (FMEA and FMECA)», MOD) путем внесения технических отклонений, которые выделены в тексте курсивом.

Международный стандарт разработан Техническим комитетом МЭК 56.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА

5 ВЗАМЕН ГОСТ Р 51901.12 —2007 (МЭК 60812:2006)

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (www.rst.gov.ru)

© IEC, 2018
© Оформление. ФГБУ «РСТ», 2021

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 применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
4 Общие положения 5
5 Методология FMEA 7
Приложение А (справочное) Общие рекомендации по адаптации FMEA 20
Приложение В (справочное) Методы анализа критичности 26
Приложение С (справочное) Пример отчета об FMEA 33
Приложение D (справочное) Связь FMEA с другими методами анализа надежности 39
Приложение Е (справочное) Прикладные аспекты применения FMEA 40
Приложение F (справочное) Примеры применения FMEA в различных отраслях промышленности . 46
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 63
Библиография 65

Введение

Анализ видов и последствий отказов (FMEA) является систематизированным методом исследования объекта или процесса, в основе которого лежит выявление возможных отказов, а также влияния этих отказов на функционирование объекта или процесса, окружающую среду и персонал. В настоящем стандарте описана методология выполнения FMEA.

Целью выполнения FMEA является поддержка принятия решений, направленных на снижение вероятности отказов и значимости их последствий. Применение FMEA помогает улучшить работу объекта либо непосредственно, либо с помощью других методов, использующих результаты FMEA. Применение FMEA способствует повышению безотказности, снижению воздействия на окружающую среду, снижению закупочных и эксплуатационных расходов, повышению деловой репутации и т. п.

Метод FMEA может быть адаптирован для применения во всех отраслях промышленности и организациях любого вида. Метод FMEA применим к оборудованию, программному обеспечению, процессам, действиям человека и их различным сочетаниям.

Метод FMEA может быть выполнен несколько раз в течение срока службы объекта или процесса. Предварительный анализ может быть проведен на ранних стадиях жизненного цикла (на ранних этапах проектирования), затем при наличии бóльшего количества информации может быть проведен более детальный анализ. Метод FMEA может быть выполнен с учетом существующих средств контроля или рекомендованных методов, направленных на снижение вероятности и/или значимости последствий отказов. В случае анализа замкнутого цикла метод FMEA позволяет оценить эффективность всех воздействий на отказы.

Метод FMEA может быть адаптирован к различным ситуациям и применен различными способами в зависимости от поставленных целей.

Виды отказов могут быть ранжированы в соответствии с их значимостью. При ранжировании могут быть учтены не только последствия или критичность отказа, но и другие важные характеристики. При использовании ранжирования отказов метод называют анализом видов, последствий и критичности отказов (FMECA). В настоящем стандарте под FMEA следует понимать также и FMECA.

Настоящий стандарт содержит общее руководство по планированию, выполнению, документированию и поддержке метода FMEA путем.

a) описания принципов анализа;

b) рассмотрения этапов анализа;

c) представления примеров документации;

d) представления примеров применения метода.

Метод FMEA может быть использован при сертификации продукции или страховании. Например, метод FMEA может быть использован при анализе безопасности для целей регулирования, но, поскольку настоящий стандарт является общетехническим, он не содержит специального руководства по применению FMEA в области анализа безопасности.

Метод FMEA должен соответствовать применимым законодательным требованиям и требованиям в области риска.

Основными пользователями настоящего стандарта являются руководители и участники анализа.

В настоящем стандарте ссылки на международные стандарты заменены ссылками на межгосударственные и национальные стандарты.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежность в технике

АНАЛИЗ ВИДОВ И ПОСЛЕДСТВИЙ ОТКАЗОВ

Dependability in technics. Failure modes and effects analysis

Дата введения — 2022—01—01

1 Область применения

В настоящем стандарте приведено описание планирования, выполнения, документирования и поддержки применения метода анализа видов и последствий отказов (FMEA), включая анализ видов, последствий и критичности отказов (FMECA).

Анализ видов и последствий отказов (FMEA) направлен на выявление способов отказа объектов или процессов и способов предотвращения таких отказов в дальнейшем. FMEA представляет собой систематизированный метод идентификации видов отказов и их последствий для объекта или процесса на локальном и глобальном уровне. Этот метод может включать в себя определение причин отказов. Виды отказов могут быть ранжированы для использования при принятии решений об их устранении. Если ранжирование отказов включает в себя определение и учет значимости и других важных показателей последствий отказов, то анализ называют анализом видов, последствий и критичности отказов (FMECA).

Настоящий стандарт применим к оборудованию, программному обеспечению, процессам, включая действия человека, и их взаимодействию в любом сочетании.

FMEA может быть использован при анализе безопасности, выполнения законодательных и других требований, однако настоящий стандарт не содержит специального руководства по применению FMEA в области анализа безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO 13849-1—2014 Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования

ГОСТ 27.002 Надежность в технике. Термины и определения

ГОСТ Р 22.0.12—2015 Безопасность в чрезвычайных ситуациях. Международные термины и определения

ГОСТ Р 27.013 Надежность в технике. Методы оценки показателей безотказности

ГОСТ Р 27.302 Надежность в технике. Анализ дерева неисправностей

ГОСТ Р 27.606 Надежность в технике. Управление надежностью. Техническое обслуживание, ориентированное на безотказность

ГОСТ Р 55.0.01 Управление активами. Национальная система стандартов. Общее представление, принципы и терминология

ГОСТ Р 51897 Менеджмент риска. Термины и определения

ГОСТ Р 51901.14 Менеджмент риска. Структурная схема надежности и булевы методы

ГОСТ Р 57273 Устойчивое развитие производственных сетей. Общие положения

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

Издание официальное

ГОСТ Р ИСО/МЭК 31010 Менеджмент риска. Методы оценки риска

ГОСТ Р МЭК 61165 Надежность в технике. Применение марковских методов

ГОСТ Р МЭК 61508-1 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

ГОСТ Р МЭК 61508-2 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам

ГОСТ Р МЭК 61508-3 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р МЭК 61508-4 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

ГОСТ Р МЭК 61508-5 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности

ГОСТ Р МЭК 61508-6 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3

ГОСТ Р МЭК 61508-7 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

ГОСТ Р МЭК 62061 Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью

ГОСТ Р МЭК 62502 Менеджмент риска. Анализ дерева событий

ГОСТ Р МЭК 62508 Менеджмент риска. Анализ влияния на надежность человеческого фактора

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по *ГОСТ Р 51897*, [*1*], а также следующие термины с соответствующими определениями:

3.1.1 **вид отказа** (failure mode): Способ и особенности возникновения отказа[1)].

Примечания

1 Вид отказа может представлять собой нарушение функции или ее утрату или другое изменение состояния.

2 Видами отказа оборудования могут быть, например: для клапана — «клапан не открывается» или для двигателя — «двигатель не запускается».

3 Вид отказа, связанного с действиями человека, представляет собой утрату функции объекта в результате действий человека (совершенных или не совершенных).

3.1.2 **последствия отказа** (failure effect): Результаты воздействия отказа на объект (явления, процессы, события и состояния) внутри или вне границ отказавшего объекта.

Примечания

1 В некоторых случаях может потребоваться рассмотрение отдельных видов отказов и их последствий.

2 Последствия отказа также охватывают последствия внутри или вне границ отказавшего процесса.

---

1) *См. также ГОСТ 27.002.*

3.1.3 **система** (system): Набор взаимодействующих элементов, сформированный для достижения одной или нескольких поставленных целей[1)].

Примечания

1 Систему иногда рассматривают как объект или как предоставляемые услуги.

2 На практике значение этого термина часто разъясняется с помощью ассоциативного существительного, например система летательного аппарата. Слово «система» часто опускают, используя синоним; например, вместо термина «система летательного аппарата» используют термин «самолет», хотя он не подчеркивает то, что объект является системой.

3.1.4 **объект** (item): Любая часть, элемент, устройство, подсистема, функциональная единица, аппаратура или система, рассматриваемые самостоятельно.

Примечания

1 Объект может быть отдельной деталью, компонентом, устройством, функциональным блоком, оборудованием, подсистемой или системой.

2 Объект может представлять собой аппаратное обеспечение, программное обеспечение, персонал или любую их комбинацию.

3 Объект часто состоит из элементов, каждый из которых может быть рассмотрен отдельно.

4 В [*1*] введен в качестве английского синонима термин «сущность», который не всегда может быть применен.

5 Определение в [*1*] больше похоже на описание. В настоящем стандарте использован термин «объект». Определение термина по [*1*] приведено в качестве примечания 1.

3.1.5 **процесс** (process): Совокупность взаимосвязанных и/или взаимодействующих действий, преобразующих входы в выходы.

3.1.6 **иерархический уровень** (hierarchy level): Уровень деления системы, объекта или процесса на составные части в соответствии с их структурой.

Примечания

1 Иерархический уровень также называют контрактным уровнем (см. *[1]*).

2 Верхний и нижний иерархические уровни соответствуют верхнему и нижнему уровням структуры системы соответственно. Средний иерархический уровень соответствует одному из уровней между высшим и низшим уровнями.

3.1.7 **элемент** (element): Неделимая (в соответствии с иерархической структурой) часть системы, объекта или процесса, для которой должны быть идентифицированы виды отказов[2)]).

3.1.8 **сценарий** (scenario): Возможная последовательность заданных ситуаций и обстоятельств, которые могут возникнуть при функционировании системы, объекта или процесса.

Примечания

1 Ситуации и обстоятельства могут включать действия или факторы вне границ исследуемого объекта или процесса, которые могут повлиять на работу объекта или процесса.

2 Физические ситуации и обстоятельства охватывают все факторы окружающей среды, такие как температура, влажность, освещенность, ударные нагрузки, наличие загрязнения, уровни излучений.

3 Организационные ситуации и обстоятельства включают такие факторы, как уровень квалификации, физические и психологические нагрузки персонала.

3.1.9 **причина отказа** (failure cause): Совокупность обстоятельств (явлений, процессов, событий и состояний), приводящая к отказу.

Примечания

1 Причина отказа может возникнуть при установлении требований, в процессе проектирования, изготовления, монтажа, эксплуатации или обслуживания объекта.

2 Примерами причины отказа могут быть загрязнение или недостаточная смазка, что приводит к такому виду отказа, как заклинивание подшипника.

3 Причины отказа процесса могут охватывать ошибки человека, такие как чрезмерная нагрузка, нарушение памяти, неверное понимание, ошибочные предположения.

3.1.10 **механизм отказа** (failure mechanism): Процесс, приводящий к отказу.

Примечание — Процесс может быть физическим, химическим, логическим, психологическим или их комбинацией.

---

1) *См. также [2].*

2) *См. также ГОСТ 27.002.*

3.1.11 **правдоподобность (появления события)** (likelihood): Характеристика возможности и частоты появления события.

Примечания

1 Термин «правдоподобность» часто используют в качестве характеристики возможности появления события, которая может быть определена или оценена объективно или субъективно, качественно или количественно и описана с использованием терминов общих или математических (вероятность или частота события за заданный период времени).

2 Английский термин «правдоподобность» не имеет прямого эквивалента в некоторых языках; вместо него часто применяют термин «вероятность».

3.1.12 **значимость (последствий)** (severity): Относительный ранг возможных или фактических последствий отказа или неисправности[1].

Примечание — Значимость может быть определена для любых последствий.

3.1.13 **метод обнаружения** (detection method): Способ, позволяющий выявить вид отказа или его зарождение.

3.1.14 **средства контроля** (control): Предусмотренные конструкцией объекта встроенные устройства или самостоятельное оборудование, которые способны предотвратить отказ, снизить вероятность его возникновения или изменить его последствия.

Примечание — Средства контроля также могут быть отнесены к компенсационному обеспечению.

3.1.15 **критичность (вида отказа)** (**criticality**): Уровень значимости, определяемый при ранжировании отказов, с использованием установленных критериев оценки.

Примечания

1 Критерии оценки критичности обычно относятся к последствиям отказа для верхнего уровня иерархии системы, объекта или процесса.

2 Мера критичности обычно сочетает значимость последствий, по крайней мере с одной другой характеристикой вида отказа.

3 Конкретное значение критичности зависит от метода оценки, определенного при анализе и подробно рассмотренного в настоящем стандарте.

4 Критичность относится к виду отказа, а не к причинам отказа (если последние определены).

3.1.16 **обработка (вида отказа)** (treatment): Действия, направленные на изменение вероятности и/или последствий вида отказа.

Примечания

1 Обработку иногда называют снижением вероятности или последствий отказа.

2 Обработка может включать действия по устранению причины отказа, изменению вероятности возникновения отказа и/или последствий отказа.

3.1.17 **ошибка человека** (human error): Несоответствие между действиями человека, предпринятыми или невыполненными, и действиями, выполнение которых предполагается или необходимо.

Пример — Выполнение неверного действия; невыполнение требуемого действия; ошибка в расчетах, неверное прочтение значения.

3.1.18 **резервирование** (redundancy): Способ обеспечения надежности системы за счет использования нескольких способов выполнения функции[2].

Примечание — Способы выполнения функции могут быть преднамеренно различными для снижения возможности возникновения отказов общего вида.

3.1.19 **отказы по общей причине** (common cause failures): Отказы нескольких объектов, возникающие вследствие одного события, которые без рассмотрения причин считались бы независимыми.

Примечания

1 Отказы по общей причине также могут быть «отказами общего вида».

2 Возможность возникновения отказов по общей причине снижает результативность резервирования системы.

---

[1] *См. также [3].*

[2] *См. также ГОСТ Р 27.002.*

3.1.20 **отказы общего вида** (common mode failures): Отказы различных объектов (внутри системы), характеризующиеся одним и тем же видом отказа.

Примечания

1 У отказов общего вида могут быть различные причины.

2 Отказы общего вида могут быть также отказами по общей причине.

3 Возможность возникновения отказов общего вида снижает результативность резервирования системы.

3.1.21 **тестируемость (объекта)** (testability): Степень, до которой объект может быть проверен в процессе и после функционирования для обнаружения и выделения отказов или неисправностей.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

APPN — значение приоритетности альтернативного риска;

CCF — отказы по общей причине;

COTS — покупная продукция;

CSU — компонент программного обеспечения;

DC — диагностический охват;

EMI — электромагнитные помехи;

EMP — электромагнитный импульс;

ESD — аварийное отключение;

ETA — анализ дерева событий;

FIT — количество отказов в единицу времени;

FTA — анализ дерева неисправностей;

FMEA — анализ видов и последствий отказов;

FMECA — анализ видов, последствий и критичности отказов;

FMEDA — анализ видов, последствий и выявления отказов;

MTBF — средняя наработка между отказами;

MTTR — среднее время восстановления;

OEM — изготовитель оригинального оборудования;

RBD — структурная схема надежности;

RCM — техническое обслуживание, ориентированное на безотказность;

RPN — ранг приоритетности риска;

SFF — доля безопасных отказов;

SIL — уровень полноты безопасности;

SOD — значимость, возникновение и обнаруживаемость.

4 Общие положения

4.1 Цель и задачи

FMEA — метод, в котором объект или процесс разбивают на элементы и для каждого элемента по очереди идентифицируют и анализируют виды отказов и их последствия. Анализ позволяет выявить все необходимые улучшения путем устранения неблагоприятных последствий или снижения их вероятности и/или значимости. Целью добавления к FMEA анализа критичности является обеспечение возможности ранжирования видов отказов для их обработки. Применение FMEA позволяет обеспечить:

- идентификацию видов отказов, оказывающих нежелательное влияние на работу системы, например прерывающих или значительно ухудшающих работу объекта или влияющих на безопасность пользователя и других лиц;

- улучшение конструкции и изготовление объекта или процесса экономически эффективным способом за счет улучшений на ранних этапах программы проектирования и разработки;
- идентификацию риска в рамках процесса менеджмента риска (*ГОСТ Р ИСО 31000*);
- выполнение установленных законодательных и обязательных требований путем демонстрации того, что выявленные виды риска идентифицированы и учтены;
- основу для применения других видов анализа надежности (в приложении D рассмотрена взаимосвязь FMEA с другими методами анализа надежности);
- разработку и поддержку программы испытаний на безотказность;
- основу планирования программ технического обслуживания и ремонта, таких как техническое обслуживание, ориентированное на безотказность (*ГОСТ Р 27.606*);
- ключевой процесс системы управления активами (*ГОСТ Р 55.0.01*).

FMEA — метод анализа последствий единичных отказов. Если FMEA используют для анализа отказов взаимозависимых объектов, то он может быть рассмотрен с ограничениями (5.3.6 и 5.3.7.2).

4.2 Функции, обязанности и компетентность персонала

Метод FMEA требует, чтобы выполняющие его лица (например, команда FMEA) приняли на себя ответственность за следующее:
- управление процессом выполнения FMEA;
- определение формы FMEA и его адаптацию с учетом особенностей применения;
- идентификацию и анализ видов отказов и их последствий для объекта или процесса;
- определение необходимой обработки видов отказов;
- составление отчета об FMEA, включая предложения и рекомендации.

В настоящем стандарте предполагается, что в выполнении FMEA участвуют аналитик, специалисты, руководитель и заинтересованные стороны, функции и обязанности которых описаны ниже.

а) Аналитик

Лицо, ответственное за анализ применимости FMEA, управление адаптацией FMEA, обеспечение правильного и последовательного выполнения FMEA и взаимодействие с руководителями и другими заинтересованными сторонами. Аналитик должен быть компетентен в области FMEA и должен иметь соответствующие технические знания для рассмотрения работы других компетентных сотрудников, участвующих в выполнении анализа.

Примечание — При выполнении FMEA в команде FMEA функции отвода члена команды может выполнять ведущий заседаний (далее — фасилитатор).

б) Специалисты

Лица, обладающие соответствующими знаниями и опытом для рассмотрения всех аспектов исследуемого объекта или процесса, включая, при необходимости, социальные, экономические и экологические аспекты.

в) Руководитель

Лицо, ответственное за определение цели FMEA, использование ресурсов, утверждение адаптации анализа, разработку предложений и рекомендаций по обработке видов отказов. Функции руководителя FMEA может выполнять руководитель, имеющий полномочия на выполнение проекта.

г) Заинтересованные стороны

Люди или организации, которые могут затронуть, быть затронутыми или чувствовать себя затронутыми решением или действием. Заинтересованными сторонами могут быть потребители (например, владельцы контрактов), органы власти (например, регулирующие органы), пользователи (например, изготовители и специалисты по техническому обслуживанию), поставщики (например, поставщики услуг, компонентов) и лица, которые могут пострадать в результате отказов.

4.3 Особенности применения использованных терминов

Для удобства в настоящем стандарте термин «анализ видов и последствий отказов», сокращенно «FMEA», использован в качестве общего термина для всех вариантов применения или степени адаптации анализа, включая FMECA.

Термины «объект» или «процесс» использованы для обозначения объекта анализа FMEA. Объект или процесс могут быть частью более крупной системы, для которой необходимо применение нескольких видов FMEA.

Примеры терминов, относящихся к верхнему, среднему и нижнему иерархическим уровням, приведены в таблице 1. Термины в таблице 1 не являются исчерпывающими. Например, программное обеспечение может быть встроено в аппаратную систему или система может содержать человеческий фактор.

Таблица 1 — Примеры терминов, относящихся к иерархическим уровням системы

Исследуемый объект	Верхний уровень	Средний уровень	Нижний уровень
Аппаратные средства	Объект в сборе	Блок, составная часть	Компонент
Программное обеспечение	Пакет программ	Программный модуль	Функция
Процесс	Процесс в целом	Задача	Этап задачи

5 Методология FMEA

5.1 Общие положения

На рисунке 1 показана блок-схема действий, выполняемых в процессе FMEA. Действия включают три этапа: планирование, выполнение и документирование. Действия обычно выполняют последовательно, но возможны итерации (повторения), например в ситуациях, когда FMEA является частью программы разработки или когда анализируемая система является объектом изменения.

FMEA должен быть выполнен в соответствии со всеми законодательными требованиями, распространяющимися на область применения FMEA, и типом соответствующих рисков.

В случае, когда в настоящем стандарте дана ссылка на запись/идентификацию/определение/описание/состояние/документ/некоторую информацию, это означает, что информация должна быть включена в соответствующую документацию FMEA, например в отчет об FMEA, в план FMEA, документацию после завершения FMEA, такую как план последующих действий.

Действия, показанные на рисунке 1, должны быть адаптированы по отношению к области применения FMEA. Это означает, что не все перечисленные действия всегда должны быть выполнены. В приложении А приведены общее руководство и примеры адаптации метода.

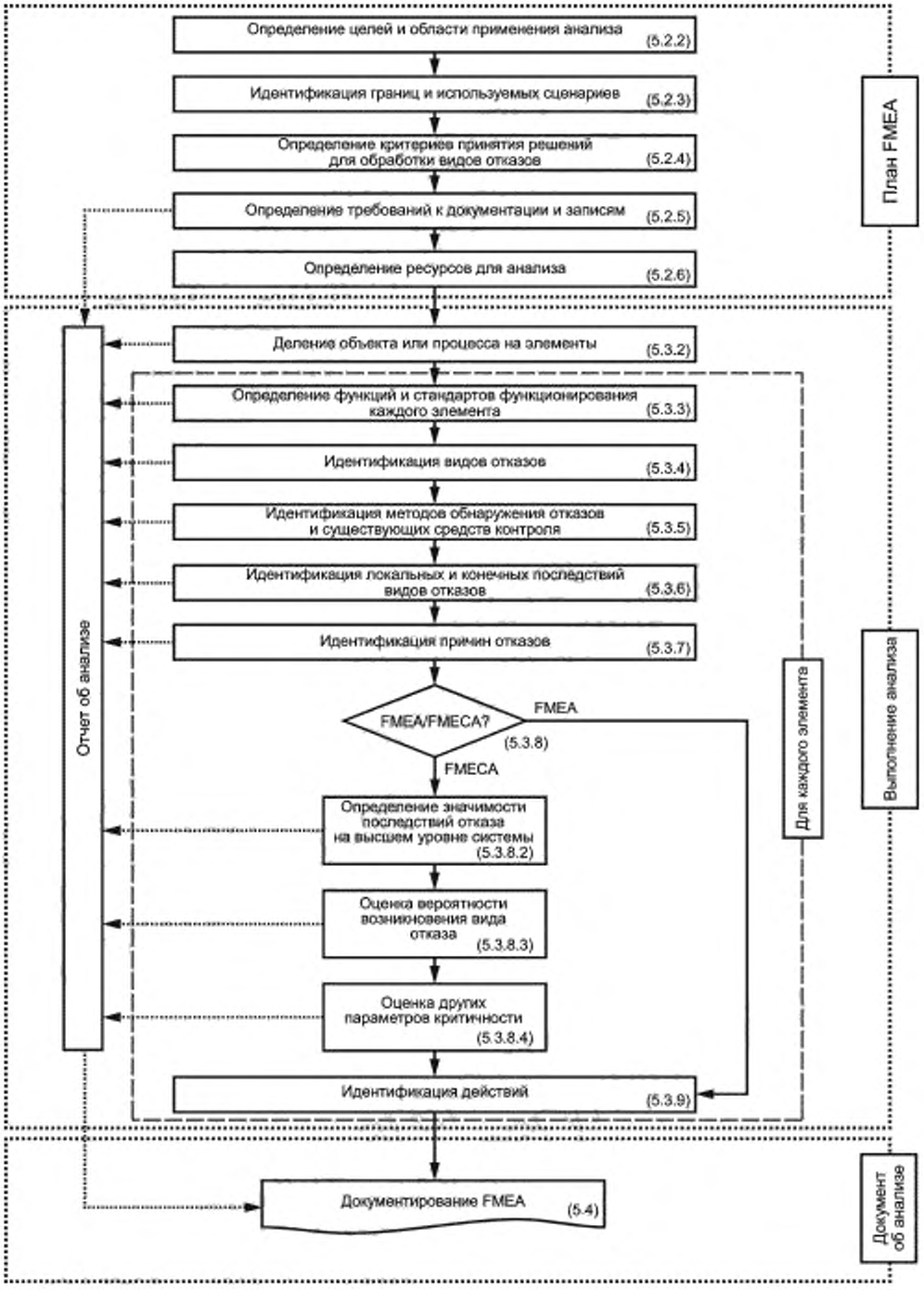

Рисунок 1 — Общая методология FMEA (до адаптации)

5.2 Планирование FMEA

5.2.1 Общие положения

Планирование FMEA включает в себя рассмотрение следующих вопросов. зачем должен быть выполнен анализ, какие объекты или элементы процесса должны быть исследованы, какие сценарии использованы и как анализ должен быть выполнен наиболее эффективно и результативно. При необходимости следует консультироваться с руководителями и заинтересованными сторонами, чтобы их цели и интересы были правильно поняты и учтены при выполнении анализа.

Результатом этапа планирования является план применения FMEA в конкретных условиях. План FMEA определяет:

- цели и область применения анализа (5.2.2);
- границы объекта анализа и используемые сценарии (5.2.3);
- критерии принятия решений для обработки видов отказов (5.2.4);
- способы документирования и записей об анализе (5.2.5);
- способ выделения ресурсов для анализа (5.2.6).

План может также включать описание факторов, влияющих на анализ, таких как:

- взаимосвязи с основными этапами проекта для определения времени, необходимого для получения результатов анализа;
- методологии или документация, необходимые для понимания функции объекта или последовательности действий процесса;
- требования контракта;
- предыдущий опыт и доступная информация.

План FMEA может быть самостоятельным документом или частью документа более высокого уровня, такого как план разработки проекта или план управления разработкой системы.

5.2.2 Определение целей и области применения анализа

При определении целей и области применения анализа устанавливают основы анализа и выбирают подход к FMEA, при котором результаты анализа соответствуют его целям.

Результатом этих действий должно быть следующее:

- установление цели, определяющей причины выполнения анализа.

Пример — Исследование робастности возможной конструкции; определение средств улучшения процесса и процедур уменьшения количества отказов; выявление возможностей повышения безотказности; идентификация рисков; выполнение договорных требований; предложение требований к программам технического обслуживания и поддержки;

- установление целей, определяющих конечную результативность FMEA способом, позволяющим оценить результаты анализа как успешные или неуспешные.

Формулировка целей должна быть включена в план FMEA.

В некоторых случаях может оказаться целесообразным проведение более официальных консультаций с заинтересованными сторонами и подробное документирование решений и результатов анализа.

5.2.3 Идентификация границ и используемых сценариев

5.2.3.1 Общие положения

Объект анализа, его границы и условия использования должны быть описаны так, чтобы гарантировать, что область применения анализа будет понятна как пользователям FMEA, так и аналитикам. Это обеспечивает то, что важные аспекты не упущены в результате неверных предположений относительно области применения анализа. Это описание должно становиться более подробным по мере выполнения планирования и может включать в себя диаграммы, такие как технологические схемы, функциональные блок-схемы, структурные схемы надежности, функционально-иерархические структурные схемы или ссылки на документы, их содержащие.

Для больших или сложных систем (например, железная дорога) может потребоваться разделить систему на подсистемы (например, подвижной состав, система сигнализации, диспетчерский пункт), для каждой из которых FMEA выполняют отдельно. Деление системы может соответствовать физическим или функциональным границам и может зависеть от договорных требований или организационных факторов. Деление системы должно быть выполнено так, чтобы объем каждого FMEA был управляемым и каждый FMEA был логически связан со всеми другими, что позволяет учесть влияние подсистем друг на друга и на систему в целом. Особое внимание следует уделять интерфейсам[1)] между подсистемами. Границы подсистем должны быть четко установлены.

[1)] *Интерфейс — совокупность средств, методов и правил, обеспечивающих взаимодействие.*

5.2.3.2 Определение уровня применения и подхода FMEA

FMEA может быть применен на всех уровнях иерархии объекта или процесса (таблица 1). Варианты выполнения FMEA могут быть различными в зависимости от цели и стадии жизненного цикла. В приложении А приведены общее руководство и примеры FMEA.

Пример — На ранних стадиях разработки объекта FMEA может быть применен к верхним или средним уровням иерархии объекта, при этом причины отказов рассматривают как отказы элементов на следующем, более низком уровне. На более поздних этапах разработки объекта рассматривают элементы самого низкого уровня иерархии, соответствующего целям анализа. Идентифицируют все виды отказов, связанные с такими элементами, и их влияние на следующий, более высокий уровень. FMEA всегда определяет влияние видов отказов на высший уровень иерархии в пределах области применения анализа.

5.2.3.3 Определение границ объекта анализа

Границы, взаимосвязи, зависимости и интерфейсы между объектом, исследуемым FMEA, и другими частями системы, включая интерфейсы с человеком, должны быть определены. Определение границ должно включать входы и выходы объекта или процесса и четко устанавливать, какие интерфейсы относятся к области определения анализа, а какие нет.

Границы объекта зависят от условий и могут зависеть от таких факторов, как конструкция или предполагаемое использование. Может возникнуть необходимость в явном размещении объектов или этапов процесса за границами исследований для сокращения объема FMEA или потому, что детальные знания о границах не могут быть получены.

По возможности следует определять границы объектов в каждом FMEA для облегчения выполнения анализа и объединения с другими соответствующими исследованиями. В некоторых случаях полезно определить границы объекта с функциональной точки зрения, чтобы ограничить количество связей с другими объектами или процессами вне анализа. Это часто имеет место, если объект или процесс является функционально сложным с множеством взаимосвязей внутри и/или вне границ.

5.2.3.4 Определение используемых сценариев

При выполнении FMEA его всегда необходимо рассматривать в условиях одного или нескольких установленных сценариев использования объекта. Используемые сценарии, к которым должен быть применен FMEA, необходимо определить в соответствии с целями анализа и достаточно подробно описать для облегчения идентификации всех соответствующих отказов. Сценарии могут включать определенные состояния вне установленных нормальных условий использования объекта.

Пример — Сценарии при анализе оборудования могут иметь вид «нормальная работа» или «хранение», при анализе процесса — «ночная смена» или «экстренное реагирование».

Описание сценария обычно включает в себя физические условия окружающей среды, такие как внешние условия в сочетании с условиями, создаваемыми другими объектами или действиями в непосредственной близости от исследуемого объекта. Другие соответствующие факторы включают в себя организационные ограничения, такие как уровни компетентности персонала, физические или психологические стрессы, которые могут влиять на поведение человека.

Все внутренние и внешние факторы, которые могут повлиять на виды и последствия отказов, должны быть установлены так, чтобы они могли быть рассмотрены при анализе.

Должен быть установлен контрольный журнал для документов, используемых при определении сценариев.

5.2.4 Определение критериев принятия решений для обработки видов отказов

Критерии для определения того, по каким видам отказов необходима обработка, и приоритеты действий должны быть определены до проведения анализа. Эти критерии должны учитывать цели анализа, все юридические или договорные требования и мнения заинтересованных сторон относительно того, что является приемлемым. Критерии должны обеспечивать последовательный и обоснованный выбор режимов отказов, по которым необходима обработка. Кроме того, критерии должны указывать, когда рекомендованная обработка является достаточной. Критерии принятия решений относительно отказов, по которым необходима обработка, должны быть утверждены и одобрены руководством проекта.

Виды последствий, относящихся к анализу, должны быть определены (например, последствия, связанные с экономическими воздействиями, физическим ущербом, психологическими травмами или нематериальными последствиями, такими как потеря репутации).

Критерии принятия решений зависят от области применения FMEA и должны регулярно пересматриваться, например, с учетом опыта эксплуатации. Обработка видов отказов может быть рекомендована как часть FMEA или как часть последующих действий.

Решение о необходимости обработки видов отказов и приоритеты обработки обычно учитывают значимость воздействия отказа на цели и функции системы в целом, а также относительные преимущества вариантов обработки и затраты на их выполнение.

В некоторых случаях может быть выполнен формальный анализ критичности, когда каждому виду отказа присваивают ранг критичности. Критерии определения критичности включают в себя:

- значимость влияния отказа на цели и функции системы или высший уровень, относящийся к предмету анализа;
- вероятность того, что отказ может возникнуть и привести к последствиям указанной значимости;
- возможность своевременного обнаружения отказа для смягчения или предотвращения его последствий.

Значимость и вероятность отказа или значимость, вероятность и обнаруживаемость отказа могут быть объединены для определения меры критичности. Это может быть сделано с использованием матрицы, графика или значений приоритетности риска (RPN). Не существует единого универсального метода анализа критичности. В приложении В приведено два наиболее распространенных метода. Они могут быть использованы без изменений или адаптированы к условиям организации.

Примечание 1 — Метод, используемый для анализа критичности, может варьироваться в зависимости от особенностей проекта, даже в пределах одной организации, хотя предпочтителен последовательный подход к анализу критичности.

Анализ критичности особенно полезен, когда существуют ограничения на варианты обработки, связанные с затратами, техническими сложностями или ограничениями по времени.

Анализ критичности может оказаться бесполезным, если необходимо выполнить обработку по всем выявленным видам отказов или если недостаточно информации для получения обоснованных оценок значений критичности. Кроме того, в некоторых случаях анализ критичности может быть неэффективным.

Примечание 2 — Критичность можно рассматривать в соответствии с риском. Руководство по анализу риска приведено в *ГОСТ Р ИСО/МЭК 31010*.

План FMEA должен включать детали критериев принятия решений и, если необходим анализ критичности, метод определения критичности. Критерии принятия решений также должны быть подробно описаны в отчетах об FMEA.

5.2.5 Определение требований к документации и записям

5.2.5.1 Общие положения

Целью является документирование в логической последовательности всей информации, использованной и разработанной в процессе FMEA. Таким образом, анализ и полученные по его результатам выводы и рекомендации должны быть понятными и однозначными. Документация FMEA должна обеспечивать возможность проверки, четкую прослеживаемость и включать:

- описание способов использования результатов;
- обоснование решений, принятых на основе анализа;
- обоснование адаптации анализа, включая метод, используемый для оценки и ранжирования критичности;
- перечень источников информации, используемых при выполнении FMEA, с проверяемыми ссылками на источники;
- свидетельства соответствия нормативным и договорным обязательствам.

Результаты FMEA могут быть входными данными для других видов анализа или представлять собой отдельный отчет FMEA.

Форма документации FMEA должна быть установлена при планировании FMEA. Форма отчета о результатах FMEA должна соответствовать стандартам и процедурам организации с учетом целей, сложности и объема FMEA. Документация, разрабатываемая при выполнении FMEA, может представлять собой комбинацию баз данных, электронных документов и отчетов на бумаге. Средства обеспечения прослеживаемости в таких разнородных средах должны быть определены.

Поскольку FMEA является итеративным методом, документацию разрабатывают постепенно в течение срока службы исследуемого объекта или процесса. Документацию FMEA необходимо обновлять

в установленные сроки. Например, на ключевых этапах проекта, при появлении новой информации, по мере продвижения работ по проектированию, при определении и выполнении действий по улучшению, при получении данных обратной связи и опыта использования объекта. Пересмотр документации FMEA необходимо контролировать в соответствии с процессом управления документацией в организации. Опыт и результаты, полученные при выполнении FMEA, должны быть использованы в будущем при разработке новых проектов.

5.2.5.2 Содержание отчета об FMEA

Отчет об FMEA, как минимум, должен включать:

- описание анализируемой системы, объекта или процесса вместе с соответствующими ограничениями, функциональной схемой и чертежами, которые определяют структуру объекта (процесса);
- четкое описание области применения и границ с указанием конкретных исключений;
- критерии, используемые для определения необходимости обработки;
- предположения, сделанные в отношении анализируемых объекта или процесса и соответствующих используемых сценариев;
- детальное описание методологии, лежащей в основе анализа;
- идентификацию заинтересованных сторон и вовлеченного персонала;
- описание метода проведения анализа критичности, которое должно быть достаточно подробным и обеспечивать независимую проверку;
- источники данных и других применимых материалов (с указанием их статуса, даты выпуска/пересмотра), на которых должен быть основан FMEA;
- определение видов отказов, их последствий и, при необходимости, их критичности и причин. Описание видов и последствий отказов не должно содержать ссылки на документы, не указанные в отчете,
- краткое изложение результатов и рекомендуемой обработки видов отказов, если такие рекомендации получены, включая рекомендации относительно будущего анализа, если это необходимо. Документация FMEA может включать только краткое изложение рекомендуемой обработки. Такая обработка затем должна быть выполнена в соответствии с планом действий, не относящимся к документации FMEA;
- ограничения и недостатки FMEA, которые должны быть устранены при выполнении FMEA в будущем;
- изменения проекта, которые уже были включены в объект в результате FMEA, и все нерешенные проблемы. В некоторых случаях никакие действия не могут быть предприняты, даже если в результате FMEA рекомендована обработка видов отказов. В таких случаях обоснование невозможности выполнения действий должно быть зафиксировано в документации по управлению действиями, а документация FMEA должна быть обновлена после принятия окончательного решения. Необходимы мониторинг и анализ возможного воздействия невыполнения рекомендованной обработки;
- записи об анализе, которые могут быть включены в качестве приложения к отчету в виде рабочих листов. Если эти записи обширны или используют базы данных, должны быть даны ссылки, указывающие, где можно найти соответствующую информацию.

Сбор и хранение информации, ее поддержка и обеспечение доступа к ней могут потребовать значительных затрат для организации, следует заботиться о том, чтобы все разработанные документы повышали ценность FMEA. Возможны любые форматы отчетов FMEA, выбранный формат часто определяет полученную информацию, сделанные оценки и процесс, используемый для получения результатов. В приложении С приведены примеры рабочих листов FMEA.

5.2.6 Определение ресурсов для анализа

5.2.6.1 Информационные ресурсы

Для выполнения FMEA обычно требуется следующая информация:

- исследуемый объект или процесс, его цели и функции в системе в целом;
- элементы объекта или процесса и их характеристики, изготовление и функции;
- логические, физические и функциональные связи между элементами, например структурные схемы надежности, функциональные блок-схемы, технологические карты, чертежи системы, версии программного обеспечения, структура и процессы управления. Эта информация, возможно, уже была собрана при проведении соответствующего анализа надежности (приложение D);
- уровень резервирования и особенности запасного оборудования, резервированные оборудование или процессы, или параллельно работающие составные части;
- положение и значимость объекта или процесса для организации (если это возможно);

- входы и выходы объекта или процесса и их элементов;
- взаимодействия с другими связанными объектами или процессами и с окружающей средой, в которой работает объект;
- все изменения структуры объекта для различных режимов работы;
- общие базы данных, содержащие виды отказов, событий, относящихся к их возникновению, и интенсивности отказов;
- данные эксплуатации;
- данные предыдущего анализа FMEA по тем же или аналогичным объектам или процессам, если это необходимо.

Информация, относящаяся к функциям, характеристикам и работе, необходима для всех уровней рассматриваемых объектов или процессов, вплоть до самого высокого уровня в пределах области применения FMEA, что позволяет при выполнении анализа должным образом учитывать виды отказов, влияющие на все функции.

Сбор информации продолжают в процессе FMEA, так как анализ часто показывает, где необходима дополнительная информация. Информация должна быть достоверной и понятной всем участникам.

Основная информация об исследуемом объекте или процессе может быть представлена в виде информационного пакета до начала анализа, аналитик, выполняющий FMEA, должен иметь доступ ко всей соответствующей информации.

5.2.6.2 Персонал

Для выполнения FMEA необходимы специалисты, компетентные в области технических аспектов исследуемого объекта или процесса, а также видов и последствий его отказов, имеющие соответствующие полномочия.

Необходимые навыки и компетенции включают в себя:

- умение применять метод FMEA;
- понимание технических аспектов исследуемого объекта или процесса, а также видов и последствий его отказов;
- навыки фасилитатора (при выполнении анализа командой).

Для работы может потребоваться междисциплинарная группа, подход и состав которой зависят от целей анализа.

Пример — В случае информационной системы в команде могут участвовать системный инженер и эксперт по программному обеспечению.

При проведении анализа также могут быть необходимы дополнительные знания о конкретной продукции или услуге. В этом случае в анализе также должны участвовать другие лица с соответствующими компетенциями.

5.2.6.3 Физические ресурсы

Физические ресурсы обычно необходимы для распределения информации и работ в процессе анализа среди реальных или виртуальных членов команды или заинтересованных сторон. К физическим ресурсам относятся выделенные конференц-залы, аудиовизуальная поддержка для виртуальных обсуждений и общие информационные системы, включая существующие базы данных FMEA и т. д. Такие ресурсы следует выбирать на основе экономической целесообразности и ценности с точки зрения качества, полезности (при начальном и повторном использовании) и своевременности результатов анализа.

5.3 Выполнение FMEA

5.3.1 Общие положения

Этапы выполнения анализа установлены в 5.3.2—5.3.9.

5.3.2 Деление объекта или процесса на элементы

Для выполнения FMEA объект анализа подразделяют на элементы в соответствии со следующими правилами:

- систему можно разделить на функциональные блоки;
- объекты аппаратного обеспечения могут быть разделены на более мелкие и менее сложные составные части или компоненты;
- процессы могут быть представлены в виде последовательности действий, или этапов;
- программное обеспечение может быть разделено на программные модули или функции;

- отдельные интерфейсы могут быть идентифицированы в виде связей между элементами, между элементом и пользователем или элементом и средой.

Примечание 1 — Объект анализа может представлять собой комбинацию аппаратных средств, программного обеспечения и/или процессов.

Примечание 2 — Люди могут являться элементом системы, механизмы возникновения ошибок человека при работе могут быть учтены в анализе причин аппаратного и/или программного отказа.

Соответствующий уровень детализации анализа зависит от особенностей и желаемых результатов анализа. В целом большое количество уровней деления объекта FMEA обеспечивает эквивалентный уровень детализации возможных видов и последствий отказов, а также более подробные стратегии обработки, но в этом случае анализ потребует больше времени.

5.3.3 Определение функций и стандартов функционирования каждого элемента

Для формирования основы FMEA необходимо четкое установление всех функций каждого элемента. При анализе каждую функцию элемента следует рассматривать отдельно.

Для каждой идентифицированной функции должен быть определен стандарт функционирования, что позволяет определить, что является отказом, и, следовательно, определить виды отказов. Функцию каждого элемента можно вывести на основе функциональных требований или других доступных источников.

Выбранный стандарт функционирования должен отражать уровень работы, необходимый для выполнения элементом его функций в условиях использования объекта или процесса, а не его возможности. Стандарт функционирования должен быть однозначным и, по возможности, использовать количественные величины.

5.3.4 Идентификация видов отказов

Для каждого элемента объекта или процесса должны быть установлены ситуации, в которых элемент или процесс может перестать соответствовать критериям своего работоспособного состояния. Элемент может иметь несколько видов отказа. Каждый вид отказа должен быть описан отдельно. Анализ должен быть направлен на выявление всех возможных видов отказа, относящихся к целям анализа.

В зависимости от цели и области применения анализа для определения видов отказов каждого элемента в процессе жизненного цикла объекта рассматривают следующее:

- применение;
- режим работы;
- соответствующие функциональные требования;
- нагрузки, возникающие под воздействием экологических факторов, и тенденции их изменения;
- психологические стрессы и социальные изменения;
- рабочие нагрузки при хранении, транспортировке и техническом обслуживании;
- нагрузки в процессе утилизации и ликвидации.

Как правило, информация о виде отказа может быть получена из следующих источников:

- для новых объектов и процессов могут быть использованы данные о других объектах и процессах с аналогичной функцией и структурой, работающих в близких условиях;
- для существующих элементов и процессов виды отказов могут быть известны из предыдущего FMEA. Однако следует провести проверку для выявления различий в использовании элементов, которые могут привести к различным видам отказов (А.2.1);
- опыта эксплуатации;
- эксплуатационных и экологических испытаний внутри установленных границ или за их пределами;
- контрольных перечней общих видов отказов для установленных типов элементов;
- баз данных о техническом обслуживании и ремонте;
- базы данных об инцидентах и авариях;
- знаний, относящихся к области исследований.

5.3.5 Идентификация методов обнаружения отказов и существующих средств контроля

5.3.5.1 Общие положения

Для каждого вида отказов должны быть идентифицированы существующие методы обнаружения отказов и средства контроля.

Средства контроля представляют собой устройства, используемые для предотвращения или уменьшения вероятности возникновения вида отказа или смягчения его последствий, в то время как

методы обнаружения отказа представляют собой способы идентификации вида отказа, неисправности или инцидента[1)].

Раннее обнаружение отказа или признаков его приближения может позволить операторам, специалистам по техническому обслуживанию, пользователям и другим лицам вмешаться и уменьшить вероятность неблагоприятных воздействий или их последствия. В конкретных приложениях контроль и обнаружение могут иметь различные значения, хотя обычно эти понятия близки. В приложениях E и F приведены соответствующие рекомендации и примеры.

Если рассмотренные средства контроля или методы обнаружения являются неподходящими, следует определить новые или улучшенные средства контроля и методы обнаружения отказов и сформировать рекомендации по их обработке (5.3.9).

5.3.5.2 Методы обнаружения

Обнаружение отказа может принимать различные формы в зависимости от типа выполняемого FMEA.

Пример — Методы обнаружения могут включать в себя следующее: предупреждающие световые или звуковые сигналы; индикаторы, калибры, мониторинг; испытания на безотказность в процессе разработки; статистическое управление процессами; скрининг нагрузок и напряжений для обеспечения безотказности; эксплуатационные испытания на работоспособность; аудит; контроль; диагностику.

Если более одного вида отказов может быть обнаружено с помощью одних и тех же средств, следует описать способы устранения неоднозначности, чтобы ни один из видов отказа не остался невыявленным и, при необходимости, можно было предпринять правильные действия.

5.3.5.3 Средства контроля

Должны быть перечислены особенности конструкции и существующие средства, способные предотвратить или уменьшить вероятность возникновения вида отказа или изменить его влияние, и описаны способы их функционирования.

Пример — Средства контроля могут включать следующее: резервирование элементов или системы, позволяющее продолжать работу в случае отказа одного или нескольких элементов; соблюдение технических или других стандартов: наличие альтернативных средств работы при обнаружении проблемы; требования к материалам; регулировка машины; техническое обслуживание; конструкция объекта или процесса, учитывающая человеческий фактор.

5.3.6 Идентификация локальных и конечных последствий видов отказов

Последствие отказа является следствием возникновения вида отказа в соответствии со сценарием, определенным для анализа. Одни и те же последствия могут быть вызваны одним или несколькими видами отказов одного или нескольких элементов объекта или процесса.

Влияние вида отказа на элемент может быть идентифицировано на локальном уровне (локальное последствие) вместе с влиянием на высшем уровне исследуемого объекта (глобальное или конечное последствие). Последствия на промежуточных уровнях также могут быть определены, если это необходимо.

Примечание 1 — Локальный уровень может означать анализируемый объект или его физическое местоположение.

При рассмотрении относительной значимости отказов важна идентификация конечных последствий. Идентификация локальных последствий дает информацию, которая может помочь при разработке альтернативных методов обработки отказов. В некоторых случаях не может быть локальных последствий, кроме вида отказа как такового.

В дополнение к последствиям, влияющим на функцию объекта, процесса или системы в целом, могут быть и другие последствия, например связанные с безопасностью, окружающей средой или соответствием требованиям. Их обоснованность должна быть установлена в плане FMEA.

Примечание 2 — Для идентификации конечных последствий вида отказа может потребоваться использование других видов анализа, например анализа дерева событий (ГОСТ Р МЭК 62502).

Последствия отказов должны быть описаны достаточно подробно, чтобы пользователь FMEA мог делать выводы об их значимости. Последствия отказов могут быть выведены на основе знаний об объекте или процессе, их функций, взаимодействий и месте в анализируемой иерархии. Часто для

[1)] *См. ГОСТ Р 22.0.12—2015 (пункт 2.1.15).*

упрощения анализа последствия отказа подразделяют на группы в зависимости от значимости или особенностей.

Зафиксированное описание последствий отказа должно включать информацию, позволяющую точно оценить тяжесть и значимость возможных последствий. Способы регистрации последствий и типы последствий, которые следует учитывать, должны соответствовать описанным в плане FMEA.

Поскольку FMEA исследует конечные последствия, рассматривая элемент за элементом или функцию за функцией, то последствия, возникающие в результате множественных отказов, обычно не идентифицируют. Однако в некоторых ситуациях, таких как анализ дополнительных или защитных свойств, отказ, не имеющий немедленно обнаруживаемых последствий (т.е. не выявленный), может привести к последствиям высшего уровня после второго отказа, который в противном случае не был бы важен. Эти события должны быть записаны для дальнейшего исследования или анализа.

Пример — Отказ защитного устройства приводит к неблагоприятным последствиям только в случае отказа защитного устройства и отказа объекта, для защиты которого оно предназначено. Последствия таких множественных отказов указывают в отчете об анализе.

Примечание 3 — Анализ дерева неисправностей (*ГОСТ Р 27.302*) можно использовать для исследования влияния сочетаний отказов или для понимания дополнительных функций и взаимосвязей между защищенными и защитными объектами.

5.3.7 Идентификация причин отказов

5.3.7.1 Общие положения

Понимание того, как возникает отказ, полезно для определения наилучшего способа снижения вероятности отказа или его последствий. Этапы FMEA не включают метод полного анализа причин отказов. В некоторых случаях полезно определить физический, логический или психологический механизм отказа, однако это не всегда необходимо для достижения целей анализа.

Пример — Идентификация того, что протечка (вид отказа) связана с процессом коррозии, может привести к рекомендации по замене материала.

Примечание — Методы более детального анализа причин отказов приведены в анализе корневой причины (см. *[4]*).

Степень, до которой необходимо исследовать причины отказов, зависит от результативности затрат. Например, больше усилий можно посвятить анализу причин видов отказов, которые оказывают существенное влияние на функции и цели, чем видов отказов, оказывающих меньшее влияние.

При выявлении причин отказа следует учитывать условия использования. Следует рассмотреть причины, связанные с аппаратным и программным обеспечением, человеческим фактором и интерфейсами между ними.

5.3.7.2 Отказы по общей причине и отказы общего вида

В процессе FMEA необходимо рассмотреть возможные источники отказов по общей причине (CCF). Отказ по общей причине — это отказ, когда несколько (более одного) элементов отказывают одновременно или в течение достаточно короткого периода времени. Поэтому отказы по общей причине противоречат фундаментальному предположению о том, что рассматриваемые в FMEA виды отказов являются независимыми. Отказ по общей причине является частным случаем, когда причина связана с самими элементами.

Пример 1 — Причиной отказа источника питания является неправильное номинальное значение для ожидаемой высокой температуры работы компонента. Таким образом, когда возникает высокая температура, более одного источника питания отказывают в течение короткого периода времени.

Примечание — Объект или процесс, в котором использованы резервирование или множественные средства контроля для поддержания функции или снижения последствий в случае отказа, подвержен отказам по общей причине.

Если средство контроля может отказать по той же причине, что и элемент, для контроля состояния которого его используют, то такой отказ по общей причине следует включить в качестве причины отказа таким же образом, как и другие причины, а обоснование его включения следует привести в документации.

Отказы общего вида возникают в нескольких элементах, отказавших одним и тем же способом (с одним и тем же видом отказа) по одной и той же либо по разным причинам. Часто возникают проблемы, когда потеря функции связана с резервированными объектами, изготовленными по одной и той же технологии и имеющими одинаковую конструкцию.

Пример 2 — Использование компонентов с недостаточной номинальной емкостью (конденсаторов) с несоответствующей интенсивностью отказов из-за повышенного напряжения может привести к короткому замыканию (отказ общего вида) в резервных элементах.

Отказ общего вида должен быть идентифицирован и обработан в процессе анализа, если соответствующий элемент относится к области применения анализа. Источники и последствия отказов общего вида могут быть лучше исследованы с помощью таких методов, как анализ дерева неисправностей (*ГОСТ Р 27.302*).

5.3.7.3 Человеческий фактор

Персонал можно рассматривать как элемент объекта или процесса, который имеет свои виды отказов, или ошибку человека можно идентифицировать как причину отказа аппаратного, программного или технологического элемента, включая их взаимодействия.

Анализ причин ошибок человека, как правило, более сложен, чем анализ причин отказа аппаратного или программного обеспечения, поскольку в этом случае существует гораздо больше механизмов отказов, каждый из которых имеет много возможных причин. Отказ от рассмотрения ряда психологических механизмов может привести к чрезмерно упрощенному и неправильному определению причины и, следовательно, к неправильной стратегии ее устранения.

Пример 1 — Вид отказа «действие не выполнено» может произойти потому, что человек отвлекся, сделал ошибочные предположения, или из-за недостатка знаний о последовательности действий. Если какое-либо действие не выполнено по невнимательности или халатности, дополнительное обучение может быть бесполезным или даже контрпродуктивным.

Примечание 1 — Причины ошибок человека и факторы, влияющие на его деятельность, приведены в *ГОСТ Р 62508*. Таксономия видов, механизмов и причин ошибок человека, а также формальные методы, которые могут быть использованы для анализа ошибок человека, приведены в [*4*].

Примечание 2 — Человек может совершить как преднамеренную, так и непреднамеренную ошибку.

Процедуры устранения ошибок человека направлены на уменьшение вероятности возникновения ошибок. Поскольку устранить ошибку может быть сложно, цель состоит в том, чтобы сделать объект или процесс более устойчивым к ошибкам человека.

Пример 2 — В процессе движения поезда, а также для хорошей видимости сигналов могут быть предусмотрены блокировки, предотвращающие подачу машинистом ошибочных сигналов об опасности, независимо от причины ошибки.

5.3.8 Оценка значимости вида отказов

5.3.8.1 Общие положения

В плане FMEA должно быть установлено, следует ли учитывать относительную значимость видов отказов и как это следует делать.

Ранжирование может быть выполнено либо в процессе анализа каждого вида отказа, так как для каждого вида отказа анализируют его последствия, либо после идентификации всех видов отказов. Результатом является перечень всех видов отказов, ранжированных в порядке актуальности их обработки. При ранжировании необходимо учитывать экономическую эффективность обработки отказов, простоту ее выполнения и влияние обработки на другие части системы.

5.3.8.2 Определение значимости последствий отказа на высшем уровне системы

Значимость последствий, определяемая для каждого вида отказа, должна отражать значимость его влияния на высший уровень системы, объекта (конечные последствия) или на цели процесса. Определение высшего уровня в условиях анализа должно быть четко установлено.

Пример 1 — Анализ объекта может быть выполнен изготовителем для анализа его конструкции; в этом случае значимость последствий может быть представлена через влияние на характеристики объекта в целом. Этот же объект может быть проанализирован в составе группы объектов; в этом случае значимость последствий связана с влиянием на характеристики группы.

Пример 2 — Анализ процесса или процедуры может быть выполнен для оценки их воздействия на небольшое подразделение или группу или как часть более крупного анализа.

Примечание — Степень влияния может оказаться более значительной на низких уровнях иерархии объекта, если резервирование и средства контроля учитывают только на более высоких уровнях иерархии системы.

Чтобы обеспечить согласованность приоритетов видов отказов в процессе FMEA, значимость последствий необходимо оценивать, используя четко установленную общую шкалу, которая охватывает

типы последствий (5.2.4), установленные в плане. В приложении В приведена более подробная информация.

5.3.8.3 Оценка вероятности возникновения вида отказа

Вероятность возникновения каждого вида отказа должна быть определена, если она необходима в качестве входных данных для анализа критичности (приложение В) или если результаты анализа используют в качестве входных данных в других методах анализа надежности (приложение D).

При оценке вероятности возникновения вида отказа следует учитывать технические, человеческие, организационные и экологические факторы, которые могут влиять на отказ и вероятность его возникновения.

При оценке вероятности возникновения вида отказа должен быть четко установлен период времени, для которого сделаны оценки. Выбранный период времени должен соответствовать целям FMEA.

Пример — Обычно используемые периоды времени включают: гарантийный период; ожидаемую продолжительность полезного использования объекта; установленный период использования объекта или процесса; продолжительность смены.

Вероятность возникновения вида отказа может быть оценена с использованием различных методов и источников данных, включая:

- данные испытаний компонентов на стойкость или лабораторно рассчитанных интенсивностей ошибок человека;
- доступные базы данных о видах отказов, интенсивностях отказов, вероятностях отказов или неготовности;
- данные об отказах в процессе эксплуатации;
- данные мониторинга работы человека;
- данные об отказах аналогичных объектов с сопоставимым использованием.

Примечание — Существуют базы данных о видах отказов обычно используемых компонентов оборудования (например, [5], *ГОСТ Р 27.013*), о видах ошибок человека (например, [6]), методах оценки надежности человеческого фактора (например, *ГОСТ Р МЭК 62508*), об оценке отказов аналогичных объектов (например, [7]).

5.3.8.4 Оценка других параметров критичности

Если необходимо провести анализ критичности, можно оценить и другие параметры, кроме вероятности и значимости последствий. Например, общим дополнительным параметром, используемым при оценке критичности, является рейтинг «обнаруживаемости». Вид отказа, в котором отказ или признаки будущего отказа могут быть легко обнаружены, обычно менее важен, чем вид отказа, который невозможно обнаружить до возникновения неблагоприятных последствий. В приложении В приведены примеры, в которых при анализе критичности использован рейтинг обнаруживаемости.

Примечание — В некоторых случаях применения FMEA, особенно в автомобильной отрасли, обнаруживаемость имеет другое значение и является частью идентификации возможного вида отказа в процессе выполнения программы разработки.

Аналогично при ранжировании критичности вида отказа может быть использован дополнительный параметр, отражающий результативность существующих средств контроля.

5.3.9 Идентификация действий

5.3.9.1 Общие положения

В зависимости от области применения FMEA, возможные действия для видов отказа, требующих обработки (5.2.4), должны быть идентифицированы, оценены и документированы. В некоторых случаях только способы обработки, которые сразу становятся очевидными, документируют как часть FMEA, а выбор окончательного решения является целью дальнейшего анализа и компромиссных решений за пределами FMEA.

Также может потребоваться детальное применение FMEA в области, вызывающей особую озабоченность, или выполнение анализа причин отказов до разработки рекомендаций.

Обоснование рекомендаций по возможной обработке должно быть основано на критериях принятия решения (5.2.4), согласованных с планом FMEA, и должно быть документировано. При определении способа обработки отказов следует проявлять осторожность при интерпретации факторов, используемых при определении критичности вида отказа.

При определении способа обработки не следует устанавливать уровень точности, не совместимый с данными и используемыми методами, даже если была проведена полная количественная оценка FMECA.

5.3.9.2 Варианты обработки

Обработка вида отказа может включать изменение конструкции объекта или процесса, действий во время эксплуатации или технического обслуживания оборудования.

Как правило, внесение изменений на этапе проектирования менее затратно, особенно в отношении изменения оборудования.

Пример 1 — Изменения в конструкции включают: замену компонентов на более безотказные; внедрение систем резервирования или резервного копирования; эргономичное проектирование оборудования или процессов для снижения вероятности ошибок; применение новых или улучшенных способов, с помощью которых объект, операторы, пользователи могут обнаружить отказ; а также применение устройств, обеспечивающих безопасность или ограничивающих последствия отказа.

В процессе работы могут быть выполнены действия по обнаружению вида отказа или признаков будущего отказа для его предотвращения или снижения его последствий.

Пример 2 — Для аппаратных средств возможные способы обработки отказа включают в себя изоляцию, снижение нагрузки, изменение маршрута и активацию функций подавления. Для процессов возможные способы обработки отказа включают проверки и регулировки в процессе работы.

Программы технического обслуживания также могут быть использованы в качестве средства контроля и должны быть разработаны структурированным образом на основе результатов FMEA.

Примечание — Процесс разработки таких программ — это техническое обслуживание, ориентированное на безотказность (см. *ГОСТ Р 27.606*).

Обработка отказа может привести к одному или нескольким из следующих действий:

- устранению вида отказа;
- снижению вероятности возникновения вида отказа;
- устранению или уменьшению последствий вида отказа.

Для определения того, какие виды отказов требуют обработки, должны быть использованы критерии принятия решения (5.2.4).

В некоторых случаях никакие действия не могут быть предприняты, даже если обработка была идентифицирована в процессе FMEA.

Следует также рассмотреть возможность удаления средств контроля, которые неэффективны или излишни.

Документация должна включать, как минимум, краткое изложение всех сделанных рекомендаций.

Если рекомендации приняты и введены новые средства контроля или методы обнаружения отказов, может возникнуть необходимость пересмотра анализа для проверки:

- возникновения новых видов или последствий отказов;
- приемлемости критичности конкретных видов отказов.

Изменения в документации на объект или процесс, которые должны быть учтены при следующем пересмотре FMEA, должны быть идентифицированы.

5.4 Документирование FMEA

Анализ должен быть документирован и представлен в соответствии с планом FMEA (5.2.5)[1].

---

[1] *Существуют коммерческие пакеты программ для разработки отчета о результатах FMEA. Для отчета о простом анализе с небольшим количеством участников может быть полезно использование электронных таблиц. Для составления отчета о более сложном анализе с несколькими источниками информации и сложными требованиями к отчету может быть полезна реляционная база данных.*

Приложение А
(справочное)

Общие рекомендации по адаптации FMEA

А.1 Общие положения

А.1.1 Обзор

Адаптация позволяет сформировать экономически эффективный способ достижения целей FMEA и включает в себя принятие решений:

- о границах анализируемых системы, объекта или процесса;
- о начальной точке анализа в иерархии объекта;
- об уровне детализации при делении объекта анализа на элементы;
- о рассматриваемых этапах анализа;
- об уровне детализации на каждом этапе анализа;
- о применимости ранжирования видов отказов на основе их критичности и используемом методе оценки.

В целом выбор зависит от таких факторов, как:

- цель анализа (например, улучшение или модификация объекта или процесса, создание свидетельств о надежности ([*8*]) для демонстрации соответствия установленным требованиям, планирование технического обслуживания или материально-технического обеспечения, обеспечение безопасности);
- степень, в которой процесс или объект являются новыми или инновационными;
- наличие соответствующих данных (например, об эксплуатации аналогичных объектов, данных испытаний);
- необходимость выполнения обработки отказа или передачи выполнения этих действий другой стороне, не участвующей в FMEA;
- юридические или договорные требования;
- зрелость конструкции объекта или проекта;
- стадия жизненного цикла, на которой выполняют FMEA.

В общем случае должен быть выполнен анализ того, что для некоторых объектов, процессов или их элементов не требуется применение FMEA в любой форме, это особенно важно, если нет четкой идентификации преимуществ выполнения анализа или если более полезно применение других видов анализа надежности. FMEA приобретает экономическое значение, например, в результате влияния на конструкцию, эксплуатацию и представление информации для разработки экономически эффективных предупреждающих и корректирующих программ технического обслуживания. Если результаты анализа не могут повлиять на эти факторы, тогда применение FMEA может быть неоправданным.

Примечание — Во многих случаях готовые объекты или элементы, приобретаемые у конкретных поставщиков, могут быть рассмотрены в виде «черного ящика» и могут быть удовлетворительно проанализированы лишь в отношении интерфейсов, входов и выходов.

Примеры вариантов адаптации в конкретных отраслях промышленности приведены в А.3. Общие положения по применению FMEA приведены в приложении Е.

А.1.2 Начальная точка FMEA в структуре объекта

Выбор начальной точки для адаптации FMEA зависит от цели, стадии анализа и способа достижения наилучших результатов (5.2.3.2).

Подход, когда начальная точка анализа находится на верхнем или среднем уровне структуры объекта, а в качестве причин видов отказов рассматривают лишь отказы элементов на следующем, более низком уровне, в настоящем стандарте назван подходом «сверху вниз» или нисходящим подходом.

Подход, когда начальной точкой анализа являются элементы самого низкого уровня структуры объекта, связанные с достижением целей, в настоящем стандарте назван подходом «снизу вверх» или восходящим подходом.

Нисходящий подход обычно используют на ранних этапах проектирования, и, следовательно, он может давать неполные по глубине и охвату результаты из-за преднамеренного ограничения области применения или отсутствия необходимой информации. Тем не менее раннее применение анализа (с использованием оценок там, где это необходимо) может оказать положительное влияние на надежность и стоимость объекта. Если FMEA продолжается до завершения разработки, FMEA должен быть завершен с использованием детализованного подхода «снизу вверх» и должен соответствовать целям FMEA.

Примечание 1 — В настоящем стандарте термин «нисходящий» использован для описания подхода выполнения FMEA и соответствует применению анализа дерева неисправностей.

Примечание 2 — Если область применения анализа является более обширной, чем внутренняя работа объекта (например, включает внешние события, такие как пожар, наводнение или влияние оператора), или продолжение разработки маловероятно (например, возможности выполнения анализа ограниченны), то более полезным, чем FMEA, может быть анализ дерева неисправностей.

Обзор особенностей нисходящего и восходящего подходов приведен в таблице А.1. Приведенные в таблице особенности позволяют понять особенности данных подходов.

Таблица А.1 — Особенности нисходящего и восходящего подходов FMEA

Подход FMEA	Особенности
Нисходящий	Чаще всего подход понимают как функциональный анализ, фокусирующий усилия на наиболее важных требованиях или функциях объекта или процесса. Применим на ранних стадиях разработки, когда известны только функциональные требования на верхнем уровне объекта. Помогает более детально определить структуру объекта, полезен для более поздних FMEA (которые затем могут стать восходящими), особенно для сложных систем. Может быть применен в случаях, когда исследуют конкретные последствия и нужны только конкретные виды отказов. Может быть экономически эффективен, если анализ сконцентрирован на конкретных элементах или функциях. Позволяет оценить потерю объектом функции, но ограничивается оценкой того, как могут происходить заранее определенные события отказа, без идентификации всех отказов, которые могут произойти. Требуется обоснование оценки точки, в которой продолжение анализа на более низких уровнях структуры объекта не даст или почти не даст полезной информации для достижения цели анализа. Может обеспечивать определение требований на более низких уровнях структуры объекта.
Восходящий	Подход чаще всего применяют в тех случаях, когда отдельные элементы объекта или процесса рассматривают на самом детальном уровне, а последствия их отказа анализируют на заданных более высоких уровнях структуры. Обеспечивает большую уверенность в том, что все возможные виды отказов рассмотрены, так как делается мало предположений относительно покупных составных частей или составных частей в сложных одноразовых модулях (их рассматривают как черный ящик). Хорошо подходит для определения всех возможных последствий при разработке совершенно нового расположения компонентов, использования существующих элементов в новой среде или в новой области применения. Часто используют для новых конструкций, когда влияние на верхний или более высокий уровень неизвестно. Не требует знания функциональных требований верхнего уровня объекта, поскольку потерю функции на верхнем уровне объекта выводят путем распространения последствий отказа компонента вверх по иерархической структуре объекта. Может значительно увеличить объем FMEA и, следовательно, усилия, необходимые для выполнения анализа.

А.1.3 Степень детализации при выполнении анализа

FMEA может быть выполнен с разной степенью детализации для получения дополнительной информации, например для анализа возможных вариантов восстановления или для оказания помощи в выполнении соответствующих видов анализа при эксплуатации, техническом обслуживании или поддержке логистической программы. Глубина и объем FMEA зависят от сложности исследуемых системы, объекта или процесса.

А.1.4 Ранжирование видов отказа

Расширение FMEA для включения анализа критичности может быть полезно, если требуется мера значимости конкретного вида отказа. Такая информация об относительной значимости может быть использована при планировании очередности действий по оценке и обработке отказов. Если все виды отказов должны быть обработаны определенным образом (например, если это необходимо в соответствии с обязательными требованиями), то проведение анализа критичности может быть бесполезным.

При определении очередности обработки отказов не следует рассматривать только значимость или критичность отказа. Также следует рассмотреть, например, экономическую эффективность доступных методов обработки, простоту их выполнения и их влияние на другие части системы.

При оценке параметров, таких как значимость и вероятность, могут быть использованы количественные или качественные шкалы.

- Количественные шкалы могут быть полезны при наличии соответствующих данных эксплуатации, испытаний или прогноза, позволяющих для конкретных видов отказов назначить интенсивность или вероятность отказов.

- Качественные шкалы могут быть полезны в ситуации, когда отказы должны быть ранжированы по значимости, но подробная информация недоступна или объект недостаточно определен для применения соответствующих количественных данных.

Обзор общих характеристик качественных и количественных оценок критичности для подходов FMEA сверху вниз и снизу вверх приведен в таблице А.2.

В приложении В приведено подробное руководство по методам анализа критичности.

Содержание таблицы А.1 является общим. В некоторых случаях может потребоваться более детальное рассмотрение. Например, системы, критически важные для безопасности, могут требовать наличия доказательств того, что они были разработаны или выбраны способом, обеспечивающим прозрачность идентификации, анализа, оценки и обработки вероятности и значимости отказа. FMEA может быть настроен для отображения, например, прослеживаемости смягчения или обработки последствий отказов вместе с доказательством того, что используемый метод соответствует условиям применения. Дальнейшее рассмотрение вопросов, связанных с общими типами применения FMEA, приведено в приложении Е.

Таблица А.2 — Применение общих подходов FMEA

Подход FMEA	Качественный анализ	Количественный анализ
Нисходящий	Обычно анализ проводят на ранней стадии разработки объекта, когда такой подход может быть экономически эффективным, поскольку он позволяет останавливать анализ при достижении уровня, на котором дальнейшее деление конструкции объекта невозможно или знание вида отказа недоступно по какой-либо другой причине. Примером является проверка достоверности низкой стоимости, которая определена режимом поддержки изготовителя оригинального оборудования для зрелого объекта, который имеет некоторое соответствие с ожидаемыми видами отказов в исследуемой конструкции. Это может быть сделано с помощью нисходящего анализа, показывающего прослеживаемость определенных задач технического обслуживания и видов отказов, количество которых сокращено или является контролируемым. Нисходящий подход на ранних этапах проектирования может не включать даже качественную оценку, если цель состоит в изучении и понимании только видов отказов и их последствий.	В целом совместим с проектированием новых объектов, у которых структура известна, а обработка направлена на выявление возможностей улучшения конструкции путем ранжирования видов отказов и их последствий. Такая форма анализа обеспечивает прослеживаемость видов отказов, их последствий и возможного значения смягчающих действий, но может быть более трудной для выполнения. В целом применение оправдано, когда необходимы поддающиеся проверке выходы, такие как возможность регулировки, представление или демонстрация положительных результатов приложенных усилий.
Восходящий	Обычно применяют к существующим сложным и часто устаревшим объектам, когда фактические количественные данные о работе объекта могут быть не доступны. Может быть использован в тех случаях, когда значительная модификация объекта требует интеграции нового оборудования в процессе проектирования, а для количественного анализа данные не доступны. Поощряет начинать анализ с уровня детализации, который удовлетворяет цели анализа (например, предотвращать применение FMEA к покупным элементам, когда усилия не способствуют пониманию и существует мало вариантов конструкции).	Как правило, полезен при завершении проектирования объекта для демонстрации соответствия требованиям к конструкции и как подробный материал для использования в других видах анализа, таких как анализ безопасности или материально-технического обеспечения. Такая форма анализа может быть продолжительной, дорогостоящей и, как правило, оправдана только в случае большого объема производства или существенного влияния отказа конкретного объекта, когда применение процесса FMEA скорее всего приведет к возврату вложенных усилий.

А.2 Факторы, влияющие на адаптацию FMEA

А.2.1 Повторное использование данных (информации) анализа аналогичного объекта.

Повторное использование данных предыдущего анализа позволяет сократить усилия и время FMEA. Тем не менее данные должны быть пригодны для нового анализа. Пригодность данных предыдущего анализа для проводимого FMEA может быть оценена путем рассмотрения следующих вопросов:

- Конструкции ранее и вновь исследуемого объекта (процесса) аналогичны или совпадают?
- Данные об аналогичных объектах или процессах соответствуют целям анализа?
- Условия использования и эксплуатации исследуемого объекта и объекта-аналога совпадают?

Примечание — Объекты серийного производства, которые могут быть приобретены для использования несколькими потребителями и, возможно, в различных отраслях, могут не иметь данных FMEA, имеющихся у изготовителя. В этих случаях FMEA может принести небольшую пользу, за исключением случаев, когда есть уверенность в предлагаемой изготовителем программе технического обслуживания. Кроме того, приобретенный объект можно рассматривать в виде «черного ящика» и исследовать на самом низком уровне иерархии объекта.

FMEA может быть одним из методов, применяемых как часть программы обеспечения надежности; в этом случае могут быть использованы данные применения других методов анализа (см. приложение D).

А.2.2 Зрелость[1] конструкции объекта и разработки проекта

Зрелость относится как к разработке проекта (то есть к развитию проекта в процессе жизненного цикла объекта), так и к конструкции объекта. Зрелость конструкции объекта и проекта рассматривают вместе, поскольку они связаны.

На этапе разработки концепции, когда формируется структура объекта, нисходящий функциональный FMEA обеспечивает возможность идентификации видов отказов высокого уровня, что помогает при выборе структуры объекта. По мере перехода от стадии концепции к детальному проектированию при выборе существующих конструкций элементов объекта может быть применен восходящий подход. Начальная точка восходящего подхода обычно зависит от выбора начальной точки в иерархии объекта, выбранной посредством нисходящего функционального анализа или декомпозиции структуры объекта.

Конструкции приобретаемых объектов часто создаются в течение длительного периода времени в результате этапов модификации и улучшения надежности. Зрелые конструкции могут не иметь доступной документации об FMEA, например потому, что конструкция объекта разработана до общего осознания значения FMEA или без использования процессов улучшения, основанных на FMEA. Тем не менее зрелые конструкции могут иметь известные показатели безотказности и соответствующие программы технического обслуживания, которые обеспечивают непрерывное функционирование объекта. Выполнение подробного FMEA для таких объектов может оказывать лишь незначительное влияние на конструкцию или программу технического обслуживания.

Для незрелых конструкций часто характерно применение недавних инноваций в структуре объекта, применение новых материалов и деталей для достижения улучшенных характеристик и/или экономической эффективности. Изготовители оборудования могут иметь доступный официальный FMEA для включения в общий анализ объекта. Отсутствие FMEA для таких конструкций может быть причиной выполнения дополнительных действий, таких как экологические испытания для обеспечения требуемых значений параметров. Незрелая конструкция может возникнуть в результате использования как зрелых, так и незрелых компонентов, это может влиять на трудоемкость выполнения анализа.

А.2.3 Степень инноваций

Анализ и обработка видов отказов, связанных с технологическими инновациями, могут поддерживаться всеми четырьмя комбинациями форм FMEA и различных форм, используемых при переходе проекта со стадии концепции и определения конструкции на стадию полномасштабной разработки объекта.

Пример — Технологическая инновация может быть новой технологией процесса, новым применением существующей технологии или новым процессом.

Зрелые технологии похожи по своей природе на зрелые конструкции. Длительная эволюция зрелых технологий может мешать разработке, включающей функциональные описания объекта и его элементов. Таким образом, полезным способом установления преимуществ FMEA является оценка возможного влияния на конструкцию, изменение или определение возможных значений показателей безотказности и ремонтопригодности, а также верификация технического обслуживания и связанных с ним потребностей в поддержке.

А.3 Примеры адаптации FMEA для объектов и процессов

А.3.1 Общие положения

Чтобы показать адаптацию FMEA на практике, ниже приведено несколько примеров. Для каждого примера описаны предмет анализа и условия применения, объяснены причины адаптации FMEA. Для примеров, содержащих анализ критичности, рассмотрены только причины выбора метода. В приложении В приведена подробная информация о методах анализа критичности.

А.3.2 Пример адаптации FMEA для анализа офисного оборудования

Предметом исследования является новая конструкция офисного оборудования, включающая интегрированное аппаратное и программное обеспечение, которую необходимо оценить на этапах предварительного и детального проектирования. Конструкция объекта была основным вариантом установленного семейства продукции. Использованы элементы нового дизайна и новые технологии. Компания поддерживает базу данных о безотказности, которая включает данные, например, о нагрузке, виде и механизме отказа, структуре объекта и другую соответствующую информацию для всех существующих деталей. Все элементы объекта соединены последовательно для выполнения требуемой функции верхнего уровня.

---

[1] *Определение термина «зрелость» см. в ГОСТ Р 57273.*

FMEA был проведен в рамках программы безотказности для анализа конструкции объекта и процесса его производства. Прогнозирование и сокращение количества появлений вида отказа на стадии проектирования очень важно для разработки конкурентоспособной продукции. Организация имеет значительный опыт эксплуатации продукции данного семейства. Поэтому при выполнении FMEA могут быть использованы такие данные для устранения технических недостатков продукции и процесса на стадии проектирования.

Восходящий FMEA выбран из-за простоты и в соответствии с целью программы по обеспечению функциональности и безотказности системы, основанной на полном понимании работы элементов низкого уровня в условиях использования, установленных заказчиком. Кроме того, конструкция объекта представляет собой смесь существующих и новых технологий. Даже при использовании существующей технологии изменение условий эксплуатации может привести к различным видам отказов, поэтому был применен восходящий FMEA.

В FMEA включен анализ критичности, поскольку он позволяет ранжировать отказы по значимости последствий и вероятности их возникновения. Поскольку цикл проектирования был коротким, FMEA использован для разработки рекомендаций по распределению ресурсов для проверки согласованности параметров элементов в конструкции, так как не было возможности для проверки и анализа всех комбинаций. Существует значительный опыт эксплуатации аналогичной продукции для поддержки данного типа FMEA и обеспечения его достоверности.

Критичность была определена с использованием качественного метода RPN (см. приложение В), поскольку метод прост в применении и является достаточно всесторонним. Стандартные таблицы, определяющие шкалы измерений категорий значимости и вероятности отказов, разработаны для обеспечения согласованности в применении и оценке. Использование стандартных таблиц для оценки параметров критичности позволило легко сопоставить FMEA для различных типов продукции.

А.3.3 Пример адаптации FMEA для распределенной энергосистемы

С помощью FMEA необходимо выявить недостатки конструкции для обеспечения работоспособности и отказоустойчивости системы распределенного энергоснабжения. Анализ был также первым шагом к полному анализу готовности системы. Система распределенного энергоснабжения — новый проект в данном семействе продукции. В новом проекте использован основной вариант более ранних проектов с известной и понятной технологией. Структура системы неоднородна, но с одинаковыми функциями. FMEA должен быть выполнен на стадии детального проектирования, во время которого новые данные о конструкции и аспектах работы системы доступны из других видов анализа надежности и инженерных исследований.

Выбран нисходящий подход FMEA. Сначала было выполнено детальное определение функций системы. Это позволило определить отклонения от этих функций для поддержки анализа причин отказов на более низком уровне. Функциональные возможности системы охарактеризованы посредством разработки нисходящего FMEA, в котором проведена декомпозиция функции системы для идентификации видов отказов, их причин и последствий.

FMEA также включал анализ критичности, поскольку поддающаяся количественному определению информация о возникновении вида отказа и его последствиях необходима для последующего использования метода анализа готовности. В первом цикле FMEA использован качественный метод RPN, а когда стало доступно больше деталей проекта для количественной оценки вероятности возникновения отказов, были использованы фактические оценки интенсивности отказов.

А.3.4 Пример адаптации FMEA для медицинских процессов

Многие организации здравоохранения в нескольких странах в рамках своей аккредитации обязаны регулярно оценивать свои процедуры для определения недостатков системы. Цель состоит в идентификации частей процесса и сокращении неблагоприятных событий в области здравоохранения. FMEA — признанный способ выполнения этих требований. FMEA может быть применен к любой медицинской процедуре (например, составление необходимой дозы, введение лекарственного препарата, выполнение операции и анестезии).

В данном примере рассмотрен FMEA медицинской процедуры, в которой процедура может быть простой, но люди могут совершать ошибки и могут быть неспособны выполнить действия в соответствии с назначением из-за причин, связанных с оборудованием или окружающей средой.

Начало и конец исследуемой процедуры должны быть четко определены, а выполняемые задачи разделены на этапы, для которых определяют каждый вид отказов.

При применении FMEA в медицине рекомендуемые адаптации чаще всего включают добавление проверок и сопоставлений, а не изменение проекта процедуры в целом.

Может потребоваться выполнение вспомогательного FMEA для таких ситуаций, когда, например, отказ оборудования может привести к невозможности правильного выполнения этапа процесса или когда один этап описанной процедуры фактически выполняют в несколько этапов.

Обычно при применении FMEA к медицинской процедуре рассматривают все виды отказов с серьезными последствиями для пациентов. При проведении анализа критичности обычно используют метод RPN. Причина этого состоит в том, что возможные отказы, которые легко обнаруживают до возникновения неблагоприятных последствий, менее важны, чем виды отказов, которые остаются скрытыми до тех пор, пока не возникнут неблагоприятные последствия.

Количественный анализ интенсивности ошибок человека обычно сложен и может быть ненадежным. Простой метод, такой как RPN, или матрица критичности — это часто все, что необходимо для обеспечения полезных оценок критичности и определения приоритетов улучшения процесса.

А.3.5 Пример адаптации FMEA для электронных систем управления

FMEA применяют на стадии концепции и детального проектирования электронных систем управления для обеспечения безопасности, таких как система торможения поездов и предотвращения столкновений. Обычно такие системы являются вариантами ранее разработанных систем. Отличие новых систем от существующих, как правило, связано со структурой системы и используемой технологией.

Целью FMEA является демонстрация характеристик безопасности системы. По этой причине выбран подход FMEA «снизу вверх», этот подход позволяет аналитику систематически доказывать, что определенные меры способны надлежащим образом смягчить все идентифицированные сценарии ошибочных действий системы независимо от того, какой элемент нижнего уровня отказал.

FMEA ориентирован на анализ возможностей снижения риска отказов системы. Это обязательная часть анализа, выполняемого для систем, связанных с безопасностью. Последствия отказов обычно классифицируют независимо от того, считают их безопасными или нет. Для выбора обоснованного решения область применения описания последствий должна быть понятной. Например: если уровень слишком сосредоточен на локальных последствиях, то аналитик может не вывести критичность последствий для системы в целом; если уровень системы слишком обширен, анализ может быть не способен проследить отказ до конечных последствий.

Такой подход к FMEA вызывает дискуссию по ряду вопросов. Например, обычно дискуссии возникают о видах отказов, влияющих на возможности системы диагностики без нарушения ее основных функций. Другой аспект — это реакция на действия, направленные на смягчение последствий отказа (то есть в какой степени действия по смягчению последствий отказа могут быть учтены, если они происходят слишком редко для обнаружения зарождающегося отказа).

Методы, используемые в FMEA, варьируются от специальных электронных таблиц до специализированных баз данных, которые применяют RBD для встраивания видов отказов в модели функционирования объекта. Например, подсистемы могут ссылаться на экземпляры компонентов с определением присущих видов отказов, когда различные виды отказов могут привести к одним и тем же последствиям, которые тесно связаны с некоторым способом классификации.

А.3.6 Пример адаптации FMEA для гидроблока насоса

Основной FMEA должен быть выполнен для получения информации о предварительной конструкции гидроблока насоса для газового котла. Функции гидроблока включают функцию насоса (расход, давление), функцию отводного клапана (переключение работы котла с режима центрального отопления на режим независимого горячего водоснабжения), сброс воздуха из контура центрального отопления (отдельно сброс воздуха из жидкости), герметичность в условиях давления в системе, возможность подключения к внешним гидравлическим разъемам и т. д. Организация имеет значительный опыт работы с аналогичными объектами, исследуемый насос представляет собой существующий объект с небольшими изменениями в конструкции.

FMEA необходимо выполнить так, чтобы наилучшим образом использовать команду разработчиков. С учетом разработки предварительной конструкции и опыта работы проектировщиков логической отправной точкой для FMEA выбрана идентификация функций верхнего уровня объекта. Для идентификации видов отказов (функция за функцией) был использован семинар. Принятие процесса FMEA состоялось при участии в семинаре соответствующих специалистов, где они высказали свои опасения. Цель — исследование и фокусировка на технических компромиссах для известных видов отказов и их причин, а не проведение исчерпывающего FMEA.

Данные, собранные в ходе семинара, представлены в виде последовательности видов отказов составных частей и их причин. Например, в случае проблемы, связанной с утечками, последствия могут варьироваться от неудовлетворенности потребителя до появления воды на полу, внешних утечек, невыполнения обязательств и т. д. В этом случае вид отказа может быть утечкой, составная часть — компонентом *X*, а причиной — усталостная трещина под воздействием высокого давления.

А.3.7 Пример адаптации FMEA для ветряной турбины ветроэлектрической установки

FMEA выполнен для поддержки детального проектирования ветряной турбины ветроэлектрической установки (далее — турбина).

Область применения FMEA охватывает турбину в целом, включая такие подсистемы, как структура, ступица, силовая передача, система управления и т. п. Цель, основанная на опыте предыдущих разработок, — поддержка разработки турбины нового поколения. В данном проекте необходимо оценить весь спектр последствий на каждом уровне системы путем ранжирования видов отказов на основе риска.

Принят подход снизу вверх для каждой из отдельных взаимозависимых подсистем, при котором учитывались последствия взаимодействия подсистем, что в конечном итоге привело к последствиям на уровне системы в целом. Начальной точкой выбрана структура системы/подсистемы, например, с элементами ввода-вывода, элементами управления, коробкой передач, двигателями, координирующими устройствами, электродвигателями, датчиками, блоками питания, преобразователями сигналов, подшипниками.

Использован подход снизу вверх, поскольку необходимо тщательное изучение всех возможных воздействий на уровне подсистем и систем, как с точки зрения безотказности и готовности, так и с точки зрения безопасности. Анализ критичности использован для определения отказов, требующих большего внимания. Метод анализа критичности RPN выбран из-за его простоты.

Приложение В
(справочное)

Методы анализа критичности

В.1 Общие положения

Методы анализа критичности обеспечивают способ ранжирования видов отказов. В данном приложении приведены только те методы, которые объединяют параметры: вероятность отказа, последствия отказа и (в случае ранга приоритетности риска) обнаруживаемость отказа.

Примечание — Использование единственного параметра для ранжирования значимости не классифицируют как анализ критичности.

Существует много способов объединения названных параметров для определения характеристики критичности.

В данном приложении приведено четыре метода: матрица критичности, график критичности, ранг приоритетности риска и альтернативный ранг приоритетности риска.

Рассматриваемые виды последствий, шкалы, используемые для каждого параметра, и метод их объединения для определения критичности необходимо установить на этапе планирования. Описанные методы носят общий характер и должны быть адаптированы для применения в отношении условий и целей анализа.

В.2 Шкалы определения параметров критичности

В.2.1 Общие положения

Параметры критичности могут быть выражены качественно, количественно или полуколичественно.

- Параметры критичности могут быть выражены качественно с использованием упорядоченных описательных категорий. Например, «незначительный», «крупный» или «катастрофический» (для значимости последствий); или «частый», «редкий» или «маловероятный» (для вероятности возникновения отказа).

- Параметры критичности могут быть выражены количественно с использованием эмпирических или других данных в форме интенсивности отказов или вероятности отказов, а также количественных оценок, таких как экономические или финансовые издержки в результате отказа. Шкалы отношений устанавливают в соответствии с диапазоном данных в установленных единицах.

- Если данные позволяют давать только описательные или порядковые оценки, параметры критичности могут быть выражены с использованием порядковых шкал, иногда называемых шкалами ранжирования. Если числовые значения делений шкалы связаны с рангами вероятности и значимости последствий или диапазоном интенсивности отказов и диапазонами финансовых затрат, такой подход иногда называют полуколичественным.

Точки на шкале соответствуют области применения. Для качественного, количественного и полуколичественного подходов точки соответствуют описательным категориям, числовым оценкам и рангам/диапазонам соответственно.

При разработке шкал для измерения параметров критичности следует использовать наилучшую имеющуюся информацию, чтобы избежать предвзятых результатов. Полезная система классификации может уже существовать в организации и должна быть рассмотрена для применения.

В.2.2 Определение шкалы

Диапазон шкалы должен простираться от самых тяжелых до самых благоприятных последствий из области исследований, от самой высокой до самой низкой вероятности и от самой высокой до самой низкой степени обнаруживаемости, присущей рассматриваемым видам отказов.

Точки делений на принятой шкале должны иметь четкое и точное определение, имеющее смысл для анализа и способствующее последовательной и точной оценке. Определения должны соответствовать имеющимся данным и быть выражены в терминах, понятных тем, кто проводит анализ.

Для количественных данных могут быть более подходящими логарифмические, а не линейные шкалы, как для последствий, так и для вероятности. Точки на шкалах при использовании для качественных и полуколичественных подходов должны быть определены соответствующим образом.

Пример — Предполагается, что затраты, связанные с катастрофическими отказами, на несколько порядков, а не в несколько раз выше, чем затраты, связанные с обычным отказом.

Выбор категорий (или диапазонов) с помощью качественных и полуколичественных шкал должен быть основан на рассмотрении смысла выбранных параметров. Должно быть выбрано достаточное количество категорий, допускающее классификацию и адекватное деление всей совокупности последствий. Как правило, требуется не менее трех категорий для обеспечения достаточной дифференциации всей рассматриваемой совокупности последствий. Большое количество категорий может быть неудобно, поскольку это может потребовать чрезмерных усилий для правильной категоризации, хотя последующая обработка может не существенно отличаться между категориями.

Примечание — Рекомендуется использовать от трех до десяти категорий.

Выбор описаний категорий и значений каждой из них должен быть тщательно рассмотрен с учетом способа их использования. Следует проявлять осторожность при составлении словесных описаний и числовых или буквенных обозначений при использовании качественного подхода, поскольку они сами по себе могут влиять на выбор, сделанный в процессе анализа. Для каждой из шкал должна быть разработана таблица, определяющая значение используемых слов и обозначений.

В.2.3 Оценка вероятности

Вероятность отказа может быть выражена количественно, полуколичественно или качественно.

При количественном подходе значения вероятности могут быть получены для конкретных видов отказов, они могут быть выведены на основе общих источников данных или оценены с использованием данных эксплуатации аналогичных объектов в сопоставимых условиях и областях применения.

Обычно при наличии количественных данных они, как правило, связаны с отказами объекта или процесса в целом, а не с конкретными видами отказов элементов. Оценка вероятности вида отказа может быть получена путем декомпозиции вероятности отказа объекта в целом на вероятности возможных видов отказов. Кроме того, может быть сделана корректировка для представления вероятности того, что вид отказа приведет к конкретным последствиям (обычно определенной значимости).

Примечание — Если в качестве показателя используют интенсивность отказов, то, если не указано иное, этот подход предполагает, что интенсивность отказов постоянна и, следовательно, это может быть неприемлемым в некоторых ситуациях. Кроме того, хотя интенсивность отказов объекта может быть получена из конкретных данных, условная вероятность видов отказов и вероятность того, что конкретный уровень последствий соответствует данному виду отказа, также часто получают из другого набора источников данных или на основе выводов и заключений.

Если используют диапазоны/категории вероятности, описания могут быть сделаны с использованием эмпирических данных, экспертных заключений команды разработчиков или на основе других источников данных. Важно, чтобы была использована соответствующая шкала, позволяющая применять точную оценку относительной частоты видов отказов и ее соответствие имеющимся данным.

Чтобы облегчить точное и согласованное применение, следует учитывать следующее.

a) При использовании количественных показателей, таких как вероятность или частота, единицы измерений должны быть четко указаны.

Пример 1 — Если используют значение в процентах, то указывают величину, относительно которой определяют процент, например процент объектов, отказавших в течение года.

b) Количественные пояснения описания категории, соответствующей диапазону вероятностей, ожидаемых для данного применения, должно быть приведено (по возможности) для общего понимания.

Пример 2 — Для технических систем с высокой безотказностью частота вида отказа элемента может составлять один отказ за несколько лет, а для менее надежных систем частота вида отказа объекта может составлять несколько отказов за год.

Описание вероятности для редких отказов должно быть реалистичным и применимо к наихудшему случаю.

В.3 Назначение критичности с использованием матрицы или графика

В.3.1 Общие положения

Для обеспечения возможности определения ранга критичности взаимосвязь параметров критичности может быть представлена несколькими способами. Вероятность и последствия отказа могут быть представлены с помощью непрерывных шкал или категорий, а затем объединены для визуального представления в форме графика или матрицы. График или матрицу критичности затем используют для определения приоритетности обработки.

Значение каждого ранга критичности и его связь с соответствующей обработкой необходимо обсудить и согласовать с заинтересованными сторонами до проведения анализа при планировании FMEA. Это дает четкое и однозначное понимание способа обработки вида отказа и возможного влияния такого решения на бизнес. Невозможность выполнения этого сводит на нет значение анализа критичности и может привести к существенным затратам времени и средств из-за излишних действий или неадекватной обработки отказов. Количество необходимых рангов критичности определяют требования организации и область применения анализа.

В.3.2 Матрица критичности

Анализ матрицы критичности формирует меру значимости путем объединения значений вероятности и последствий. Матрицу критичности также называют матрицей риска. Значения по каждому параметру формируют в виде матрицы, а ранг критичности присваивают каждой ячейке матрицы. Ранг критичности может быть связан с уровнем обработки, которую применяют к соответствующему виду отказа. Для видов отказов с низким рангом обработка может включать «бездействие». На рисунке В.1 показан пример качественной матрицы критичности

Вероятность \ Значимость последствий	Катастрофические	Крупные	Средние	Незначительные
Высокая	X	X	1	2
Средняя	X	X	1	2
Низкая	X	X	1	2
Очень низкая	X	1	1	2
Крайне низкая	1	2	2	3

Рисунок В.1 — Пример качественной матрицы критичности

Примечание 1 — Примером четырех уровней категорий критичности (как на рисунке В.1) являются:
Категория X: «Недопустимый риск»;
Категория 1: «Нежелательный риск»;
Категория 2: «Приемлемый риск»;
Категория 3: «Несущественный риск».

В некоторых случаях вид отказа может привести к ряду различных последствий в зависимости от обстоятельств. В этом случае должны быть указаны последствия, которым соответствует вероятность. В такой ситуации полезно рассмотреть критичность нескольких возможных последствий.

В матрице на рисунке В.1 риск, соответствующий каждой категории критичности, возрастает от нижнего правого угла матрицы до верхнего левого. Однако обработка каждого вида отказа зависит только от классификации критичности (то есть цвета или кода критичности), а не от положения ячейки матрицы.

Примечание 2 — Использование термина «приемлемый риск» не означает, что дальнейшая обработка является нежелательной.

Матрица, представленная на рисунке В.1, является только примером, ее не следует рассматривать как обязательную форму матрицы критичности. Фактическая форма матрицы зависит от конкретной ситуации. Если количество диапазонов вероятности, категорий значимости и последствий различно, то форма матрицы будет отличаться от представленной на рисунке В.1. Если критичность, соответствующая комбинациям вероятности и значимости последствий, отличается от приведенной на рисунке В.1, кодирование также будет иным.

Матрица не обязательно ограничена двумя измерениями, ее можно расширить, добавив третий параметр или, теоретически, столько других параметров, сколько требуется. Однако сложность и усилия, необходимые для описания правильной и управляемой многомерной матрицы, могут быть значительными и неэффективными, поскольку каждая комбинация параметров требует оценки.

Матрица критичности должна быть выверена так, чтобы видам отказов с одинаковой значимостью соответствовали одинаковое значение критичности и одинаковая обработка. Кроме того, если категории значимости последствий или вероятности основаны на количественных или полуколичественных оценках, следует рассмотреть вопрос о приемлемости различных вариантов обработки, применяемых к видам отказов по обе стороны от границы критичности.

В.3.3 График критичности

На рисунке В.2 показаны примеры простых графиков вероятности и последствий с назначенными рангами критичности. В этом случае как вероятность, так и значимость последствий представляют собой непрерывные количественные шкалы.

Границы между диапазонами не обязательно должны быть прямыми (пример В) или кривыми (пример А). В соответствии с требованиями обработки выявленных видов отказов граница может быть ступенчатой (пример С) или комбинацией прямых и кривых линий.

Примечание 1 — В примере В границы диапазонов представляют собой линии одинакового уровня риска. Если для вероятности и последствий использована линейная шкала, границы будут кривыми. Если использованы логарифмические шкалы, границы будут прямыми.

Рисунок B.2 — Примеры графиков критичности

Примечание 2 — Если для вероятности использована линейная шкала, вероятность может принимать значение, равное нулю. Это может привести к ошибочным рангам критичности для высоких последствий и низкой вероятности отказов.

На практике гладкие границы диапазонов имеют смысл только в том случае, если вероятность может быть выражена количественно, а последствия отказов изменяются непрерывно (например, финансовые последствия) и могут быть полностью определены.

График критичности не обязательно должен быть ограничен двумя параметрами, при необходимости он может быть расширен до трех параметров. Однако сложность и усилия, необходимые для формирования правильных границ, могут быть значительными и неэффективными с точки зрения затрат.

В случаях, когда для значимости последствий может быть использована количественная шкала, имеющая различные значения или диапазоны значений, график критичности все еще применим, но границы значений критичности почти наверняка будут ступенчатыми. Это приводит к аналогичному представлению в матрице критичности.

B.4 Назначение критичности с использованием ранга приоритетности риска

B.4.1 Общие положения

Ранг приоритетности риска (RPN) выводят путем объединения полуколичественных оценок, выполненных по порядковым шкалам, со значениями для последствий, вероятности и обнаруживаемости. В данном методе эти параметры соответственно обозначают значимость последствий (S), вероятность возникновения отказа (O) и обнаруживаемость отказа (D), что в некоторых приложениях приводит к тому, что этот метод также называют методом «SOD». Приведено два метода оценки RPN.

B.4.2 Ранг приоритетности риска

Общая формула ранга приоритетности риска (RPN) — это произведение рангов значимости последствий, вероятности возникновения отказа и обнаруживаемости отказа RPN = S × O × D.

Диапазон значений RPN зависит от диапазона шкал этих трех параметров, обычно используют порядковые шкалы от 1 до 10, при этом значения RPN изменяются в диапазоне от 1 до 1 000.

Примечание 1 — В некоторых приложениях FMEA параметр обнаружения не используют, тогда RPN изменяется от 1 до 100.

Примечание 2 — Особенности применения определяют количеством точек на шкале, так чтобы можно было использовать менее 10 точек.

Значения S, O и D определяют с помощью таблиц рангов, в которых для каждого уровня параметра дано описательное предложение, которое помогает аналитику точно и последовательно выбирать ранг.

Обнаруживаемость D может представлять собой среднюю вероятность, с которой вид отказа будет обнаружен во время работы до того, как возникнут существенные последствия отказа. Это число обычно ранжируют в обратном порядке по отношению к значимости последствий и вероятности возникновения отказа: чем выше значение обнаружения, тем меньше вероятность обнаружения. Следовательно, более низкая вероятность обнаружения приводит к более высокому RPN и более высокому рангу вероятности возникновения вида отказа.

Пример 1 — В данном примере рассмотрена ветряная турбина. Типичная шкала ранга значимости последствий может иметь следующий вид.

Таблица В.1 — Описание рангов значимости

Ранг значимости последствий (S)	Описание
1	Отсутствие влияния на генерацию электроэнергии; посещение необходимо в течение следующих 14 дней; предупреждающий сигнал тревоги не вызывает остановку турбины; возможно, отказ вызван отказом компонент
2	Кратковременная потеря генерации электроэнергии; посещение, необходимо в ближайшие 14 дней; остановка турбины, но удаленно перенастраиваемая; возможно, отказ вызван отказом компонент
.....	
8	Потеря генерации электроэнергии в течение более длительного периода (от 2 до 4 недель); замена значительного количества компонент, требующих обслуживания
9	Потеря генерации электроэнергии в течение более продолжительного периода времени (более четырех недель); замена значимых компонент, требующих существенного обслуживания
10	Инцидент с обеспечением безопасности; потеря всей структуры; общая потеря производительности на несколько месяцев

Пример 2 — В данном примере рассмотрена ветряная турбина. Типичная шкала ранга вероятности возникновения отказа может иметь следующий вид.

Таблица В.2 — Описание рангов вероятности

Ранг вероятности возникновения отказа (O)	Описание
1	Возникновение вида отказа в течение года у одной машины из 10 000
2	Возникновение вида отказа в течение года у одной машины из 2000
.....	
8	Возникновение вида отказа один раз в год на каждой машине
9	Возникновение вида отказа на каждой машине один раз в течение четырех месяцев
10	Возникновение вида отказа на каждой машине один раз в месяц

Пример 3 — В данном примере рассмотрена ветряная турбина. Типичная шкала ранга обнаруживаемости отказов может иметь следующий вид.

Таблица В.3 — Описание рангов обнаруживаемости отказов

Ранг обнаруживаемости отказа (D)	Описание
1	Вид отказа всегда обнаруживают до появления последствий
2	Вид отказа очевиден, и обычно его обнаруживают до появления последствий
.....	
8	Вид отказа может быть обнаружен только при проверке, например при выборочном контроле
9	Вид отказа трудно обнаружить, и поэтому он почти неизбежно приводит к появлению последствий
10	Объекты не могут быть проверены, вид отказа не может быть обнаружен, например из-за недоступности

Затем виды отказа упорядочивают в соответствии с их RPN, более высокий приоритет обычно присваивают более высоким значениям RPN. В дополнение к значению RPN на решение об обработке может повлиять значимость последствий вида отказа, а это означает, что если существуют виды отказов с аналогичными или идентичными RPN, то в первую очередь необходимо рассматривать виды отказов с высокой значимостью последствий.

Примечание 3 — В некоторых ситуациях последствия с RPN, значение которого превышает определенный порог, неприемлемы, в других ситуациях большое значение придают высокой значимости последствий независимо от значения RPN.

Ранговый порядок RPN зависит от способа определения шкалы. При формировании заключений на основе значений RPN или сравнения его значений следует учитывать следующие характеристики данного метода, в противном случае могут быть получены неверные решения:

a) шкала RPN не является непрерывной.

Пример 4 — При работе с тремя шкалами с делениями от 1 до 10 разработано только 120 из 1 000 доступных значений.

b) количественные соотношения между значениями не имеют смысла.

Примечание 4 — В результате того, что шкалы являются порядковыми, а значения на шкалах значимости последствий, вероятности возникновения и обнаруживаемости отказов одинаковы, значения RPN могут мало отличаться, но соответствовать различным ситуациям. Например, значения: S = 6, O = 4 и D = 2 приводят к RPN, равному 48, а S = 6, O = 5 и D = 2 дают RPN, равный 60. Последний RPN стоит лишь немного выше, в то время как O = 5 может, например, соответствовать во много раз большей вероятности возникновения отказа, чем O = 4.

c) RPN может быть чувствительным к небольшим изменениям в значении одного из параметров.

Примечание 5 — Небольшое изменение одного из параметров оказывает явно гораздо большее влияние на значение RPN, когда другие параметры велики, чем в случае, когда они малы (пример: 9 × 9 × 3 = 243 и 9 × × 9 × 4 = 324 против 3 × 4 × 3 = 36 и 3 × 4 × 4 = 48).

Хорошей практикой использования RPN является проведение тщательного анализа значений исходных параметров до формирования заключения об оценке критичности и определения действий по обработке.

В.4.3 Альтернативный метод ранга приоритетности риска

Так называемый альтернативный метод RPN (ARPN) является модифицированной версией обычно используемого метода RPN, описанного в В.4.2, который был разработан с целью обеспечения более последовательной оценки критичности, когда параметры могут быть определены количественно в логарифмическом масштабе [9].

Для ARPN точки на шкалах параметров определяют так, чтобы значения количественных шкал измерений сохранялись. Затем используют логарифмическую шкалу, где каждое значение, соответствующее точке на шкале, умножают на постоянный коэффициент (например, 10 или квадратный корень из 10). Один и тот же коэффициент должен быть использован для каждой из шкал значимости последствий, вероятности возникновения и обнаружения отказов. В результате количество делений на шкалах параметров определяется исследуемым диапазоном и может быть больше или меньше используемых обычно десяти делений для RPN (см. В.4.2).

Таблицы, определяющие ранг значимости последствий, вероятности возникновения и обнаружения отказов, должны устанавливать значение, соответствующее рангу, в дополнение к описательному предложению.

Пример 1 — Пример относится к железнодорожной отрасли. Шкала вероятности возникновения отказов может быть тарирована на основе умножения на 10 или на квадратный корень из 10, который равен приблизительно 3. В последнем случае значения двух соседних делений шкалы представляют собой величины одного порядка. Соответствующие деления шкалы вероятности возникновения данного вида отказа объекта могут иметь вид, приведенный в таблице В.4.

Таблица В.4 — Описание рангов вероятности возникновения отказа

Ранг вероятности возникновения отказа (O)	*Описание*
1	*Интенсивность отказов составляет не более одного отказа за 100000 лет*
2	*Интенсивность отказов составляет более одного отказа за 100000 лет, но не более одного отказа за 30000 лет*
3	*Интенсивность отказов составляет более одного отказа за 30000 лет, но не более одного отказа за 10000 лет*
4	*Интенсивность отказов составляет более одного отказа за 10000 лет, но не более одного отказа за 3000 лет*

Пример 2 — Пример относится к железнодорожной отрасли. Шкала для показателя потенциальной опасности (например, значимости последствий), связанной с железнодорожной промышленностью, основана на использовании квадратного корня из 10, с округлением (приближенно 3).

Таблица В.5 — Описание ранга значимости последствий

Ранг значимости последствий (S)	Описание
1	Несущественная возможность опасности, травмы не ожидают
2	Легкие травмы у одного человека
.....	
6	Критический, один смертельный исход или много людей с тяжелыми травмами
7	Катастрофический с несколькими смертельными случаями
8	Катастрофический с большим количеством смертельных случаев

Пример 3 — Пример относится к железнодорожной отрасли. Шкала для показателя предотвращения последствий (например, вероятности обнаружения отказа) в железнодорожной отрасли основана на использовании квадратного корня из 10 с округлением (приближенно 3).

Таблица В.6 — Описание ранга обнаруживаемости отказа

Ранг обнаруживаемости отказа (D)	Описание
1	Предотвращение последствий почти всегда возможно, например, с помощью независимой технической системы
2	Избежать последствий часто возможно благодаря благоприятным условиям
3	Избежать последствий возможно только иногда из-за неблагоприятных условий
4	Избежать последствий практически невозможно

Иногда шкалы значимости последствий, вероятности возникновения или обнаружения отказа не имеют значений, соответствующих точкам шкалы (в дополнение к описанию). В этом случае аналитик все равно должен убедиться, что соседние уровни приблизительно отличаются на фиксированный множитель по отношению друг к другу. Это может быть сделано посредством выводов с учетом того, что увеличение или уменьшение на один уровень должно означать увеличение или уменьшение, например, значимости последствий или вероятности обнаружения отказа в 10 или в корень квадратный из 10 раз, в зависимости от выбранного множителя.

Устанавливая параметры для вида отказа, целесообразно добавить уровни параметров S, O и D для вида отказа, а не умножать их, поскольку тарированные шкалы параметров являются логарифмическими. Таким образом:

ARPN = S + O + D.

Аналогично В.4.2 виды отказов затем могут быть упорядочены в соответствии с ARPN, более высокий приоритет обычно соответствует более высокому значению ARPN. В дополнение к значению ARPN на решение об обработке может влиять значимость последствий вида отказа, что означает, что если существуют виды отказов с аналогичным или идентичным ARPN, то в первую очередь необходимо рассмотреть виды отказа, имеющие высокую значимость последствий.

Примечание 1 — В некоторых ситуациях действия с ARPN, значение которого превышает определенный порог, невозможны, в других приложениях большое значение имеет высокая значимость последствий, независимо от значения ARPN.

Подход APRN удовлетворяет требованиям непрерывной шкалы критичности и монотонного отображения риска, соответствующего каждому виду отказа, с его RPN. Кроме того, небольшие изменения уровней параметров критичности приводят лишь к небольшим изменениям RPN, что означает, что ARPN менее чувствителен, чем RPN (В.4.2). Следует отметить, что значения ARPN обычно ниже, чем значения RPN для одних и тех же входных значений параметров критичности.

Пример 4 — Идентифицированный вид отказа, который все еще считается приемлемым, может иметь соответствующие значения S = 5, O = 5 и D = 5 и RPN, равный 125, при использовании обычного метода RPN. При использовании альтернативного метода RPN для тех же данных ARPN = 15.

Примечание 2 — Если для всех трех параметров доступны количественные данные, более уместно просто рассчитать риск, перемножив значения без установления полуколичественных диапазонов на шкалах.

Приложение С
(справочное)

Пример отчета об FMEA

С.1 Общие положения

В данном приложении приведены варианты отчета о результатах анализа блока питания путем создания рабочих таблиц и диаграмм из информационной базы данных.

В целом полный отчет должен содержать цели анализа и описывать результаты анализа в соответствии с целями. Поскольку примеры, приведенные в приложении С, являются рабочими таблицами и диаграммами, сгенерированными на основе базы данных, они составляют только часть отчета FMEA (5.2.5.2). В полный отчет FMEA должна быть включена информация, описанная в 5.2.5.2, отчет должен быть понятен всем, кто не связан с выполнением анализа. Дополнительная информация может быть представлена на отдельных листах отчета FMEA.

Дополнительные примеры форм рабочих таблиц для различных применений FMEA приведены в приложении F. Единого формата отчета не существует, поскольку отчет об FMEA зависит от целей и особенностей анализа.

Примечание 1 — Фактическая форма отчета может отличаться от форм, показанных в примерах.

Существуют коммерческие пакеты программ для разработки отчета о результатах FMEA.

Примечани 2 — Для простого анализа с небольшим количеством участников может быть полезно использование электронных таблиц. Для более сложного анализа с несколькими источниками информации и сложными требованиями к отчету может быть полезна реляционная база данных для управления несколькими взаимосвязями между видами отказов, функциями, объектами, компонентами и причинами отказов.

С.2 Пример разработки отчета с использованием информационной базы данных для FMEA блока питания

На рисунке С.1 показано, как можно структурировать информационную базу данных. Если доступна информационная база данных, то FMEA может быть файлом, который связывает следующие базы данных:

- перечень спецификаций;
- перечень составных частей (ведомость материалов);
- перечень видов отказов, соответствующих компонентам и продукции организации;
- перечень возможных действий по обработке отказов (база данных о действиях).

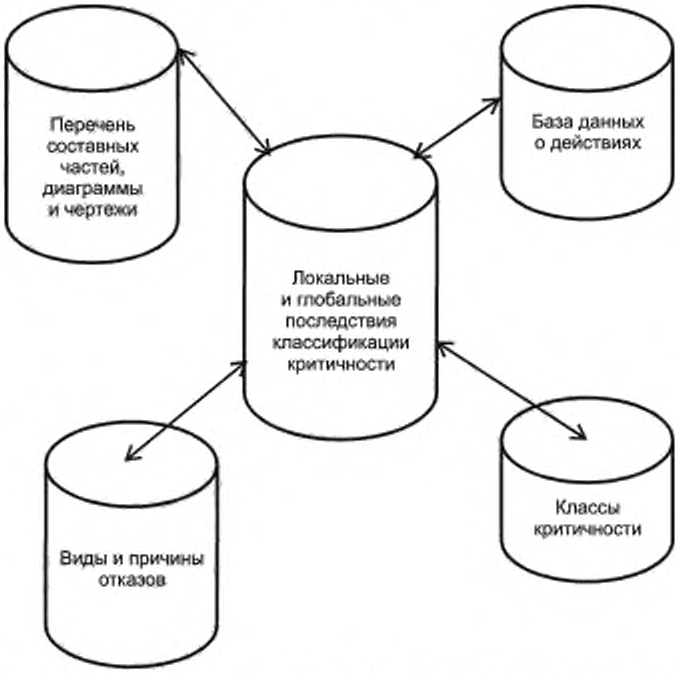

Рисунок С.1 — База данных информационной системы для поддержки разработки отчета об FMEA

Преимущество использования базы данных состоит в том, что информацию не нужно вводить несколько раз и легче поддерживать FMEA в рабочем состоянии, по мере продвижения разработки и появления изменений.

Полный набор полей для отчета об FMEA, которые можно заполнить из информационной базы данных, показан в таблице С.1 на примере источника питания, показанного на рисунке С.2. За счет выбора различных комбинаций полей можно создавать различные рабочие таблицы FMEA (таблицы С.2—С.5) и диаграммы (рисунок С.3).

Для источника питания в процессе FMEA оценивают возможное воздействие отказа внутри устройства только на пользователя. Показанные результаты действительны в любых условиях окружающей среды, указанных в техпаспорте. Данный FMEA отражает только опасности, возникающие в процессе использования источника питания, а не на других стадиях жизненного цикла.

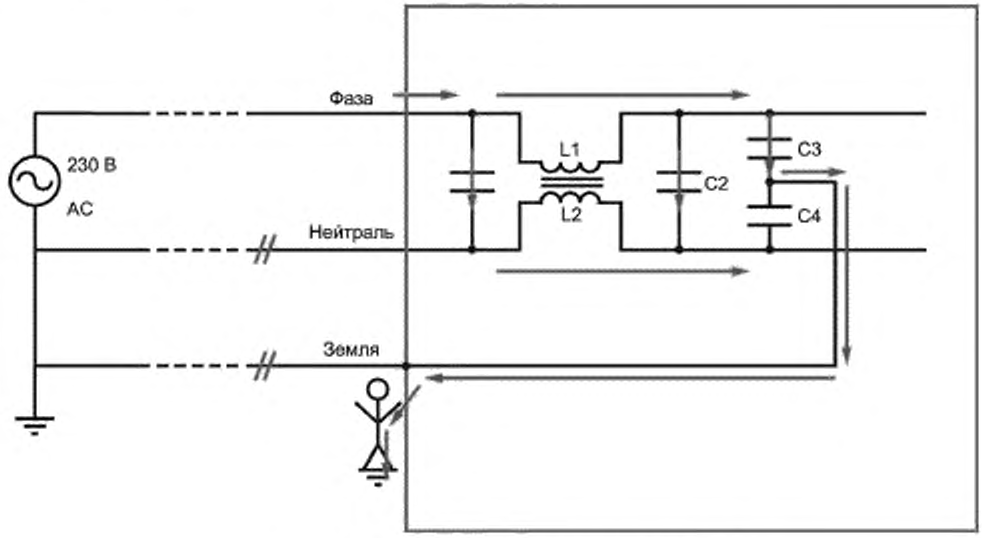

Рисунок С.2 — Схема источника питания типа XYZ

Таблица С.1 — Пример полей, выбранных для отчета об FMEA источника питания на основе информации базы данных

Описание отчета об FMEA	Чертеж объекта	FMEA компонента	FMEA части	FMECA с RPN	RPN FMECA с матрицей критичности	
	Рисунок С.2	Таблица С.2	Таблица С.3	Таблица С.4	Таблица С.5	Рисунок С.3
Дело №					Строка	
Компоненты			Строка	Строка	Столбец	
Перечень составных частей		Строка				
Виды отказов		Столбец	Столбец	Столбец		
Локальное последствие						
Глобальное (окончательное) воздействие			Столбец	Столбец	Столбец	
Значимость последствий			Столбец	Столбец		
Вероятность возникновения отказов				Столбец		
Вероятность обнаружения отказа				Столбец		
Возможный CCF		Столбец				
Действия по обработке (из базы данных действий)			Столбец			

Окончание таблицы С.1

Описание отчета об FMEA	Чертеж объекта	FMEA компонента	FMEA части	FMECA с RPN	RPN FMECA с матрицей критичности	
	Рисунок С.2	Таблица С.2	Таблица С.3	Таблица С.4	Таблица С.5	Рисунок С.3
Определение значимости последствий						
Определение вероятности появления отказа						
Определение обнаруживаемости отказа						
Ссылки на отчеты			Столбец			
Диаграммы/рисунки, чертежи	Да					
Матрица критичности						Да
Анализ дерева неисправностей						

Примечание 1 — Строка (колонка) указывает выбранное поле и должна быть отображена в строке (колонке) отчета FMEA. «Да» указывает на выбранный тип рисунка.

Примечание 2 — Вторая строка этой матрицы относится к последующим различным рабочим таблицам FMEA и матрице критичности (рисунок), приведенной в приложении С.

Таблица С.2 — Пример отчета об FMEA компонента

Отчет FMECA № XX Дата: гггг.мм.дд
Последнее обновление: гггг.мм.дд
Анализируемый объект. блок питания типа XYZ
Фасилитатор: NN1
Аналитическая группа: NN2, NN3, NN4, NN5, NN6, NN7
Одобрено: NN8

Компонент	Вид отказа	Глобальные последствия	Тяжесть последствий	Срок выполнения действий	Ссылка на отчеты (нажмите на иконку, чтобы увидеть отчет)
C1	s/c	Питание отсутствует	2	Отсутствует	Недоступно
C2	s/c	Перегорел предохранитель Питание отсутствует	2	Отсутствует	Недоступно
C3	s/c	В шкафу 230 В	4	Ответственный NN3 Дата ггммдд.	Иконка — Отчет по предохранительным конденсаторам
C4	s/c	В шкафу 230 В	4	Ответственный NN3 Дата ггммдд.	Иконка — Отчет по предохранительным конденсаторам
L1	o/c	Питание отсутствует	2	Отсутствует	Не доступно
L2	o/c	Нейтраль отключена Питание отстутствует	4	Ответственный NN4 Дата ггммдд.	Иконка — Отчет вероятности отказа L2
Выключатель «фазы»	o/c	Питание отсутствует	2	Отсутствует	Недоступно

Окончание таблицы С.2

Отчет FMECA № XX Дата. гггг.мм.дд
Последнее обновление: гггг.мм.дд
Анализируемый объект: блок питания типа XYZ
Фасилитатор. NN1
Аналитическая группа: NN2, NN3, NN4, NN5, NN6, NN7
Одобрено: NN8

Компонент	Вид отказа	Глобальные последствия	Тяжесть последствий	Срок выполнения действий	Ссылка на отчеты (нажмите на иконку, чтобы увидеть отчет)
Выключатель «нейтрали»	о/с	Нейтраль отключена Питание отсутствует	4	Ответственный NN4 Дата ггммдд.	Пока отсутствует
Выключатель «земли»	о/с	Нейтраль отключена Питание отсутствует	4	Ответственный NN4 Дата ггммдд.	Пока отсутствует
Паяные соединения	о/с	Нейтраль отключена Питание отсутствует	4	Ответственный NN5 Дата ггммдд.	Иконка — Отчет об испытаниях на прочность припоя

Примечание — Ранг значимости последствий может варьироваться от воздействия на чувства пользователя до опасности для его здоровья. В рамках данного FMEA решение о предпринятых действиях основывалось исключительно на ранге значимости последствий.

Таблица С.3 — Пример отчета о составных частях с возможными отказами по общей причине

Отчет FMECA № XX
Дата: гггг.мм.дд
Последнее обновление: гггг.мм.дд
Анализируемый объект: блок питания типа XYZ
Фасилитатор: NN1
Аналитическая группа: NN2, NN3, NN4, NN5, NN6, NN7
Одобрено: NN8

Линия перечня составных частей — тип-изготовитель	Обозначение	Вид отказа
#15 конденсатор — тип XYZ, значение XYZ, напряжение XY, поставщик XYZ	C1, C2, C3, C4	s/c
#71 катушка — тип XYZ, номинал XYZ, поставщик XYZ	L1, L2	о/с
# 83 выключатель — тип XYZ, номинал XYZ, ожидаемый срок службы XYZ, поставщик XYZ	Выключатель питания	о/с

Данный перечень создан из перечня составных частей и показывает, какие виды отказов необходимо обрабатывать при использовании. Этот выбор обычно делают для определенного типа устройств, разработанных организацией, информация об их выборе (5.3.4) должна быть доступна и присоединена к отчету.

Примечание — В данном примере перечислены компоненты одного типа с одним и тем же видом отказа. Часто основные причины видов отказов в процессе основного FMEA не анализируют. Поэтому изучение базы данных для определения компонентов, у которых возможны отказы по общей причине, может помочь и сэкономить время при поиске возможных отказов по общей причине.

Таблица С.4 — Пример отчета об FMECA с использованием анализа критичности RPN

Отчет FMECA No. XX дата: гггг.мм. последнее обновление: гггг.мм. дд
Анализируемый объект: блок питания типа XYZ
Фасилитатор NN1
Группа анализа: NN2, NN3, NN4, NN5, NN6 NN7
Одобрение NN8

Значимость последствий	Вероятность возникновения отказа	Вероятность обнаружения отказа	RPN	Компонент	Вид отказа	Глобальные последствия
4	3	5	60	L2	o/c	Отказ o/c нейтрали индикаторная лампа «вкл.»
4	3	5	60	Паяные соединения	o/c	Отказ o/c нейтрали индикаторная лампа «выкл.»
4	2	5	40	Включение «нейтрали»	o/c	Отказ o/c нейтрали индикаторная лампа «выкл.»
4	3	3	36	C3	s/c	230 В на корпусе
4	3	3	36	C4	s/c	230 В на корпусе
3	2	5	30	Включение «земли»	o/c	Отсутствует безопасное заземление
2	3	1	6	C1	s/c	Питание отсутствует
2	3	1	6	C2	s/c	Питание отсутствует
2	2	1	4	Включение фазы	o/c	Питание отсутствует
2	2	1	4	L1	o/c	Питание отсутствует

Примечание — Данный FMECA создан для оценки RPN. Он исследует обновленную схему, которая также включает выключатель питания, который включает все три контакта питания и индикаторную лампу, показывающую, что устройство включено.

Таблица С.5 — Пример отчета FMECA с использованием матрицы критичности глобальных последствий

Отчет FMECA № XX
Дата: гггг.мм.дд
Последнее обновление: гггг.мм.дд
Анализируемый объект: блок питания типа XYZ
Фасилитатор: NN1
Аналитическая группа: NN2, NN3, NN4, NN5, NN6, NN7
Одобрено: NN8

№ строки	Компонент	Глобальные последствия
#1	C1	Питание отсутствует
#2	C2	Питание отсутствует
#3	C3	230 В на корпусе
#4	C4	230 В на корпусе
#5	L1	Питание отсутствует
#6	L2	Нейтраль не подключена, питание отсутствует
#7	Выключатель фазы	Питание отсутствует
#8	Выключатель нейтрали	Нейтраль не подключена, питание отсутствует

Окончание таблицы С.5

Отчет FMECA № XX Дата. гггг.мм.дд Последнее обновление: гггг.мм.дд Анализируемый объект: блок питания типа XYZ Фасилитатор. NN1 Аналитическая группа: NN2, NN3, NN4. NN5, NN6, NN7 Одобрено: NN8		
№ строки	Компонент	Глобальные последствия
#9	Выключатель заземления	Нейтраль не подключена, питание отсутствует
#10	Паяное соединение	Нейтраль не подключена, питание отсутствует
Примечание — В данном примере отчета показана та же функция безопасности, которая включена в матрицу критичности. Схема разработана в виде двумерного изображения без учета обнаруживаемости для оценки последствий для пользователя.		

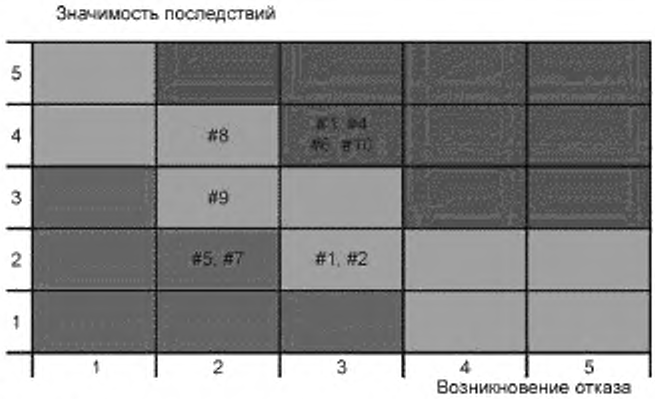

Рисунок С.3 — Матрица критичности для отчета FMECA в соответствии с таблицей С.5, разработанная в виде двумерного изображения, без учета обнаруживаемости

Приложение D
(справочное)

Связь FMEA с другими методами анализа надежности

Сочетание FMEA с другими методами анализа надежности может повысить его результативность.

Например:

- Для определения области применения и в качестве помощи при разработке FMEA может быть использован метод структурной схемы надежности (RBD). Результаты FMEA могут быть впоследствии использованы для пересмотра или обновления RBD.

Примечание 1 — В отличие от FMEA RBD рассматривает успешную работу системы.

- Для выбора важных объектов сложной системы для FMEA может быть использован анализ дерева неисправностей (FTA) с соответствующей вершиной событий.

Примечание 2 — Как и в случае FMEA, FTA рассматривает отказ системы.

- Результаты (нижнего уровня) FMEA могут определять основные события для FTA, и эти события должны быть включены в качестве основных событий FTA.
- Информация, полученная в результате анализа первопричин, может помочь в идентификации причин отказов процесса ([*4*]).
- В дополнение к FMEA, который обычно учитывает только независимые отказы, можно использовать более подробные методы анализа, такие как FTA, RBD, анализ дерева событий (ETA), марковский анализ, сети Петри для учета взаимозависимости событий отказов (порядок появления отказов, условная вероятность возникновения отказов, резервирование, исключение возникновения, отказы по общей причине).
- FMEA может быть использован поэтапно в сочетании с другими методами анализа надежности в процессе разработки объекта или процесса. На стадии концепции FMEA может быть объединен с RBD и FTA для рассмотрения отказов на функциональном уровне. В процессе детального проектирования FMEA может быть разработан на более детальном уровне. Для выбранных критических компонентов или процессов FMEA может быть выполнен на наиболее детальном уровне.
- Прогнозирование безотказности и анализ результатов испытаний или отказов в эксплуатации могут быть использованы для определения количественной оценки вероятности в FMEA.

Примечание 3 — Ссылки на другие стандарты анализа надежности, которые могут быть применимы: RBD (*ГОСТ Р 51901.14*); FTA (*ГОСТ Р 27.302*); ETA (*ГОСТ Р МЭК 62502*); Марковский анализ (*ГОСТ Р МЭК 61165*); Сети Петри ([*10*]); прогнозирование безотказности см. в [7] и *ГОСТ Р 27.013*.

Результаты FMEA обеспечивают информацию о критических аспектах проекта сложного объекта или процесса, эта информация в процессе разработки может быть использована в качестве входных данных или может быть объединена с данными:

- анализа технического обслуживания;
- устранения неисправностей при техническом обслуживании;
- анализа тестируемости;
- определения и спецификации контрольных примеров и анализа результатов испытаний (тестирования);
- анализа логистической поддержки;
- анализа безотказности выполнения целевой задачи;
- анализа готовности;
- оценки последствий изменения конструкции (проекта);
- документации об обязательных целях (например, одобрение безопасности для конкретной системы или для определенного типа систем).

Приложение Е
(справочное)

Прикладные аспекты применения FMEA

Е.1 Общие положения

В данном приложении рассмотрено общее применение FMEA и конкретные вопросы, которые необходимо рассмотреть при проведении FMEA в соответствии с общей методологией, приведенной в настоящем стандарте, и руководством по адаптации, приведенным в приложении А. Рассмотренные варианты применения не являются исчерпывающими.

Обсуждаемые варианты применения FMEA могут включать определенные требования в отношении анализа критичности (например, безопасности) или могут обеспечивать совместимость с конкретными стандартами (например, FMECA в рамках технического обслуживания, ориентированного на безотказность). Также рассмотрено использование FMEA для сложных систем (например, безотказность и готовность по модулям и компонентам).

Е.2 FMEA программного обеспечения

FMEA программного обеспечения аналогично FMEA аппаратного обеспечения, процедур и функций. Для программного обеспечения обычно устанавливают, что:

- ошибка программного обеспечения — это ошибка в программном коде,
- программная ошибка — это проблема с выполнением процедуры/функции,
- отказ программного обеспечения — это полная или частичная деградация конкретной функции программного обеспечения.

Дефекты в программном обеспечении (обычно называемые «ошибками») могут привести к отказу программного обеспечения. Последствия такого отказа для функций программного обеспечения и выхода программного обеспечения могут быть проанализированы, как и для любого другого объекта. Вероятность отказа можно оценить как количество случаев активации функции, содержащей «ошибку», деленное на общее количество выполнения функции, но поскольку эта информация обычно недоступна, количественный анализ редко возможен. Состояния отказа в программном обеспечении часто являются неустойчивыми и в некоторых случаях могут быть устранены путем переустановки программного обеспечения. Все отказы программного обеспечения связаны с проектом, независимо от того, были ли они вызваны неверной интерпретацией требований, ошибками в кодах, нехваткой памяти, наличием разомкнутых циклов, синтаксическими ошибками и т. п.

Программное обеспечение может быть проанализировано сверху вниз или снизу вверх. Как и оборудование, программное обеспечение разбивают на несколько уровней, например пакет программ, программные модули и функции кода (таблица 1). Для каждого элемента анализ должен рассматривать вход, выполнение и выход. Выполнение зависит от начальных условий до ввода данных, например положения в структуре меню, содержимого регистров и памяти (ОЗУ, а также ПЗУ). На более низких уровнях отказы могут возникать во входных данных (например, неверные или поврежденные данные), в начальных условиях (например, неправильная позиция в меню, неверное или поврежденное содержимое памяти) или из-за неправильной работы (например, ошибок в алгоритмах). Отказы на уровне системы часто связаны с выходными данными (например, поврежденные выходные данные или неверные данные). Наконец, выход программного обеспечения может вызвать проблемы взаимодействия с аппаратным обеспечением, например проблемы синхронизации. Анализ обычно фокусируется на видах отказов, связанных с программным обеспечением, однако причины, показатели и последствия отказов могут быть связаны с соответствующим аппаратным обеспечением. Поэтому в анализе должны участвовать как аналитики, знающие программное обеспечение, так и аналитики, знающие аппаратное обеспечение.

Глубина и область применения FMEA программного обеспечения могут быть различны. FMEA может быть ограничен только программными компонентами или модулями. При запуске на раннем этапе разработки программного обеспечения FMEA может быть направлен на функции программного обеспечения, необходимые для работы системы, и на возможные ошибки или отказы, которые могут стать причиной отказа функции в одном или нескольких видах отказа. Такой анализ выполняют в начале разработки программного обеспечения и используют в качестве источника информации для создания контрольных примеров программного обеспечения. По мере разработки системы влияние программных ошибок, сбоев или отказов может быть определено лучше, а также определены обстоятельства или их комбинации, которые могут вызвать отказ.

Ключевые причины отказов могут представлять собой ошибки программиста («ошибки»), а также причины, связанные с состоянием аппаратных средств. Для выполнения FMEA необходимо определить, может ли единичный отказ программного обеспечения стать причиной неприемлемых локальных последствий (помимо конечных/глобальных последствий), например:

- переменная принимает непредусмотренное значение;
- сообщение содержит непредусмотренные данные или затрачивает на выполнение неожидаемое время;
- модуль дает неожидаемые выходы.

Затем анализируют каждый вид отказа для (конечных) последствий системы. Это правило, основанное на анализе сложных единичных последствий, которые зависят от времени и состояния системы. Перед выполнением FMEA для программного обеспечения необходимо провести отдельный анализ спецификации требований. Поскольку программная ошибка или сбой часто приводят к нежелательным последствиям для аппаратного обеспечения, сначала необходимо выполнить FMEA для аппаратного обеспечения, чтобы установить влияние системы. В этом случае последствия для системы программного обеспечения могут основываться на последствиях для системы аппаратного обеспечения.

Следующий перечень основан на примерах, приведенных в [*11*]. FMEA программного обеспечения также должно учитывать условия эксплуатации, например:

- аппаратные отказы, вызывающие отказ памяти;
- периферические отказы карты памяти (например, отказы аналоговых/цифровых преобразователей или устройств ввода-вывода);
- отказ источника питания, например сброс из-за падения напряжения питания;
- электромагнитные помехи (EMI), электромагнитные импульсы (EMP);
- неправильно обработанные неверные входные данные, включая ошибки загрузки.

Примеры причин отказа на уровне системы:

- неправильное использование вызовов операционной системы;
- неверная синхронизация, например коллизия данных из-за изменения времени передачи данных;
- прерывание обработки и неадекватный анализ;
- неадекватная или отсутствующая обработка исключений.

Примеры ошибок программирования (причины отказов):

- ошибки проектирования и выполнения (например, при кодировании, масштабировании, разработке алгоритмов);
- неадекватное обнаружение ошибок (например, нарушение границ, указатели вне диапазона);
- неадекватное определение допустимого диапазона;
- непреднамеренная перезапись в памяти;
- неадекватная обработка ошибок программного обеспечения (например, неожиданная ситуация).

Примеры видов отказов:

- неправильная точка выхода, превышение времени, неожиданное взаимодействие ввода-вывода;
- недостающие данные, неверные данные, неверная синхронизация данных, особые данные;
- ненормальное завершение, пропущенные события, неверные логика, синхронизация/порядок;
- остановка, аварийный отказ, зависание, медленная реакция, отказ запуска, ошибочные сообщения.

Если анализ выполняют с использованием электронной таблицы, обычно можно использовать следующие столбцы:

a) иерархия системы и компонентов;

b) обозначения компонентов;

c) виды отказов

d) причины отказов;

e) последствия неготовности отказавшей функции (при восстановлении программного обеспечения);

f) смягчающее обеспечение проекта (меры по восстановлению проекта, альтернативные пути, защита от отказов);

g) компенсационное обеспечение;

h) закрытие вопроса;

i) окончательное снижение неготовности функции в результате идентификации вида отказа.

На рисунке Е.1 показан пример модели отказа программного обеспечения.

По мере разработки конструкции аппаратного обеспечения анализ рассматривает систему в целом, включая программное и аппаратное обеспечение, и направлен на функции системы и их цепочки.

FMEA аппаратного обеспечения изменяется вслед за программной частью, анализ может разрастись до нежелательных размеров при поиске цепочки последствий, приводящих к отказу системы, и оценке влияния их деградации или значимости их потери на работу системы. При анализе смешанной аппаратно-программной системы предпочтительной практикой является отслеживание функции системы по ветвям сверху вниз для идентификации компонентов программного обеспечения, их возможных ошибок или неисправностей и возможных видов отказов, а также их причин.

Следует помнить, что FMEA одновременно исследует только один вид отказов, он не предназначен для рассмотрения функциональных зависимостей, последовательностей событий (отказов) или комбинаций событий. Отказ аппаратного обеспечения может быть причиной отказа программного обеспечения, а с точки зрения FMEA отказ программного обеспечения является следствием отказа аппаратного обеспечения.

FMEA программного обеспечения — один из методов (помимо тестирования), который помогает повысить безотказность программного обеспечения. Тестирование также может быть использовано в качестве обработки видов отказов, которые считаются критическими.

Рисунок Е.1 — Общая модель отказа программного обеспечения для компонента программного обеспечения

Е.3 FMEA процесса

Для процессов и процедур общая методология FMEA такая же, как и для аппаратного и программного обеспечения. Начальной точкой анализа является схема работы процесса, структура деления работ или анализ задач. Процесс подразделяют на элементы, которые являются этапами процесса. Уровень декомпозиции выбирают в соответствии с областью применения анализа. Функцию каждого этапа или его предполагаемого выхода определяют с помощью описания функции, достаточно специфичного, чтобы был ясен уровень работы, представляющий собой отказ. Как и в случае FMEA аппаратного и программного обеспечения, варианты отказа функций процесса должны быть перечислены в качестве видов отказов в FMEA процесса. Последствия отказа, механизмы и возможные причины отказа также должны быть определены. Механизмы и причины отказов часто охватывают как ошибки человека, так и отказы оборудования. Анализ критичности может быть применен так же, как описано в общем руководстве FMEA.

FMEA процесса впервые был применен к производственным процессам, но теперь его применяют более широко. Например, его широко используют при анализе медицинских процедур в здравоохранении.

Е.4 FMEA при проектировании и разработке

FMEA — неотъемлемая часть процесса проектирования, от концепции до разработки системы. FMEA — итеративный процесс, он начинается, как только появляется предварительная информация о проекте на высшем уровне системы, и распространяется на более низкие уровни иерархии системы по мере поступления большого количества информации. Адаптация FMEA (приложение А) должна гарантировать, что он вносит существенный вклад в решения организации в отношении осуществимости и адекватности подхода к разработке проекта.

Целью FMEA в процессе проектирования является идентификация видов отказов внутри системы и возможных критических отказов, которые могут быть устранены или сокращены с помощью проектных решений как можно раньше.

В дополнение к ориентации на надежность FMEA поддерживает усилия по сопровождению, техническому обслуживанию и анализу риска.

Е.5 FMEA в рамках технического обслуживания, ориентированного на безотказность

Для разработки успешной программы технического обслуживания, ориентированного на безотказность, необходимо четкое понимание функций объекта, отказов и последствий с точки зрения целей организации при эксплуатации объекта.

FMEA и метод анализа критичности подходят для применения к техническому обслуживанию, ориентированному на безотказность, если анализ структурирован таким образом, что соответствует требованиям стандарта технического обслуживания, ориентированного на безотказность (*ГОСТ Р 27.606*).

Для структурирования анализа необходимо, чтобы все виды отказов были четко связаны с потерей функции на соответствующем уровне иерархии объекта и чтобы такие аспекты, как «средства обнаружения» отказов, были согласованы с потенциальными задачами технического обслуживания.

Е.6 FMEA для систем управления, связанных с безопасностью

Е.6.1 Общие положения

Применительно к безопасности FMEA используют в различных ситуациях. Метод FMEA является одной из альтернатив при планировании функций, связанных с безопасностью, или анализе риска.

Пример 1 — Некоторые стандарты (например, ГОСТ Р МЭК 62061 и ГОСТ Р МЭК 61508 (все части)) требуют применения определенных форм анализа при установлении подходящих методов обработки риска, при создании функций, связанных с безопасностью, или при разработке устройств для использования таких функций. FMEA — один из методов, который можно использовать при планировании функций, связанных с безопасностью.

Применительно к безопасности FMEA классифицирует виды отказов функции, связанной с безопасностью, на безопасные и опасные. Классификация может быть различной в зависимости от условий использования, структуры системы, окружающей среды.

Пример 2 — Для многих систем безопасным состоянием (неизменным безопасным состоянием системы) является обесточенное состояние (выключенное состояние). Отказ тормозной системы воздушного судна можно считать безопасным отказом, когда самолет находится на земле, но этот отказ становится опасным отказом при взлете или посадке (переменное безопасное состояние системы (см. [12]).

Некоторые стандарты безопасности требуют, чтобы единичные отказы были обнаружены так, чтобы это приводило к безопасному состоянию или сохранению безопасного состояния за счет функциональной избыточности (резервирования), напрямую не приводило к небезопасному состоянию.

При ранжировании действий применительно к безопасности действия по проектированию должны в первую очередь рассматривать последствия отказов и не должны использовать экономические компромиссы. Следовательно, при проектировании действия должны быть направлены:

- на снижение вероятности опасных отказов;
- распознавание или обнаружение появления опасных отказов и соответствующее реагирование на них;
- оповещение пользователя о безопасном состоянии устройства;
- устранение или снижение вероятности отказов, вызванных ошибками или непониманием человека.

Е.6.2 FMEA при планировании применительно к безопасности

FMEA может быть применен на уровне системы на этапе планирования разработки применительно к безопасности. Виды и последствия отказов всех компонентов системы и их взаимодействие систематически оценивают для определения их влияния на безопасность системы.

FMEA также может быть применен в других точках проекта, где при определении методов обработки для повышения безопасности могут быть использованы идентификация риска и анализ влияния риска на функции, связанные с безопасностью. Целью FMEA в области безопасности является поиск всех элементов, связанных с функцией безопасности, и всесторонняя идентификация источников вреда. Методы, способствующие комплексной идентификации, включают в себя контрольные перечни, исследования и использование экспертных оценок в широком диапазоне.

Меру риска, основанную на тяжести вреда и качественной оценке вероятности опасного события, используют для определения требуемой целостности безопасности систем управления электрических, электронных и программируемых электронных, связанных с безопасностью в соответствии с *ГОСТ Р МЭК 62061*.

Вероятность нанесения вреда учитывает:

- частоту и продолжительность воздействия опасности на людей;
- вероятность возникновения опасного события;
- возможность избежать или ограничить возможный вред.

Эти три фактора наряду со значимостью последствий используют для создания класса необходимого снижения риска при применении. Такие классификации используют в нескольких стандартах, связанных с безопасностью.

Примечание — В *ГОСТ Р МЭК 61508* (все части) и *ГОСТ Р МЭК 62061* использован термин SIL (уровень целостности безопасности) для такой классификации.

Пример — В ГОСТ Р МЭК 62061 для наивысшей категории снижения риска требуется уровень SIL3, который эквивалентен интенсивности отказов функции управления безопасностью от 10^{-8} до 10^{-7} в час.

Е.6.3 Анализ критичности, включающий диагностику

Дополнительный уровень детализации включен в так называемый анализ видов, последствий и диагностики отказов (FMEDA).

Примечание 1 — Метод FMEDA также используют для систем, не связанных с безопасностью.

Способность системы или подсистемы обнаруживать внутренние отказы, предпочтительно с помощью автоматической онлайн-диагностики, имеет решающее значение для достижения и сохранения правильного функционирования сложных систем и систем, которые не могут в полной мере использовать все функциональные возможности в нормальных условиях, таких как редкие запросы системы аварийного отключения (система ESD). При оценке целостности системы, связанной с безопасностью, всем анализируемым компонентам добавляют количественные данные об интенсивности отказов (интенсивность отказов и распределение видов отказа). Кроме того, количественно определяют способность системы обнаруживать внутренние отказы.

Если анализируемые компоненты являются электронными устройствами, интенсивность отказов должна иметь соответствующую сопроводительную документацию для обоснования ее оценки, в идеале из опыта эксплуатации на местах. Интенсивность отказов для каждого компонента определяют на основе сведений из баз данных, для которых доказана их пригодность для данной цели. Кроме того, распределения видов отказов могут быть выведены из аналогичных источников или из стандартов (например, [7]), их, как правило, приводят в процентах от общего количества.

Примечание 2 — Интенсивность отказов часто указывают в виде количества отказов в единицу времени (FIT). FIT означает 10^{-9} отказов в час.

Примечание 3 — Распределение видов отказов соответствует доле общей интенсивности отказов компонента, которая может быть приписана каждому из видов отказов.

Во многих случаях также указывают интенсивность отказов для отказов, которые не влияют на функцию безопасности, или отказов составных частей, которые не являются частью функции безопасности, но эти интенсивности не влияют на дальнейшие вычисления.

При оценке электронного устройства анализ учитывает каждый электрический компонент и его влияние на функцию безопасности, что позволяет сделать вывод о том, какое влияние оказывает отказ на функцию безопасности.

Отказы обычно делят на безопасные отказы, опасные обнаруженные отказы, опасные необнаруженные отказы и отказы, которые не влияют на функцию безопасности. Для проверки полноты оценки иногда целесообразно перечислить компоненты, которые не влияют на функцию безопасности.

Решение о том, является ли опасный отказ обнаруженным или необнаруженным, определяется значением диагностического охвата, которое может быть выведено на основе соответствующей диагностической схемы и оценки ее результативности. Значение прибавляют к оценке, сумма характеризует качество устройства для использования в рамках функции безопасности. Полученные значения также могут быть использованы для расчета интенсивности отказов или других показателей безотказности функции безопасности или показателей качества функции безопасности, таких как доля безопасных отказов (SFF) или общий диагностический охват (DC). Определение значений этих характеристик зависит от условий, для которых они определены.

Результатом является ранг значений вероятности отказа, который позволяет оценить общий риск, соответствующий отказу функции безопасности в случае возникновения ее запроса.

При недостатке информации о возможных видах отказов и их распределении по электрическим компонентам FMEA снова является подходящим методом сбора информации о возможных видах отказов. Исходя из этого могут быть начаты практические эксперименты или теоретические обсуждения для определения этих значений.

Примечание 4 — Данный метод и возможности исключения ошибок описаны в *ГОСТ ISO 13849-1*.

Е.7 FMEA для сложных систем с распределением безотказности

Е.7.1 Общие положения

FMEA может быть использован для сложных и ответственных систем, от оборонного и аэрокосмического сектора до водоснабжения, канализации, транспорта, связи, производства и распределения электроэнергии. В этих системах требования к показателям готовности, ремонтопригодности и безотказности могут быть распределены по элементам системы. Адаптированный FMEA может быть проведен с рассмотрением характеристик отказа каждого элемента для понимания влияния на систему таких конструктивных особенностей, как использование общих компонентов и резервирования.

Е.7.2 Оценка критичности для невосстанавливаемых систем с распределенной вероятностью отказа

В процессе FMEA для сложной, не восстанавливаемой системы частоты возникновения, вероятности, интенсивности отказов или другие соответствующие показатели могут быть распределены для каждого последствия на уровне системы. Это распределение можно сравнить с приемлемым риском системы, распределенными вероятностями и значимостью в матрице риска.

Локальные последствия каждого отказа на самом низком уровне иерархии системы можно привести к последствиям на более высоком уровне и, наконец, на уровне системы. Эти фактические оценки риска затем можно сопоставить с согласованным уровнем приемлемого риска. Если критичность превышает допустимое значение, необходимо проследить ее появление до той составной части системы, откуда она возникает.

Оценки вероятностей отказов можно сравнить с допустимыми пределами для каждого уровня значимости, чтобы определить составные части или компоненты на более низком уровне с чрезмерной критичностью. Затем

выполняют инженерные действия для снижения критичности компонентов путем снижения вероятности отказа или другие меры смягчения последствий отказа. Этот процесс показан на рисунке Е.2.

Часто предполагается, что если критичность компонента более низкого уровня не превышает приемлемый уровень, то никаких действий предпринимать не нужно. Это особенно неверно, когда имеется много аналогичных компонентов, которые могут оказывать одинаковое воздействие на подсистемы или систему. Общее суммарное воздействие отказов всех компонентов, имеющих одинаковую вероятность и значимость последствий, не должно превышать допустимую вероятность отказов сборочной единицы, в которой они находятся. Эта мера гарантирует, что определенная критичность на уровне системы не будет превышена.

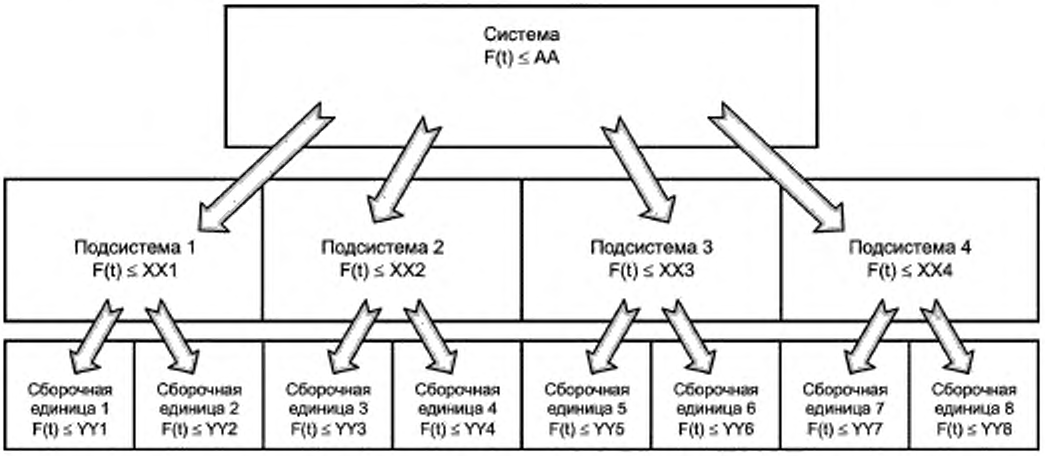

Рисунок Е.2 — Распределение вероятностей отказа в системе

Е.7.3 Оценка критичности для восстанавливаемых систем с распределением показателя неготовности

Требования к готовности для восстанавливаемых систем распределяют по показателям надежности, таким как среднее время между отказами (MTBF) для безотказности и среднее время восстановления (MTTR) для ремонтопригодности системы. Показатель неготовности системы обычно используют для оценки критичности системы. Оценка коэффициента неготовности аналогична оценке вероятности отказа (ненадежности). Коэффициент неготовности распределяют по подсистемам и сборочным единицам, он имеет два измерения, поскольку зависит от двух показателей, MTBF и MTTR.

Процесс распределения на уровне системы, подсистемы, сборочных единиц аналогичен распределению в Е.7.2, за исключением того, что вместо вероятности появления вида отказа, для вида отказа выводят коэффициент неготовности системы, подсистемы и сборочных единиц. Виды отказов, вызывающие неприемлемый уровень неготовности, должны быть обработаны.

Приложение F
(справочное)

Примеры применения FMEA в различных отраслях промышленности

F.1 Общие положения

Приведенные ниже примеры представляют собой фрагменты рабочих таблиц FMEA с кратким объяснением области применения.

Примечание — Приведенные фрагменты являются частью рабочих таблиц FMEA и содержат только краткие описания. Это означает, что в примере отсутствует полное рассмотрение целей и границ FMEA, даже если они крайне важны для анализа.

F.2 Применение к процессу заказа лекарств

В таблице F.1 приведена выдержка из таблиц FMEA процесса заказа лекарственного средства в аптеке. В примере показан один этап процесса с видами, последствиями и причинами отказов.

Таблица F.1 — Фрагмент FMEA процесса заказа лекарственного средства в аптеке

Этап процесса	Функция	Вид отказа	Последствие отказа	Механизм отказа	Причина отказа
Готовое лекарственное средство	Лекарственное средство с правильным действием, составом и концентрацией подготовлено	Неправильный препарат	Зависит от выбранного препарата	Неправильный выбор (правильное намерение) Неправильно прочитанный рецепт Рецепт допускает неоднозначное понимание	Препараты выглядят одинаково Неясное написание рецепта Использование сокращений
		Неправильная концентрация	Завышенная доза Недостаточная доза	Ошибка расчета Недостаток знаний Неправильно прочитанный рецепт	Невнимательность Неясное написание рецепта Недостаток опыта
		Неправильный разбавитель	Возможная токсичность разбавителя	Неправильный выбор (неверное намерение) Неправильный выбор (правильное намерение)	Отсутствие знаний Недоступность правильного разбавителя Внешняя схожесть емкостей (упаковок)

F.3 Применение к производственному процессу распыления краски

В таблице F.2 показана выдержка из таблиц FMEA производственного процесса распыления краски. В примере показан один этап процесса с видами, последствиями и причинами отказов.

Таблица F.2 — Фрагмент FMEA этапа распыления краски в производственном процессе

Этап процесса	Функция	Вид отказа	Последствие отказа	Механизм отказа	Причина отказа
Аэрозольное распыление краски	Нанесение гладкой пленки толщиной 75 мкм	Краска слишком густая	Плохой внешний вид. Деталь забракована	Слишком много краски	Распылитель расположен слишком близко Отказ регулятора краски

Окончание таблицы F.2

Этап процесса	Функция	Вид отказа	Последствие отказа	Механизм отказа	Причина отказа
		Эффект апельсиновой корки	Плохой внешний вид	Капли краски высыхают до слияния	Слишком мало воздуха Температура при распылении слишком высокая Слишком широкий веер распыления Слишком большое расстояние до распылителя

F.4 Применение к водяному насосу

F.4.1 Общие положения

Ниже приведен простой пример FMEA для выделения информации, используемой на каждом этапе анализа для отдельного водяного насоса с расчетной скоростью потока 600 л/мин, который подает охлаждающую воду в теплообменник. Скорость потока 400 л/мин обеспечивает идеальные условия охлаждения. Анализ представлен в виде описательной части, но может быть записан в табличной форме или в форме базы данных.

F.4.2 Функция объекта

Функции насоса:

1) подача воды в первичный теплообменник с производительностью 400 л/мин ± 30 л/мин;

2) хранение воды с утечкой менее 0,01 л/час.

Примечание — Насос имеет дополнительные конструктивные возможности для обеспечения требуемого обслуживания (критерий мощности в зависимости от нагрузки). В данном примере, если насос не достигает своей полной проектной мощности, выход ниже максимума может не отражать потерю функции.

F.4.3 Виды отказов объекта

Виды отказов насоса для функции 1:

А. Подача воды в первичный теплообменник с интенсивностью менее 370 л/мин;

В. Подача воды в первичный теплообменник с интенсивностью более 430 л/мин.

Виды отказов насоса для функции 2:

А. Утечка воды с интенсивностью более 0,01 л/ч, но менее или равной 1 л/ч;

В. Утечка воды с интенсивностью более 1 л/ч.

Примечание — Виды отказов часто просто противоположны требуемой функции (например, функции 1), но часто могут быть расширены до включения установленных уровней, на которых происходит потеря функции (например, функции 2). Обычно это имеет значение только в том случае, если с каждым уровнем связаны различные последствия.

F.4.4 Последствия отказа объекта

Последствия видов отказов насоса 1А:

- локальные: нет;
- конечные: остановка процесса (из-за недостаточного охлаждения).

Последствия видов отказов насоса 1В:

- локальные: нет;
- конечные: продукт не соответствует спецификации (из-за чрезмерного охлаждения).

Последствия видов отказов насоса 2А:

- локальные: нет;
- конечные: химическое загрязнение (вода испаряется, выделяя химические вещества).

Последствия видов отказов насоса 2В:

- локальные: нет;
- конечные: остановка процесса (переполнение емкости, повреждение электрооборудования).

Примечание — В результате такого анализа в емкости может быть размещено устройство, подающее сигнал о переполнении емкости. Анализ такого аварийного сигнала показал, что его отказ сам по себе не имеет последствий, но приводит к остановке процесса в случае утечки.

F.5 Применение FMEA с анализом критичности к сложной невосстанавливаемой системе

В данном примере использованы значения вероятности отказа. На рисунке F.1 показана иерархическая структура электронной системы, состоящей из четырех последовательных подсистем, каждая из подсистем имеет две сборочные платы с различными последовательными электронными компонентами. На рисунке F.1 также показано распределение значений вероятности отказа в системе, подсистемах и сборочных единицах.

В таблице F.3 показаны распределение и оценка значений вероятности отказа для различных категорий критических видов отказов этой системы. Данные таблицы F.3 показывают, что виды отказов в категориях III (основные) и II (критические) превышают допустимые уровни, их необходимо исследовать. Чтобы выяснить, какие из подсистем/сборочных единиц вносят наибольший вклад в проблему, необходимо рассмотреть распределение вероятности отказа для сборочных единиц/элементов.

В качестве примера в таблице F.4 показаны распределение и оценка значений вероятности отказа для подсистемы 2. Информация в таблице F.4 показывает, что виды отказов в основных и критических категориях превышают значения, соответствующие распределению вероятности отказа. Вывод состоит в том, что для снижения вероятности отказа системы и приведения критичности системы к допустимому риску необходимо смягчить последствия критических и основных режимов отказов в подсистеме 2 в сборочных единицах 3 и 4.

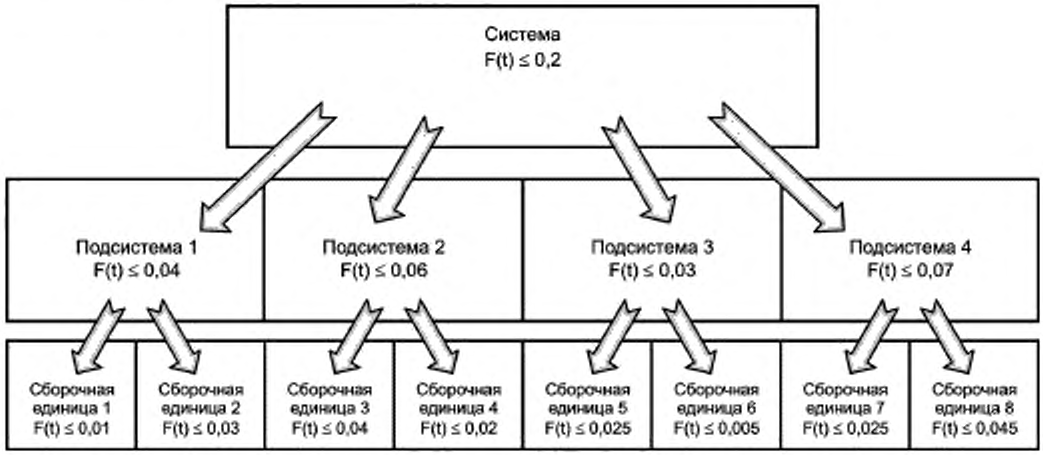

Рисунок F.1 — Иерархия последовательной электронной системы, ее подсистем и сборочных единиц с указанием значений вероятности отказа F(t)

Таблица F.3 — Распределение и оценка значений вероятности отказа для различных категорий критичности видов отказов для электронной системы, представленной на рисунке F.1

Критичность	V Незначительная	IV Малая	III Средняя	II Критическая	I Катастрофическая
Распределение вероятности отказа	≤ 0,1	≤ 0,08	≤ 0,012	≤ 0,0072	≤ 0,0008
Оценка вероятности отказа	0,06	0,05	0,03	0,01	0,0002

Таблица F.4 — Распределение и оценка значений вероятности отказа для различных категорий критичности видов отказов подсистемы 2 системы, представленной на рисунке F.1

Критичность	V Незначительная	IV Малая	III Средняя	II Критическая	I Катастрофическая
Распределение вероятности отказа	≤ 0,03	≤ 0,02	≤ 0,0052	≤ 0,0047	≤ 0,00007
Оценка вероятности отказа	0,006	0,002 1	0,029	0,008	0,00002

Это распределение и оценка вероятности отказа для четырех подсистем и соответствующих им сборочных единиц завершены. Если вероятность отказа является неприемлемой, могут быть предприняты действия для повышения безотказности таких сборочных единиц и достижения сбалансированного результата. После определения новых показателей сборочных единиц эти значения можно пересчитать на уровне системы, используя методы структурной схемы надежности или дерева неисправностей. Следует проявлять осторожность при использовании идентичных компонентов на уровне сборочных единиц, чтобы выявить возможные общие виды отказов этих компонентов.

F.6 Применение к программному обеспечению для расчета уровня сахара в крови

В таблице F.6 показан FMEA для определения сахара в крови с помощью глюкометра, в ней показаны режимы, причины и локальные последствия отказов. Из таблицы видно, как рассматривают этапы мониторинга и различных используемых компонентов для определения видов, последствий и причин отказов глюкометра. Один из очень важных видов отказов глюкометра заключается в том, что при установке микропроцессора программное обеспечение возвращается к заводским настройкам. Если заводские настройки указаны в единицах измерений США, а пользователь изменил их на европейские, то может возникнуть угроза для жизни пользователя.

F.7 Применение к устройству управления автомобильными подушками

В таблице F.7 представлена небольшая часть обширного FMEA, выполненного для подушек безопасности автомобиля. Анализируемое устройство представляет собой источник питания и его соединения (только) с аккумулятором, как показано на рисунке F.2.

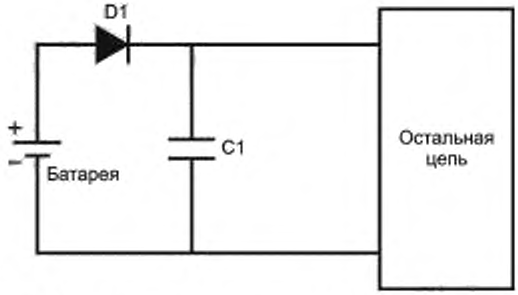

Рисунок F.2 — Часть схемы подушки безопасности автомобиля

Схема включает диод D1 на линии с положительным выходом батареи и конденсатор C1, соединяющий положительную линию с землей. Диод D1 устанавливают так, чтобы если батарея подключена в обратном направлении, ток не может течь по цепи. Конденсатор C1 предназначен для фильтрации напряжения.

Если в C1 произойдет короткое замыкание, положительная сторона батареи станет напрямую соединена с землей, что приведет к перегоранию D1 и к размыканию цепи D1. В этом случае схема управления подушками безопасности станет неработоспособной. Такой отказ считают опасным, в результате чего ему соответствует уровень значимости последствий S = 10. Вероятности возникновения отказов рассчитаны по интенсивностям отказов составных частей, в соответствующих нагрузках в течение срока службы транспортного средства, а затем сопоставлены с 10-балльной шкалой, что привело к выбору O = 3. Вероятность обнаружения признана низкой, поскольку если отказ произойдет во время управления автомобилем, водитель не узнает об отказе. Таким образом, выбрано значение D = 10.

Кроме того, разомкнутая цепь с любой стороны C1 позволяет цепи управления воздушной подушкой работать, но влияет на способность C1 фильтровать входное напряжение в цепи. Отказ размыкания цепи D1 также приводит к отключению цепи управления подушкой безопасности, так как ток не может поступать от батареи. Отказ в виде короткого замыкания D1 позволяет цепи управления подушкой безопасности работать, но при этом нет защиты от обратного тока.

В таблице F.7 столбцы «рекомендуемое действие», «ответственность и целевая дата завершения», а также «результаты обработки» не заполнены. Это отражает ситуацию, когда команда FMEA передает частично выполненный FMEA команде проектировщиков. Затем команда проектировщиков должна рассмотреть риски и предложить действия и сроки. FMEA можно затем завершить, заполнив столбец «результаты обработки».

F.8 Применение к техническому обслуживанию и поддержке Hi-Fi системы

Пульт дистанционного управления — это небольшое устройство, которое позволяет пользователю управлять системой Hi-Fi на расстоянии с помощью инфракрасной связи или радиосвязи. Цель этого примера — показать, как различные FMEA могут быть применимы к одному и тому же объекту. Был выбран очень простой объект и в качестве примеров приведены различные FMEA в сильно сокращенном виде для экономии места. Примеры FMEA системы, конструкции, процесса и технического обслуживания для одного и того же объекта — пульта дистанционного управления системы Hi-Fi показаны в таблицах F.8—F.11 соответственно. FMEA системы разработан на ранней стадии разработки проекта для рассмотрения общей планировки высшего уровня (структуры) объекта. FMEA конструкции исследует проектные решения. FMEA процесса рассматривает производственные процессы, а FMEA технического обслуживания — простоту ремонта объекта (ремонтопригодность).

Этот пример иллюстрирует различия между указанными типами FMEA для одного и того же объекта. Использован индекс приоритетности RPN.

F.9 Применение к системе управления, связанной с безопасностью

F.9.1 Электронная схема

FMEA выполняют для оценки риска, соответствующего безопасности пользовательского интерфейса объекта. Приведен пример анализа видов, последствий и диагностики отказов (FMEDA) для электронной схемы. Пример не завершен; в нем определены виды, последствия и диагностические возможности отказов основных элементов цепи электропитания, в которой использован линейный регулятор внутреннего напряжения в устройстве. Фрагмент FMEDA приведен в таблице F.12.

F.9.2 Автоматизированная система управления поездом

Автоматизированная система управления поездом — это бортовая система, которая останавливает поезд и удерживает его в случае, если путь занят другим поездом. Если стоп-сигнал подан в туннеле, необходимо, чтобы поезд все еще мог перемещаться, чтобы в случае пожара люди, находящиеся в поезде, имели возможность спастись. В данном FMEA рассмотрен риск для здоровья пассажиров.

Если автоматизированная система управления поездом в результате отказа не может остановить поезд при необходимости, может произойти столкновение. С другой стороны, опасно, если автоматизированная система управления поездом не позволяет поезду выйти из туннеля в случае пожара.

Эти опасности являются взаимно обратными, поскольку в одном случае правильно остановить поезд, а в другом — наоборот.

В таблице F.5 показана взаимосвязь видов отказов автоматизированной системы управления поездом, опасностей, безопасных и опасных отказов.

Таблица F.5 — Опасности и безопасные/опасные отказы автоматизированной системы управления движением поездов

Опасности, контролируемые автоматизированной системой управления поездом	Виды отказов автоматизированной системы управления поездом	
	Вид отказов 1 (например, короткое замыкание)	Вид отказов 2 (например, отключение)
Отказ, не позволяющий избежать столкновения	Опасный отказ	Безопасный отказ
Пожар в тоннеле	Опасный отказ	Опасный отказ

F.10 FMEA, включающий человеческий фактор

В таблице F.13 показан FMEA процесса использования кофеварки [*8*]. В этом FMEA оценивают поведение человека и соответствующие виды риска. FMEA включает в себя анализ возможного взаимодействия между вовлеченным человеком, оборудованием и средой для определения видов отказов и вариантов смягчения их последствий. Для более четкого исследования полезно разделять риски для людей и оборудования.

Факторы, связанные с человеком, можно разделить на положительные (предотвращающие отказ или уменьшение значимости последствий) и отрицательные (вызывающие отказ или ошибочные реакции). Люди также могут пострадать, и в некоторых случаях логично различать вред для оборудования и окружающей среды и вред для человека. Пример в таблице F.13 включает человека как источник отказов.

В поле «Категория внимания» различаются периоды, в процессе которых человек ведет себя некорректно. В поле «Психологический анализ причин ошибок» приведены управляющие слова для причин ошибок. Время, в течение которого появляются эти категории ошибок, зависит от количества периодов, в течение которых они могут возникнуть. Это может повлиять на вероятность возникновения ошибки такого типа.

С левой стороны оценивают необходимые обстоятельства для ошибки. В поле «Вид ошибки человека» удобно различать разные группы людей, а также уменьшать или увеличивать значение вероятности в зависимости от размера группы, для которой эта ошибка может быть присуща. Здесь можно провести различие между взрослыми (A) и детьми (C), женщинами и мужчинами (F/M), инвалидами (D) и пожилыми людьми (O) или не указанными лицами (G).

В данном случае было принято решение добавить баллы риска для оборудования и человека, чтобы получить значение риска для системы. Контрмеры также классифицируют таким образом, чтобы различать возможные способы действий: возможность предотвращения возникновения ошибки (O), возможность избежать этого путем инструктажа персонала (I), наличие системы управления, устраняющей события (M), наличие предупреждения людей (E).

Использование таких методов в высокой степени зависит от области применения.

F.11 Процесс маркировки и изоляции электронного компонента

В таблице F.14 приведен фрагмент FMEA процесса, выполняемого для изоляции и маркировки электронного компонента: так называемый внутренний процесс.

Таблица F.6 — Фрагмент таблицы FMEA процесса мониторинга уровня сахара в крови (1 из 2)

Конечный объект: глюкометр Срок эксплуатации: 5 лет			Объект: Программное обеспечение Редакция: 0 6		Подготовлено: NN Дата: 2015-07-31		Обновлено: Кем:	
Этап	Используемый объект	Функция	Вид отказа	Механизм	Причина	Локальные последствия	Метод обнаружения	Компенсационное обеспечение
Установка прибора	Глюкометр	Измерение времени с момента приема последней дозы, данные утреннего среднего значения	Неверная установка времени	Перепутаны 12 ч и 24 ч		Неправильное отображение утренних показаний Пользователь может рассчитать время с последней дозы неправильно	Только если время превышает 12 ч.	Показывать на дисплее AM/PM. Показывать на дисплее время с момента последней дозы
Калибровка		Набор кодирования для партии тест-полосок	Неправильное кодирование	Неправильное кодирование	Ошибка при чтении	Ложно высокий или низкий (ошибка до 30%) уровень сахара в крови	Показания дисплея не совпадают со значениями кодирования, легко ошибиться при чтении	Повторная калибровка каждой партии с образцом раствора
Укол пальца	Ланцет	Отбор проб крови	Недостаточно крови	Пальцы холодные, недостаточная глубина укола		Ложно низкие показания	Нет	
Перенесение крови на тест-полоску	Тест-полоски	Сбор крови и реагирование на нее	Неисправная тест-полоска	Просрочена дата полоски	Закончились непросроченные полоски	Ложно высокие или низкие показания	Проверка даты на полоске	Рекомендация пользователю проверять дату перед использованием полоски
			Неверная реакция	Полоски хранятся при слишком высокой/низкой температуре или высокой влажности	Экстремальные условия окружающей среды	Ложно высокие или низкие показания	Нет	
			Образец крови загрязнен	На уколотом пальце содержатся остатки сахара	Руки не вымыты	Ложно высокие показания	Нет	Инструкция для пользователя

Продолжение таблицы F.6

Конечный объект: глюкометр Срок эксплуатации: 5 лет			Объект: Программное обеспечение Редакция: 0.6		Подготовлено: NN Дата: 2015-07-31		Обновлено Кем:	
Этап	Используемый объект	Функция	Вид отказа	Механизм	Причина	Локальные последствия	Метод обнаружения	Компенсационное обеспечение
			Образец крови загрязнен	На пальце содержатся остатки крема для рук	Руки не вымыты	Ложно низкие показания		Инструкция для пользователя
Вставление тест-полоски в прибор	Тест-полоска, глюкометр	Применение считывающего устройства к полоске	Полоска не вставлена достаточно глубоко	Неопытный пользователь		Ложно низкие показания	Отображение сообщения об ошибке	Инструкция для пользователя
Отсутствие какого-либо сигнала	Индикаторы высокий/низкий	Индикация слишком высокого или низкого уровня сахара в крови		Не выявлен	Слишком слабая индикация			Звуковая сигнализация, различная для высоких и низких показаний
Считывание показаний	Измерительный прибор	Измерение электрического сигнала на электроде и отображение уровня сахара в крови	Отображаются неверные показания	Некоторые сегменты в изображении чисел теряются; например, 8 читается как 6	Низкий заряд батареи	Ложно высокие или низкие показания	Индикатор низкого уровня заряда батареи	
			Слишком густая кровь	Субъект обезвожен		Ложно высокие показания	Отсутствует	
			Отображаются неверные единицы измерения	Неправильная установка единиц измерения пользователем	Недостаток знаний	Ложно высокие или низкие (в зависимости от направления ошибок в 10 раз) показания	Индикатор единиц измерения, пациент обучен распознавать неправильные показания и проводить повторную калибровку в соответствии со стандартным решением	Изображение единиц измерения большими буквами, рекомендация по модификации программного обеспечения, чтобы единицы измерения были жестко подключены

Окончание таблицы F6

Конечный объект. глюкометр Срок эксплуатации: 5 лет			Объект. Программное обеспечение Редакция. 0.6		Подготовлено: NN Дата. 2015-07-31		Обновлено. Кем.	
Этап	Используемый объект	Функция	Вид отказа	Механизм	Причина	Локальные последствия	Метод обнаружения	Компенсационное обеспечение
			Неправильные единицы	При потере заряда батареи установки сбрасываются и восстанавливаются заводские настройки	Преднамеренное изменение при замене батареи	Ложно высокие или низкие (в зависимости от направления ошибок в 10 раз) показания		
					Непреднамеренное изменение при падении напряжения на батарее	Ложный максимум или минимум (в зависимости от направления ошибок) в 10 раз		
					Американец, покупающий счетчик в Европе, не замечает разные единицы (или наоборот)	Ложно высокие или низкие (в зависимости от направления ошибок в 10 раз) показания		
				Отображается правильное число/единицы, ошибка при чтении	Недостаточно четкое отображение показаний			Эргономичный дисплей для легкого чтения
Примечание — Единица измерения уровня сахара в крови — мг/дл в США и ммоль/л в Европе. Между числовыми значениями существует коэффициент, приближенно равный 10.								

Таблица F.7 — Фрагмент таблицы FMEA автомобильной электронной детали FMEA

Элемент/функция			Возможный вид отказа	Возможные последствия отказа		S	Возможная причина/механизм отказа	Детальное описание причины/механизма отказа	O	Текущие превентивные контрольные меры при проектировании	Текущие контрольные меры по обнаружению при проектировании	D	RPN	Рекомендуемые действия	Ответственный и итоговая дата завершения	Результаты обработки отказа				
Подсистема	Сборочная единица	Компонент		Локальное воздействие	Конечное воздействие											Предпринятые действия	S	O	D	RPN
Источник питания																				
	V1																			
		D1	Короткое замыкание	Нет защиты от обратного тока	Элемент не соответствует спецификации	2	Дефект компонента с вероятностью короткого замыкания 80%	Физическое разрушение	3	Выбор компонента более высокого качества и рейтинга	Оценка и испытания на безотказность	10	60							
		D1	Открытый	Нет напряжения на элементе	Элемент неработоспособен	10	Дефект компонента с вероятностью короткого замыкания 20%	Отказ соединения или трещина полупроводника	3	Выбор компонента более высокого качества и рейтинга	Оценка и испытания на безотказность	10	300							
		C1	Короткое замыкание	Полюс аккумулятора замыкает на землю. D1 перегорел	На элементе нет напряжения Элемент неработоспособен	10	Дефект компонента с вероятностью короткого замыкания 10%	Разрушение или трещина диэлектрика	3	Выбор компонента более высокого качества и рейтинга	Оценка и испытания на безотказность	10	300							
		C1	Открытый	нет фильтрации	Элемент не соответствует спецификации	2	Дефект компонента с вероятностью короткого замыкания 90%	Диэлектрик открыт, протекает, отсутствует или треснул	2	Выбор компонента более высокого качества и рейтинга	Оценка и испытания на безотказность	10	40							

Обозначения: S = значимость, O = охват, D = обнаруживаемость.

Примечание — Это частично заполненная таблица FMEA. Команда проекта должна рассмотреть риски и предложить действия и сроки. В результате FMEA заполняют столбцы «результаты обработки отказа».

Таблица F.8 — Фрагмент таблицы FMEA пульта дистанционного управления системой Hi-Fi

Компонент	Функция	Вид отказа	Локальные последствия	Глобальные последствия	Значимость	Вероятность	Обнаруживаемость	RPN	Действия по обработке отказа
Клавиатура	Возможность выбора управляющего действия при применении от 20 до 50 нажатий пальцев	Клавиши под передней панелью, предотвращающие какое-либо усилие большого пальца	Клавиши не могут быть нажаты	Пульт дистанционного управления не может управлять Hi-Fi	4	3	2	24	Печатная плата крепится к верхней панели для уменьшения проблем с допуском
PCB	Интерпретация команд с клавиатуры и передача управляющего воздействия на светодиод в течение 100 мс	Разрушение паяных соединений и контактов из-за механического резонанса	Некоторые сигналы не могут быть переданы на светодиод	Пульт дистанционного управления не может управлять некоторыми функциями Hi-Fi	4	2	5	40	Поддержка при увеличении резонансных частот
Дисплей	Визуальное отображение выбранного действия управления в течение 100 мс после выбора	Дисплей смещается от передней панели пульта дистанционного управления из-за слабого крепления	Дисплей болтается	Требуется ремонт	3	2	3	18	Большая площадь приклеивания

Таблица F.9 — Фрагмент таблицы FMEA конструкции для пульта дистанционного управления системой Hi-Fi

Компонент	Функция	Вид отказа	Локальные последствия	Глобальные последствия	Значимость	Вероятность	Обнаруживаемость	RPN	Действия по обработке отказа
Клавиатура	Преобразование кинетической энергии в электрический сигнал	Неустранимое жидкое загрязнение	Высокое контактное сопротивление	Не работает	4	5	5	100	Пластиковое покрытие под клавишами
Печатная плата	Обработка и передача сигналов	Неустранимое жидкое загрязнение	Высокое контактное сопротивление	Не работает	4	5	5	100	Пластиковое покрытие под клавишами
Дисплей	Отображение сигнала с печатной платы	Высокое сопротивление разъема	Плохой контакт	Пустой дисплей	4	2	5	40	Спецификация разъема и производственные испытания

Таблица F.10 — Фрагмент таблицы FMEA процесса для пульта дистанционного управления системой Hi-Fi

Этап	Функция	Возможные проблемы	Локальные последствия	Глобальные последствия	Значимость	Вероятность	Обнаруживаемость	RPN	Действия по обработке отказа
Пайка разъема для клавиатуры	Формирование связи между клавиатурой и печатной платой	Избыточный флюс	Высокое сопротивление	Прерывистое соединение	4	2	4	32	Отсутствие флюсов
Пайка полупроводникового компонента	Формирование связи между компонентом и печатной платой	Крепежная стойка	Нет подключения компонента к печатной плате	Низкая доходность, что приводит к высоким издержкам производства	2	2	2	8	Планировка печатной платы
Приклеивание ЖК-дисплея к передней панели	Крепление ЖК-дисплея на передней панели	Малая площадь приклеивания	Слабая адгезия	Отделение ЖК-дисплея от передней панели	4	4	5	80	Анализ методом конечных элементов

Таблица F.11 — Фрагмент таблицы FMEA технического обслуживания для пульта дистанционного управления системой Hi-Fi

Компонент	Функция	Вид отказа	Локальные последствия	Глобальные последствия	Значимость	Вероятность	Обнаруживаемость	RPN	Действия по обработке отказа
Клавиатура	Оценка работоспособности клавиатуры	Короткий соединительный кабель между клавиатурой и дисплеем	Сложно смотреть на экран и управлять клавишами одновременно	Время на проведение технического обслуживания увеличилось Риск возникновения ошибки увеличился	3	5	5	75	Сервисный кабель
Печатная плата	Замена печатной платы	Процесс снятия, требующий откручивания винтов	Винтовое отверстие разрушено	Требуется новая передняя панель	4	4	4	64	Металлическая вставка
Дисплей	Замена неисправного дисплея	Невозможно отделить дисплей от передней панели без повреждений	Новая передняя панель	Высокая стоимость ремонта	4	2	4	32	Безотказность дисплея

Таблица F.12 — Фрагмент таблицы FMEDA электронной схемы в системе контроля безопасности (1 из 2)

Принципиальная электрическая схема:
ПЕРЕЧЕНЬ деталей:
Создано: (кем)
Отзыв от:
База данных по интенсивности и распределению: для конкретной компании (пример)
Дата анализа:

Наименование	Компонент	Функция	Интенсивность отказов [FIT]	Вид отказа	Вид отказа	Последствие	Поведенческое последствие S: Безопасное D: Опасное	Диагностическое покрытие
F50	Предохранитель	Защита от короткого замыкания на входе	25	Не открывается	50 %	Нештатная работа	Воздействие отсутствует	—
				Преждевременное открытие	10 %	Выходы обесточены	S	—
				Медленное открытие	40 %	Не влияет на функцию безопасности	Последствие отсутствует	—
D12	Диод подавления	Защита от высокого напряжения	7	Короткое замыкание	95 %	F50 перегорел	S	—
				Обрыв цепи	5 %	Отсутствуют последствия для функции безопасности	Последствие отсутствует	—
R100	Резистор, SMD	Ограничение тока, защита от высокого напряжения	0,2	Короткое замыкание	5 %	Нет текущих ограничений — отказ	D	60 %
				Обрыв	65 %	Выходы обесточены	S	—
				Изменение параметра	30 %	Функция еще поддерживается	Последствие отсутствует	—
C13	Конденсатор керамический, HDC/ MDC	Защита от высокого напряжения	2	Короткое замыкание	50 %	F50 перегорел	S	—
				Обрыв	30 %	Работа не в штатном режиме (защита отсутствует)	Последствие отсутствует	—
				Изменение емкости	20 %	Функция еще поддерживается	Последствие отсутствует	—
D25	Малый диод, сигнал менее 0,1 Вт	Мостовой выпрямитель	1	Короткое замыкание	50 %	F50 перегорел	S	—
				Обрыв	35 %	Отсутствие правильного выпрямления в случае подачи переменного тока	S	—
				Изменение параметра	15 %	Функция еще поддерживается	Последствие отсутствует	—

Окончание таблицы F.12

Принципиальная электрическая схема
ПЕРЕЧЕНЬ деталей:
Создано: (кем)
Отзыв от:
База данных по интенсивности и распределению: для конкретной компании (пример)
Дата анализа

Наименование	Компонент	Функция	Интенсивность отказов [FIT]	Вид отказа	Вид отказа	Последствие	Поведенческое последствие S: Безопасное D: Опасное	Диагностическое покрытие
C2	Электролитический конденсатор, алюминиевый электролит, не твердый электролит	Сглаживающий конденсатор	5	Короткий	53 %	F50 перегорел	S	—
				Открытый	35 %	Работа с источником постоянного тока не в нормальном режиме	Последствие отсутствует	—
				Утечка электролита	10 %	Не влияет на функцию безопасности	Последствие отсутствует	—
				Уменьшение емкости	2 %	Функция еще поддерживается	Последствие отсутствует	—
IC18	Регулятор, мощность более 1 Вт, небольшая сложность	Регулятор напряжения используется с R100 в качестве источника тока	25	Неисправно работает, слишком сильно	30 %	Нет регулирования -> переключение выхода	D	0 %
				Неисправно работает, слишком слабо	30 %	Выходы обесточены	S	—
				Короткое замыкание	15 %	Нет регулирования -> перегрузки по току на реле (разнообразные)	Последствие отсутствует	—
				Обрыв	15 %	Выходы обесточены	S	—
				Смещение	5 %	Функция еще поддерживается	Последствие отсутствует	—
				Функционирование	5 %	Функция еще поддерживается	Последствие отсутствует	—

λ_{du} = 7,504 FIT — сумма интенсивностей отказов, умноженных на уровень распределения (%) всех компонентов с поведением D и DC = 0 %.
λ_{dd} = 0,006 FIT — сумма интенсивностей отказов, умноженных на уровень распределения (%) всех компонентов с поведением D и DC > 0 %.
λ_d = 7,510 FIT = ($\Sigma\lambda_{du}$, λ_{dd}).
λ_s = 25,03 FIT — сумма интенсивностей отказов, умноженных на уровень распределения (%) всех компонентов с поведением S.
$\lambda_{no\,effect}$ = 32,66 FIT — сумма интенсивностей отказов, умноженных на уровень распределения (%) всех компонентов, отказ которых не вызывает последствий.
λ_{total} = 65,2 FIT — сумма интенсивностей отказов всех компонентов.
SFF (доля безопасных отказов) = {(общая интенсивность безопасных и опасных отказов) — (общая интенсивность опасных не обнаруженных отказов)}/(общая интенсивность опасных и безопасных отказов) = (25,03 + 7,510) — 7,504}/(7,510 + 25,03) = 25,036/32,54 = 77,8 %.

Примечание — Распределение представляет процент вида отказов от общего количества отказов.

Таблица F.13 — Выписка из FMEA для кофеварки

Категория «Внимание»	Возможность ошибки (интенсивность ошибок)	Анализ причин психологических ошибок														Анализ последствий
Усталость, монотонная работа	Высокая (0.1 и более)	x			x	x				x	x					
Рутинная работа, отдых	Достаточно высокая (от 0.01 до 0.000001)				x	x										
Позитивные действия	Низкая (0.000001 и менее)				x	x										
Суматоха, паника	Высокая (0.1 и более)				x	x				x	x			x		

Стадия работы	Действие	Связанная среда	Поврежденное оборудование	Взаимосвязь	Вид ошибки человека	Категория людей	Руководящие слова: Восприятие			Решение				Действие								Анализ последствий (опасностей): Оборудование	Человек	Система	Оценка возникновения: Оборудование	Человек	Оценка степени значимости: Оборудование	Человек	Оценка риска: Оборудование	Человек	Система = Человек + Оборудование	Классификация контролер	Контрмера (корректирующее действие)
							Трудно увидеть или услышать	Неправильное восприятие	Нет понимания	Недопонимание	Недостаточное знание	Медленное понимание	Ошибочное понимание	Нет исполнения	Забыто исполнение	Ненадлежащее исполнение	Чрезмерное исполнение	Слишком поздняя исполнение	Слишком ранне исполнение	Различное исполнение	Неверный порядок исполнения												
Разогревание	Включение прибора размещение кофейника на плите	Спешка/ неаккуратность	Неисправленность датчика температуры	И	Кофе оставлен на плите на слишком продолжительное время	G									X							Нарушение	Вторичный ущерб, причиненный пожаром	Пожар	2	1	4	4	8	4	12	0	Резервное время для очищения плиты и посуды
Использование	Наполнение чашки кофе	Усталость	Отсутствует	И	Кофе разлит	G										x		X				Отсутствует	Ожоговая травма / рана	—	1	2	1	3	1	6	7	0	Резервное время для контакта с потребителем

Продолжение таблицы F.13

Категория «Внимание»	Возможность ошибки (интенсивность ошибок)	Анализ причин психологических ошибок															Анализ последствий
Усталость, монотонная работа	Высокая (0.1 и более)	x			x	x				x	x						
Рутинная работа, отдых	Достаточно высокая (от 0.01 до 0.000001)				x	x											
Позитивные действия	Низкая (0.000001 и менее)				x	x											
Суматоха, паника	Высокая (0.1 и более)				x	x				x	x			x			

Стадия работы	Действие	Связанная среда	Поврежденное оборудование	Взаимосвязь	Вид ошибки человека	Категория людей	Руководящие слова: Восприятие			Решение				Действие								Анализ последствий (опасностей): Оборудование	Человек	Система	Оценка возникновения: Оборудование	Человек	Оценка степени значимости: Оборудование	Человек	Оценка риска: Оборудование	Человек	Система = Человек + Оборудование	Классификация контролер	Контрмера (корректирующее действие)
							Трудно увидать или услышать	Неправильное восприятие	Нет понимания	Недопонимание	Недостаточное знание	Медленное понимание	Ошибочное понимание	Нет исполнения	Забыто исполнение	Ненадлежащее исполнение	Чрезмерное исполнение	Слишком позднее исполнение	Слишком раннее исполнение	Различное исполнение	Неверный порядок исполнения												
Очистка	Удаление старого кофе	Спешка	Отсутствует	И Л И	Разлит горячий кофе	G	X															Отсутствует	Ожоговая травма/рана	—	1	2	1	4	1	8	9	0	Резервное время для очищения
	Ручное очищение	Спешка	Наличие острых углов и краев	И	Касание края голыми руками	G													X			Отсутствует	Ожоговая травма/рана	—	1	2	2	4	2	8	10	W	Разрешить только автоматическое очищение

Окончание таблицы F.13

Категория «Внимание»	Возможность ошибки (интенсивность ошибок)	Анализ причин психологических ошибок															Анализ последствий
Усталость монотонная работа	Высокая (0.1 и более)	x			x	x				x	x						
Рутинная работа, отдых	Достаточно высокая (от 0.01 до 0.000001)				x	x											
Позитивные действия	Низкая (0.000001 и менее)				x	x											
Суматоха, паника	Высокая (0.1 и более)				x	x				x	x			x			

Стадия работы	Действие	Связанная среда	Повреждение оборудования	Взаимосвязь	Вид ошибки человека	Категория людей	Руководящие слова															Анализ последствий (опасностей)			Оценка возникновения		Оценка степени значимости		Оценка риска			Классификация контрмер	Контрмера (корректирующее действие)
							Восприятие			Решение				Действие								Оборудование	Человек	Система	Оборудование	Человек	Оборудование	Человек	Оборудование	Человек	Система = Человек + Оборудование		
							Трудно увидеть или услышать	Неправильное восприятие	Нет понимания	Непонимание	Недостаточное знание	Медленное понимание	Ошибочное понимание	Нет исполнения	Забыто исполнение	Ненадлежащее исполнение	Чрезмерное исполнение	Слишком поздняя исполнение	Слишком ранняя исполнение	Различное исполнение	Неверный порядок исполнения											
Хранение	Хранение	Холодная окружающая среда	Трещины из-за замерзания воды	—	Вода не удалена	G	x								x							Опасность	Отсутствует	Нет готовности	4	4	4	2	16	8	24	W	Предупреждение в инструкции по эксплуатации

Примечание 1 — Категория человека — G: не указано M: мужчина; A: взрослый; F: женщина; C: ребенок; O: пожилой человек; I: инвалид.

Примечание 2 — Классификация контрмер — O: Меры по предотвращению возникновения ущерба; S: Меры по предотвращению распространения ущерба; W: Меры по предупреждению повреждения; E: Обучение пользователей безопасному использованию; M: Анализ системы управления безопасностью.

Таблица F.14 — Фрагмент таблицы FMEA процесса маркировки и изоляции электронного компонента

Требование к функции процесса	Возможный отказ	Возможные последствия отказа	S	Возможная причина/механизм отказа	O	Текущие средства контроля процесса	D	RPN	Рекомендуемые действия	Ответственный и срок выполнения	Действие выполнено	Новый S	Новый O	Новый D	Новый RPN
Маркировка	Размытость	Расшифровка печати не может быть выполнена	8	Лазерное управление не применимо	2	Визуальная проверка в начале работы — цикл проверки каждый лист/лот	2	32	Отсутствует						
	Сдвиги, смещение	Плохой внешний вид	8	Смещение положения	2	Тестовая маркировка каждого первого листа/партии	1	16	Отсутствует						
	Противоположное направление	Плохой внешний вид	8	Продукт установлен в противоположном направлении	2	Направление продукта оценивается по общей частоте распознавания изображений	1	16	Отсутствует						
Поломка	Преграда и черпание	Плохой размер продукта	8	Зазор при установке подложки на эксклюзивный инструмент слишком велик	4	Содержание эксклюзивного инструмента самоконтроля	2	64	Введение нового очистителя, проверенного при вводе в эксплуатацию	Производственная технология произведена 31 января 2003 г.	Введение нового очистителя, проверенного при введении. Проверка размера продукта. Cpk: 2,58	7	2	2	28
	Внешний вид продукта становится больше	Плохой размер продукта	8	Шлифовальный круг изношен	4	Измерение размера в выборке Цикл отбора проб: 4 шт. Каждые пять листов	2	64	Введение нового очистителя, проверенного при вводе в эксплуатацию	Производственная технология произведена 31 января 2003 г.	Введение нового очистителя, проверенного при введении	7	2	2	28
Удаление неровностей	Заграждение (преграда) не снято	Плохой размер продукта	8	Зажимное приспособление не выдерживает тряски	1	Самопроверка	2	16	Отсутствует						

Обозначение
S = значимость, O = возникновение, D = обнаруживаемость

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ISO 13849-1—2014	IDT	ISO 13849-1:2006 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования»
ГОСТ 27.002—2015	NEQ	IEC 60050-192:2015 «Международный электротехнический словарь. Часть 192. Надежность»
ГОСТ Р 22.0.12—2015/ ИСО 22300:2012	IDT	ISO 22300:2012 «Социальная безопасность. Терминология»
ГОСТ Р 27.302—2009	NEQ	IEC 61025:2006 «Анализ дерева неисправностей»
ГОСТ Р 27.606—2013	NEQ	IEC 60300-3-11:2009 «Управление надежностью. Техническое обслуживание, ориентированное на безотказность»
ГОСТ Р 55.0.01—2014/ ИСО 55000:2014	IDT	ISO 55000:2014 «Управления активами. Общее представление, принципы и терминология»
ГОСТ Р 51897—2011/ Руководство ИСО 73:2009	IDT	ISO Guide 73:2009 «Менеджмент риска. Словарь. Руководство по использованию в стандартах»
ГОСТ Р 51901.14—2007 (МЭК 61078:2006)	MOD	IEC 61078:2006 «Методы анализа надежности систем. Структурная схема надежности и булевы методы»
ГОСТ Р 57273—2016 (CWA 16768:2014)	NEQ	CWA 16768:2014 «Структура создания ценности устойчивого развития в производственных сетях»
ГОСТ Р ИСО 31000—2019	IDT	ISO 31000:2018 «Менеджмент риска. Принципы и руководство»
ГОСТ Р ИСО/МЭК 31010—2011	IDT	IEC 31010:2009 «Менеджмент риска. Методы оценки риска»
ГОСТ Р 27.013—2019 (МЭК 62308:2006)	MOD	IEC 62308:2006 «Безотказность оборудования. Методы оценки безотказности»
ГОСТ Р МЭК 61165—2019	IDT	IEC 61165:2006 «Применение марковских методов»
ГОСТ Р МЭК 61508-1—2012	IDT	IEC 61508-1:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
ГОСТ Р МЭК 61508-2—2012	IDT	IEC 61508-2:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
ГОСТ Р МЭК 61508-3—2012	IDT	IEC 61508-3:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
ГОСТ Р МЭК 61508-4—2012	IDT	IEC 61508-4:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»

Окончание таблицы ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р МЭК 61508-5—2012	IDT	IEC 61508-5:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»
ГОСТ Р МЭК 61508-6—2012	IDT	IEC 61508-6:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3»
ГОСТ Р МЭК 61508-7—2012	IDT	IEC 61508-7:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»
ГОСТ Р МЭК 62061—2013	IDT	IEC 62061:2005 «Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью»
ГОСТ Р МЭК 62502—2014	IDT	IEC 62502:2010 «Аналитические методы надежности. Анализ дерева событий (ETA)»
ГОСТ Р МЭК 62508—2014	IDT	IEC 62508:2010 «Анализ влияния на надежность человеческого фактора»

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты;
- NEQ — неэквивалентные стандарты.

Библиография

[1] *МЭК 60050-192 Международный электротехнический словарь. Часть 192. Надежность (Dependability management — Part 192: Guidance for management and application)*

[2] ISO/IEC/IEE 15288:2015 Разработка систем и программного обеспечения. Процессы жизненного цикла системы (Systems and software engineering — System life cycle processes)

[3] EH 13306:2010 Техническое обслуживание и ремонт. Терминология технического обслуживания и ремонта (Maintenance — Maintenance terminology)

[4] МЭК 62740 Анализ коренных причин (RCA) (Root cause analysis (RCA))

[5] MIL-HDBK-338B, Electronic reliability design handbook, Defense Quality and Standardization Office (DLSC-LM), Fort Belvoir, Virginia 22060-6221, October 1998

[6] Bell, J., and Holroyd, J., Review of human reliability assessment methods, Research Report RR 679 for Health and Safety Executive, Sudbury: HSE Books, 2009

[7] МЭК 61709 Компоненты электрические. Надежность. Стандартные условия для интенсивностей отказов и модели напряжений для преобразования (Electric components — Reliability — Reference conditions for failure rates and stress models for conversion)

[8] МЭК 62741 Демонстрация требований к надежности. Пример надежности (Demonstration of dependability requirements — The dependability case)

[9] Braband, J., Improving the Risk Priority Number concept, Journal of System Safety, 3, 2003, p. 21—23

[10] МЭК 62551 Методы анализа надежности. Метод сети Петри (Analysis techniques for dependability — Petri net techniques)

[11] Ozarin, N., Understanding, planning and performing Failure Modes & Effects Analysis on software, Tutorial, RAMS Conference, 2016

[12] Yoshimura, I., Sato, Y., Safety achieved by the Safe Failure Fraction (SFF) in IEC 61508, IEEE Transactions on Reliability, Vol. 57, No. 4, 662—669, Dec. 2008

УДК 62-192:658.51.011:658.562:623:006.354 ОКС 03.120.01, 03.120.30, 21.020

Ключевые слова: отказ, вид отказа, последствия отказа, критичность отказа, вероятность отказа, анализ видов и последствий отказов; анализ видов, последствий и критичности отказов

Редактор *В.Н. Шмельков*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 22.09.2021. Подписано в печать 17.10.2021. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 7,91. Уч.-изд. л. 7,15. Тираж 40 экз. Зак. 1337.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано в ФГБУ «РСТ»
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru