ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 51901.12— 2007 (МЭК 60812:2006)

Менеджмент риска

МЕТОД АНАЛИЗА ВИДОВ И ПОСЛЕДСТВИЙ ОТКАЗОВ

IEC 60812:2006
Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)
(MOD)

Издание официальное

БЗ 9—2007/288

Москва
Стандартинформ
2008

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН Открытым акционерным обществом «Научно-исследовательский центр контроля и диагностики технических систем» (ОАО «НИЦ КД») и Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков» на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Управлением развития, информационного обеспечения и аккредитации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. № 572-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту МЭК 60812:2006 «Методы анализа надежности систем. Метод анализа видов и последствий отказов (FMEA)»(IEC 60812:2006 «Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)») путем внесения технических отклонений, объяснение которых приведено во введении к настоящему стандарту.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2004 (подраздел 3.5)

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2008

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 и определения 2
4 Основные положения 2
5 Анализ видов и последствий отказов 5
6 Другие исследования 20
7 Применения 21
Приложение А (справочное) Краткое описание процедур FMEA и FMECA 25
Приложение В (справочное) Примеры исследований 28
Приложение С (справочное) Перечень сокращений на английском языке, используемых в стандарте . 35
Библиография 35

Введение

В отличие от применяемого международного стандарта в настоящий стандарт не включены ссылки на МЭК 60050-191:1990 «Международный электротехнический словарь. Глава 191. Надежность и качество услуг», которые нецелесообразно приводить в национальном стандарте из-за отсутствия принятого гармонизированного национального стандарта. В соответствии с этим изменено содержание раздела 3. Кроме того, в стандарт включено дополнительное приложение С, содержащее перечень используемых сокращений на английском языке. Ссылки на национальные стандарты и дополнительное приложение С выделены курсивом.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

МЕТОД АНАЛИЗА ВИДОВ И ПОСЛЕДСТВИЙ ОТКАЗОВ

Risk management. Procedure for failure mode and effects analysis

Дата введения — 2008—09—01

1 Область применения

Настоящий стандарт устанавливает методы анализа видов и последствий отказов (Failure Mode and Effects Analysis — FMEA), видов, последствий и критичности отказов (Failure Mode, Effects and Criticality Analysis — FMECA) и дает рекомендации по их применению для достижения поставленных целей путем:

- выполнения необходимых этапов анализа;
- идентификации соответствующих терминов, предположений, показателей критичности, видов отказов;
- определения основных принципов анализа;
- использования примеров необходимых технологических карт или других табличных форм.

Все приведенные в настоящем стандарте общие требования FMEA относятся и к FMECA, так как последний является расширением FMEA.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 51901.3—2007 (МЭК 60300-2:2004) Менеджмент риска. Руководство по менеджменту надежности (МЭК 60300-2:2004 «Менеджмент надежности. Руководство по менеджменту надежности», MOD)

ГОСТ Р 51901.5—2005 (МЭК 60300-3-1:2003) Менеджмент риска. Руководство по применению методов анализа надежности (МЭК 60300-3-1:2003 «Управление надежностью. Часть 3-1. Руководство по применению. Методы анализа надежности. Руководство по методологии», MOD)

ГОСТ Р 51901.13—2005 (МЭК 61025:1990) Менеджмент риска. Анализ дерева неисправностей (МЭК 61025:1990 «Анализ дерева неисправности (FNA)», MOD)

ГОСТ Р 51901.14—2005 (МЭК 61078:1991) Менеджмент риска. Метод структурной схемы надежности (МЭК 61078:2006 «Методы анализа надежности. Структурная схема надежности и Булевы методы», MOD)

ГОСТ Р 51901.15—2005 (МЭК 61165:1995) Менеджмент риска. Применение марковских методов (МЭК 61165:1995 «Применение марковских методов», MOD)

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 ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **объект** (item): Любая часть, элемент, устройство, подсистема, функциональная единица, аппаратура или система, которую можно рассматривать самостоятельно.

Примечания

1 Объект может состоять из технических средств, программных средств или их сочетания и может также, в частных случаях, включать в себя технический персонал.

2 Ряд объектов, например их совокупность или выборка, может быть рассмотрен как объект.

3 Процесс также может быть рассмотрен как объект, который выполняет заданную функцию и для которого проводят FMEA или FMECA. Обычно FMEA аппаратных средств не распространяется на людей и их взаимодействие с аппаратными средствами или программным обеспечением, в то время как FMEA процесса обычно включает в себя анализ действий людей.

3.2 **отказ** (failure): Утрата объектом способности выполнять требуемую функцию[1)].

3.3 **неисправность** (fault): Состояние объекта, при котором он не способен выполнять требуемую функцию, за исключением такой неспособности при техническом обслуживании или других плановых мероприятиях или вследствие нехватки внешних ресурсов.

Примечания

1 Неисправность часто является следствием отказа объекта, но может иметь место и без него.

2 В настоящем стандарте термин «неисправность» используется наряду с термином «отказ» по историческим причинам.

3.4 **последствие отказа** (failure effect): Следствие вида отказа для эксплуатации, функционирования или статуса объекта.

3.5 **вид отказа** (failure mode): Способ и характер возникновения отказа объекта.

3.6 **критичность отказа** (failure criticality): Сочетание тяжести последствий и частоты появления или других свойств отказа как характеристика необходимости идентификации источников, причин и сокращения частоты или количества появлений данного отказа и уменьшения тяжести его последствий.

3.7 **система** (system): Совокупность взаимосвязанных или взаимодействующих элементов.

Примечания

1 Применительно к надежности система должна иметь:

a) определенные цели, представленные в виде требований к ее функциям;

b) установленные условия функционирования;

c) определенные границы.

2 Структура системы является иерархической.

3.8 **тяжесть отказа** (failure severity): Значимость или серьезность последствий вида отказа для обеспечения функционирования объекта, окружающей среды и оператора, связанная с установленными границами исследуемого объекта.

4 Основные положения

4.1 Введение

Анализ видов и последствий отказов (FMEA) является методом систематического анализа системы для идентификации видов потенциальных отказов, их причин и последствий, а также влияния отказов на функционирование системы (системы в целом или ее компонентов и процессов). Термин «система» использован для описания аппаратных средств, программного обеспечения (с их взаимодействием) или процесса. Рекомендуется проводить анализ на ранних стадиях разработки, когда устранение или сокращение последствий и количества видов отказов является экономически наиболее эффективным. Анализ может быть начат, как только система может быть представлена в виде функциональной блок-схемы с указанием ее элементов.

[1)] *Более детально см.* [1].

Выбор времени проведения FMEA очень важен. Если анализ был выполнен на достаточно ранних этапах разработки системы, то введение изменений при проектировании для исключения недостатков, обнаруженных при проведении FMEA, является экономически более эффективным. Поэтому важно, чтобы цели и задачи FMEA были описаны в плане и графике процесса разработки. Таким образом, FMEA является итеративным процессом, выполняемым одновременно с процессом проектирования.

FMEA применим на различных уровнях декомпозиции системы — от самого высокого уровня системы (системы в целом) до функций отдельных компонентов или команд программного обеспечения. FMEA постоянно повторяют и обновляют, поскольку при разработке совершенствуется и изменяется конструкция системы. Изменения конструкции требуют внесения изменений в соответствующие части FMEA.

В целом FMEA является результатом работы команды, состоящей из квалифицированных специалистов, способных признать и оценить значимость и последствия различных типов потенциальных несоответствий конструкции и процессов, которые могут привести к отказам продукции. Работа в команде стимулирует процесс мышления и гарантирует необходимое качество экспертизы.

FMEA представляет собой метод, позволяющий идентифицировать тяжесть последствий видов потенциальных отказов, и обеспечить меры по снижению риска. В некоторых случаях FMEA также включает в себя оценку вероятности возникновения видов отказов. Это расширяет анализ.

До применения FMEA необходимо провести иерархическую декомпозицию системы (аппаратных средств с программным обеспечением или процесса) на основные элементы. Полезно использовать простые блок-схемы, иллюстрирующие декомпозицию (см. *ГОСТ Р 51901.14*). Анализ при этом начинают с элементов самого нижнего уровня системы. Последствие отказа на нижнем уровне может стать причиной отказа объекта на более высоком уровне. Анализ проводят снизу вверх по восходящей схеме, пока не будут определены конечные последствия для системы в целом. Такой процесс показан на рисунке 1.

FMECA (анализ видов, последствий и критичности отказов) расширяет FMEA и включает в себя методы ранжирования тяжести видов отказов, позволяет установить приоритетность контрмер. Сочетание тяжести последствий и частоты возникновения отказов является мерой, называемой критичностью.

Принципы FMEA могут быть применены вне разработки проекта на всех стадиях жизненного цикла продукции. Метод FMEA может быть применен к производству или другому процессу, например в больницах, медицинских лабораториях, системах образования и др. При применении FMEA к производственному процессу эту процедуру называют FMEA процесса [Process Failure Mode and Effects Analysis (PFMEA)]. Для эффективного применения FMEA важным условием работы является обеспечение адекватными ресурсами. Полное понимание системы для предварительного FMEA необязательно, однако по мере разработки проекта для детального анализа видов и последствий отказов необходимо полное знание характеристик и требований, предъявляемых к проектируемой системе. Сложные технические системы обычно требуют применения анализа к большому числу факторов проекта (механика, электротехника, системное проектирование, разработка программного обеспечения, средства технического обслуживания и т. д.).

В общем случае FMEA применяют к отдельным видам отказов и их последствиям для системы в целом. Каждый вид отказа рассматривают как независимый. Таким образом, эта процедура не подходит для рассмотрения зависимых отказов или отказов, являющихся следствием последовательности нескольких событий. Для анализа таких ситуаций необходимо применять другие методы, такие как марковский анализ (см. *ГОСТ Р 51901.15*) или анализ дерева неисправностей (см. *ГОСТ Р 51901.13*).

При определении последствий отказа необходимо рассмотреть отказы более высокого уровня и отказы того же уровня, возникшие в результате произошедшего отказа. Анализ должен выявить все возможные комбинации видов отказов и их последовательностей, которые могут быть причиной последствий видов отказа на более высоком уровне. В этом случае необходимо дополнительное моделирование для оценки тяжести или вероятности возникновения таких последствий.

FMEA является гибким инструментом, который можно адаптировать к особенностям требований конкретного производства. В некоторых случаях требуется разработка специализированных форм и правил ведения записей. Уровни тяжести видов отказов (в случаях их применения) для различных систем или различных уровней системы могут быть определены по-разному.

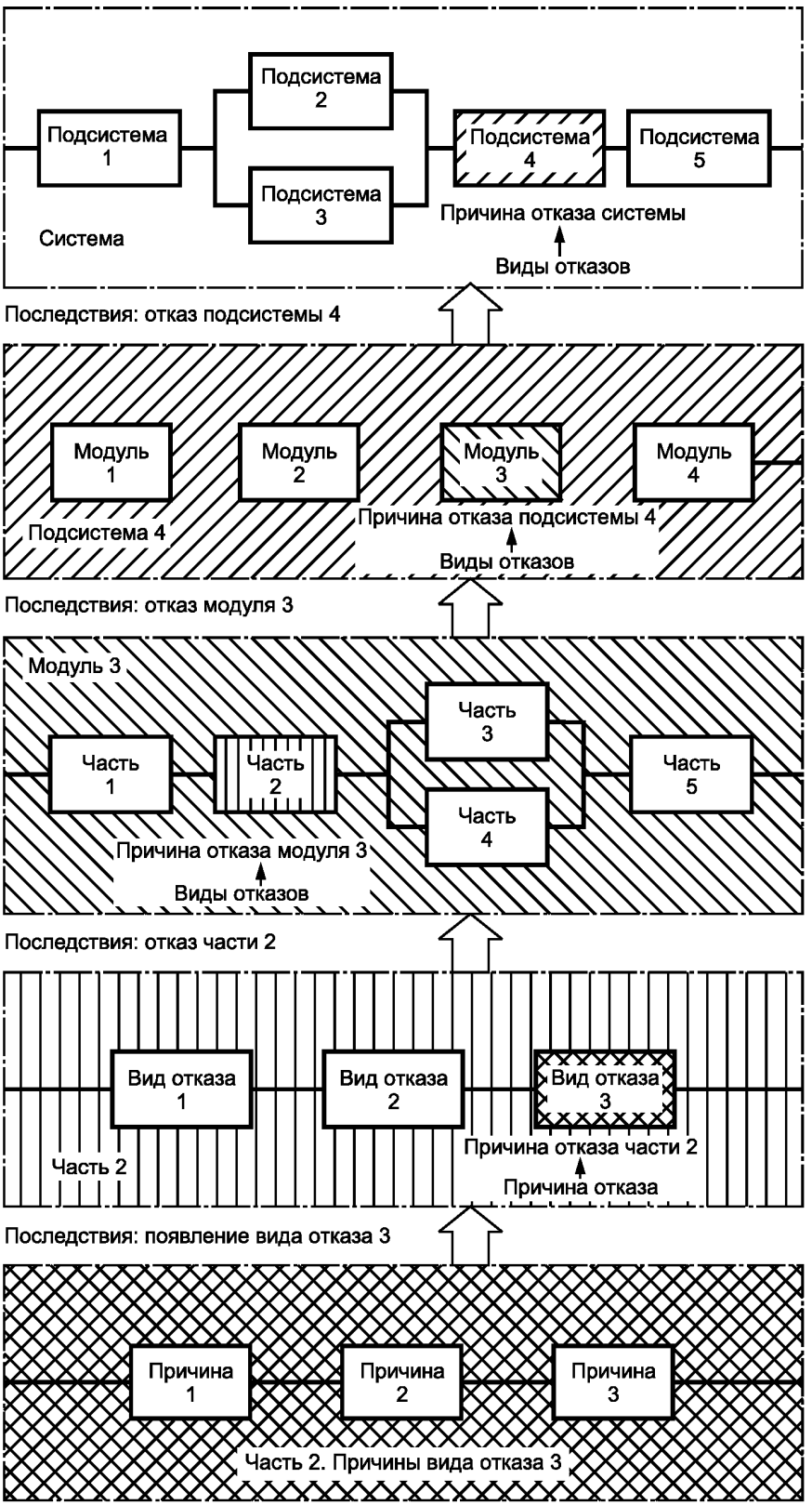

Рисунок 1 — Взаимосвязь видов и последствий отказов в иерархической структуре системы

4.2 Цели и задачи анализа

Основаниями для применения анализа видов и последствий отказов (FMEA) или анализа видов, последствий и критичности отказов (FMECA) могут быть следующие:

a) идентификация отказов, которые имеют нежелательные последствия для функционирования системы, например прекращение или значительное ухудшение работы или влияние на безопасность пользователя;

b) выполнение требований заказчика, установленных в контракте;

c) повышение надежности или безопасности системы (например, путем изменения проекта или проведения действий по обеспечению качества);

d) повышение ремонтопригодности системы путем выявления областей риска или несоответствий применительно к ремонтопригодности.

В соответствии с вышеизложенным целями FMEA (или FMECA) могут быть следующие:

a) полная идентификация и оценка всех нежелательных последствий в пределах установленных границ системы и последовательностей событий, вызванных каждым идентифицированным видом отказа общей причины на различных уровнях функциональной структуры системы;

b) определение критичности (см. раздел 6) или приоритетности для диагностики и снижения негативных последствий отказов каждого вида, влияющих на правильность функционирования и параметры системы или соответствующего процесса;

c) классификация идентифицированных видов отказов в соответствии с такими характеристиками, как легкость обнаружения, возможность диагностирования, контролепригодность, условия эксплуатации и ремонта (ремонт, эксплуатация, логистика и т. д.);

d) идентификация функциональных отказов системы и оценка тяжести последствий и вероятности возникновения отказа;

e) разработка плана улучшения проекта путем сокращения количества и последствий видов отказов;

f) разработка плана эффективного технического обслуживания для снижения вероятности возникновения отказов (см. МЭК 60300-3-11 [2]).

Примечание — При работе с критичностью и вероятностью появления отказов рекомендуется применять методологию FMECA.

5 Анализ видов и последствий отказов

5.1 Основные положения

Традиционно существуют достаточно большие различия в способах проведения и представления FMEA. Обычно анализ выполняют, идентифицируя виды отказов, соответствующие причины, непосредственные и итоговые последствия. Аналитические результаты могут быть представлены в виде рабочей таблицы, содержащей наиболее существенную информацию о системе в целом и деталях, учитывающих ее особенности, в частности о путях потенциальных отказов системы, компонентов и видах отказов, которые могут быть причиной отказа системы, а также причинах возникновения каждого вида отказа.

Применение FMEA к сложной продукции связано с большими трудностями. Этих трудностей может быть меньше, если некоторые подсистемы или части системы не являются новыми и совпадают с подсистемами и частями предыдущей конструкции системы или являются их модификацией. Вновь создаваемый FMEA должен использовать информацию о существующих подсистемах в максимально возможной степени. Он должен также указывать на необходимость испытаний или полного анализа новых свойств и объектов. Как только разработан детальный FMEA для некоторой системы, он может быть обновлен и улучшен для последующих модификаций системы, что потребует значительно меньше усилий, чем новая разработка FMEA.

Используя существующий FMEA предыдущей версии продукции, необходимо удостовериться, что конструкция (проект) повторно используется тем же способом и с теми же нагрузками, что и предыдущая. Новые нагрузки или воздействия окружающей среды при эксплуатации могут потребовать до выполнения FMEA проведения предварительного анализа имеющегося FMEA. Различия во внешних условиях и эксплуатационных нагрузках могут потребовать создания нового FMEA.

Процедура FMEA состоит из следующих основных четырех этапов:

a) установления основных правил планирования и разработки графика выполнения работ FMEA (в том числе распределения времени и обеспечения доступности экспертизы для выполнения анализа);

b) выполнения FMEA с использованием соответствующих рабочих таблиц или других форм, таких как логические схемы или деревья неисправностей;

c) подведения итогов и составления отчета о результатах анализа, включающего в себя все выводы и рекомендации;

d) обновления FMEA по мере продвижения разработки и развития проекта.

5.2 Предварительные задачи

5.2.1 Планирование анализа

Деятельность при выполнении FMEA, включая действия, процедуры, взаимодействия с процессами в сфере надежности, действия по управлению корректирующими действиями, а также сроки завершения этих действий и их этапов, должны быть указаны в общем плане программы надежности[1)].

План программы надежности должен описывать используемые методы FMEA. Описание методов может быть самостоятельным документом или может быть заменено ссылкой на документ, содержащий это описание.

План программы надежности должен содержать следующие сведения:

- определение цели анализа и ожидаемых результатов;
- область применения анализа с указанием, каким элементам конструкции FMEA должен уделять особое внимание. Область применения должна соответствовать зрелости проекта и охватывать элементы конструкции, которые могут быть источником риска, поскольку выполняют критическую функцию или изготовлены по неотработанной или новой технологии;
- описание того, как представленный анализ способствует обеспечению общей надежности системы;
- идентифицированные действия по управлению пересмотрами FMEA и соответствующей документацией. Управление пересмотрами документов анализа, рабочих таблиц и методами их хранения должно быть определено;
- необходимый объем участия в анализе экспертов по разработке проекта;
- четкое указание ключевых стадий в графике выполнения проекта для своевременного проведения анализа;
- способ завершения всех действий, указанных в процессе сокращения идентифицированных видов отказов, которые необходимо рассмотреть.

План должен быть согласован всеми участниками проекта и одобрен его руководством. В заключительном анализе FMEA на завершающей стадии проектирования продукции или ее производственного процесса (FMEA процесса) должны быть указаны все зарегистрированные действия для устранения или сокращения количества и снижения тяжести последствий установленных видов отказов, а также способ осуществления таких действий.

5.2.2 Структура системы

5.2.2.1 Информация о структуре системы

Информация о структуре системы должна включать в себя следующие данные:

a) описание элементов системы с их характеристиками, параметрами эксплуатации, функциями;

b) описание логических связей между элементами;

c) степень и характер резервирования;

d) положение и значимость системы в рамках устройства в целом (если это имеет место);

e) входы и выходы системы;

f) замены в структуре системы для измерения режимов эксплуатации.

Для всех уровней системы необходима информация о функциях, характеристиках и параметрах. Уровни системы рассматривают снизу вверх до самого высокого уровня, исследуя с помощью FMEA виды отказов, которые нарушают каждую из функций системы.

5.2.2.2 Определение границ системы для анализа

Границы системы включают в себя физический и функциональный интерфейсы между системой и ее средой, в том числе другие системы, с которыми взаимодействует исследуемая система. Определение границ системы для анализа должно соответствовать границам системы, установленным для проектирования и технического обслуживания, и относиться к любому уровню системы. Системы и/или компоненты, выходящие за границы, должны быть четко определены и исключены.

Определение границ системы в большей степени зависит от ее конструкции, предназначенного использования, источников поставок или коммерческих критериев, чем от оптимальных требований FMEA. Однако, по возможности, при определении границ необходимо учитывать требования, позволяющие упростить FMEA и его интеграцию с другими связанными исследованиями. Это особенно важно,

---

[1)] Более детально об элементах программы надежности и плане надежности см. *ГОСТ Р 51901.3.*

если система является функционально сложной, с многочисленными взаимосвязями между объектами внутри и вне границ. В таких случаях полезно определять границы исследований на основе функций системы, а не аппаратных средств и программного обеспечения. Это позволит ограничить количество входов и выходов на другие системы и может уменьшить количество и снизить тяжесть последствий отказов системы.

Необходимо четко установить, что все системы или компоненты вне границ исследуемой системы рассмотрены и исключены из анализа.

5.2.2.3 Уровни анализа

Важно определить уровень системы, который будет использован для анализа. Например, в системе могут возникнуть нарушения ее функций или отказы подсистем, сменных элементов или уникальных компонентов (см. рисунок 1). Основные правила выбора уровней системы для анализа зависят от желаемых результатов и доступности необходимой информации. Полезно использовать следующие основные принципы:

a) высший уровень системы выбирают исходя из концепции проекта и установленных требований к выходам;

b) самый нижний уровень системы, на котором анализ является эффективным, — это уровень, характеризующийся наличием доступной информации для определения и описания его функций. Выбор соответствующего уровня системы зависит от предыдущего опыта. Для системы, основанной на зрелом проекте с зафиксированными и высокими уровнями надежности, ремонтопригодности и безопасности, применяют менее детальный анализ. Более детальную проработку и соответственно более низкие уровни системы вводят для недавно разработанной системы или системы с неизвестной хронологией надежности;

c) установленный или предполагаемый уровень технического обслуживания и ремонта является ценным руководством при определении более низких уровней системы.

При проведении FMEA определение видов, причин и последствий отказов зависит от уровня анализа и критериев отказа системы. В процессе анализа последствия отказа, идентифицированного на более низком уровне, могут стать видами отказов для более высокого уровня системы. Виды отказов на более низком уровне системы могут стать причинами отказов на более высоком уровне системы и так далее.

При декомпозиции системы до ее элементов последствия одной или более причины вида отказов создают вид отказа, который в свою очередь является причиной отказов составной части. Отказ составной части является причиной отказа модуля, который в свою очередь является причиной отказа подсистемы. Воздействие причины отказа на одном уровне системы, таким образом, становится причиной воздействия на более высоком уровне. Приведенное объяснение показано на рисунке 1.

5.2.2.4 Представление структуры системы

Символическое представление структуры функционирования системы, особенно в виде схемы, очень полезно при проведении анализа.

Необходимо разработать простые схемы, отражающие основные функции системы. В схеме линии соединения блоков представляют собой входы и выходы для каждой функции. Характер каждой функции и каждого входа должен быть точно описан. Для описания различных фаз эксплуатации системы может потребоваться несколько схем.

В соответствии с продвижением проектирования системы может быть разработана схема с блоками, представляющими реальные компоненты или составные части. Такое представление дает дополнительную информацию для более точной идентификации потенциальных видов отказов и их причин.

Блок-схемы должны отражать все элементы, их отношения, резервирование и функциональные взаимосвязи между ними. Это обеспечивает прослеживаемость функциональных отказов системы. Для описания альтернативных режимов эксплуатации системы может потребоваться несколько блок-схем. Могут потребоваться отдельные схемы для каждого режима эксплуатации. Как минимум, каждая блок-схема должна содержать:

a) декомпозицию системы на основные подсистемы, включая их функциональные взаимосвязи;

b) все соответственно отмеченные входы и выходы и идентификационные номера каждой подсистемы;

c) все резервирования, предупреждающую сигнализацию и другие технические особенности, которые обеспечивают защиту системы от отказов.

5.2.2.5 Пуск, эксплуатация, управление и техническое обслуживание

Статус различных режимов эксплуатации системы, а также изменения конфигурации или положения системы и ее компонентов в течение различных стадий эксплуатации должны быть определены. Минимальные требования к функционированию системы должны быть определены так, чтобы критерии

отказа и/или работоспособности были четкими и понятными. Требования к готовности или безопасности следует устанавливать на основе заданных минимальных уровней функционирования, необходимых для работы, и максимальных уровней повреждения, допускающих приемку. Необходимо иметь точную информацию:

a) о продолжительности каждой функции, выполняемой системой;

b) об интервале времени между периодическими испытаниями;

c) о времени выполнения корректирующих действий до появления серьезных последствий для системы;

d) о всех используемых средствах, условиях окружающей среды и/или персонале, включая интерфейсы и взаимодействия с операторами;

e) о рабочих процессах при запуске системы, отключении и других переходах (ремонте);

f) об управлении в процессе стадий эксплуатации;

g) о профилактическом и/или корректирующем техническом обслуживании;

h) о процедурах испытаний, если их проводят.

Установлено, что одним из важных применений FMEA является помощь в разработке стратегии технического обслуживания. Информация о средствах, оборудовании, запасных частях для технического обслуживания должна быть известна также для предупреждающего и корректирующего технического обслуживания.

5.2.2.6 Окружающая среда системы

Условия окружающей среды системы должны быть определены, включая внешние условия и условия, созданные другими находящимися рядом системами. Для системы должны быть описаны ее отношения, взаимозависимости или взаимосвязи со вспомогательными или другими системами и интерфейсами и с персоналом.

На стадии проектирования не все эти данные известны, и поэтому должны быть использованы приближения и предположения. По мере продвижения проекта и увеличения данных для учета новой информации или измененных предположений и приближений необходимо выполнять изменения FMEA. Часто FMEA применяют для определения необходимых условий.

5.2.3 Определение видов отказов

Успешное функционирование системы зависит от функционирования критических элементов системы. Для оценки функционирования системы необходимо идентифицировать ее критические элементы. Эффективность процедур идентификации видов отказов, их причин и последствий может быть повышена с помощью подготовки списка ожидаемых видов отказов на основе следующих данных:

a) назначения системы;

b) особенностей элементов системы;

c) режима работы системы;

d) требований к эксплуатации;

e) ограничений по времени;

f) воздействий окружающей среды;

g) рабочих нагрузок.

Пример списка общих видов отказов приведен в таблице 1.

Таблица 1 — Пример общих видов отказов

Номер вида отказа	Наименование вида отказа
1	Отказ в процессе функционирования
2	Отказ, связанный с несрабатыванием в установленное время
3	Отказ, связанный с непрекращением работы в установленное время
4	Преждевременное включение

Примечание — Этот список является только примером. Различным типам систем соответствуют различные списки.

Фактически каждый вид отказов можно отнести к одному или нескольким из указанных общих видов. Однако эти общие виды отказов имеют слишком широкую область анализа. Следовательно, список необходимо расширить, чтобы сузить группу отказов, отнесенную к исследуемому общему виду отказов. Требования к параметрам управления входами и выходами, а также потенциальные виды отказов

должны быть идентифицированы и описаны на структурной схеме надежности объекта. Необходимо отметить, что один вид отказов может иметь несколько причин.

Важно, чтобы оценка всех объектов в пределах границ системы на самом нижнем уровне для идентификации всех потенциальных видов отказов была согласована с целями анализа. Затем проводят исследования, позволяющие определить возможные отказы, а также последствия отказов для подсистем и функций системы.

Поставщики комплектующих должны идентифицировать потенциальные виды отказов для своей продукции. Обычно данные о видах отказов могут быть получены из следующих источников:

a) для новых объектов могут быть использованы данные других объектов с аналогичными функцией и структурой, а также результаты испытаний этих объектов с соответствующими нагрузками;

b) для новых объектов потенциальные виды отказов и их причины определяют в соответствии с целями проектирования и детальным анализом функций объекта. Этот метод предпочтительнее приведенного в перечислении a), поскольку нагрузки и непосредственно функционирование могут различаться для аналогичных объектов. Примером такой ситуации может быть использование FMEA для обработки сигналов процессора, отличного от такого же процессора, используемого в аналогичном проекте;

c) для объектов в эксплуатации могут быть использованы данные отчетов, относящихся к обслуживанию и отказам;

d) потенциальные виды отказов могут быть определены на основе анализа функциональных и физических параметров, характерных для работы объекта.

Важно, чтобы виды отказов не были пропущены из-за отсутствия данных, а начальные оценки были улучшены на основе результатов испытаний и данных продвижения проекта. В соответствии с FMEA необходимо вести записи статуса таких оценок.

Идентификация видов отказов и, при необходимости, определение корректирующих действий проекта, предупреждающих действий для обеспечения качества или действий по техническому обслуживанию продукции имеют главное значение. Более важно идентифицировать и, по возможности, смягчить последствия видов отказов мерами проектирования, чем знать вероятность их появления. Если трудно назначить приоритеты, можно потребовать проведения анализа критичности.

5.2.4 Причины отказов

Наиболее вероятные причины каждого потенциального вида отказов должны быть идентифицированы и описаны. Так как вид отказов может иметь несколько причин, наиболее вероятные независимые причины каждого вида отказов должны быть идентифицированы и описаны.

Идентификация и описание причин отказов не всегда необходимы для всех видов отказов, идентифицированных при проведении анализа. Идентификация и описание причин отказов и предложений по их устранению должны быть выполнены на основе изучения последствий отказов и их тяжести. Чем тяжелее последствия вида отказов, тем более точно должны быть идентифицированы и описаны причины отказов. В противном случае аналитик может потратить ненужные усилия на идентификацию причин таких видов отказов, которые не влияют на функционирование системы или имеют очень незначительные последствия.

Причины отказов могут быть определены на основе анализа эксплуатационных отказов или отказов в процессе испытаний. Если проект является новым и не имеет прецедентов, причины отказов могут быть установлены экспертными методами.

После идентификации причин видов отказов на основе оценок их появления и тяжести последствий оценивают рекомендованные действия.

5.2.5 Последствия отказа

5.2.5.1 Определение последствий отказа

Последствие отказа является результатом действия вида отказов в терминах эксплуатации, функционирования или статуса системы (см. определение 3.4). Последствие отказа может быть вызвано одним или несколькими видами отказов одного или нескольких объектов.

Последствия каждого вида отказов для функционирования элементов, функции или статуса системы должны быть идентифицированы, оценены и зарегистрированы. Действия технического обслуживания и цели системы также должны быть рассмотрены всякий раз, когда это необходимо. Последствия отказа могут воздействовать на следующий и, в конечном счете, на высший уровень анализа системы. Поэтому на каждом уровне последствия отказов должны быть оценены для следующего, более высокого уровня.

5.2.5.2 Локальные последствия отказа

Выражение «локальные последствия» относится к последствиям вида отказа для рассматриваемого элемента системы. Последствия каждого возможного отказа на выходе объекта должны быть опи-

саны. Цель идентификации локальных последствий состоит в обеспечении оснований для оценки существующих альтернативных условий или разработки рекомендуемых корректирующих действий. В некоторых случаях может не быть локальных последствий, кроме самого отказа.

5.2.5.3 Последствия отказа на уровне системы

При идентификации последствий для системы в целом последствия возможного отказа для высшего уровня системы определяют и оценивают на основе анализа на всех промежуточных уровнях. Последствия высшего уровня могут быть результатом многократных отказов. Например, отказ устройства безопасности приводит к катастрофическим последствиям для системы в целом только в случае отказа устройства безопасности одновременно с выходом за допустимые пределы главной функции системы, для которой предназначено устройство безопасности. Эти последствия, являющиеся результатом многократных отказов, должны быть указаны в рабочих таблицах.

5.2.6 Методы обнаружения отказов

Для каждого вида отказа аналитик должен определить способ обнаружения отказа и средства, которые пользователь или специалист по техническому обслуживанию применяет для диагностики отказа. Диагностика отказов может быть выполнена с применением технических средств, может осуществляться автоматическими средствами, предусмотренными в конструкции (встроенное тестирование), а также путем введения специальной процедуры контроля до начала работы системы или при техническом обслуживании. Диагностика может быть проведена при запуске системы в процессе ее функционирования или через установленные интервалы времени. В любом случае после диагностики отказа должен быть устранен опасный режим эксплуатации.

Виды отказов, кроме рассматриваемого, которые имеют идентичное проявление, должны быть проанализированы и перечислены. Следует рассмотреть необходимость отдельной диагностики отказов резервных элементов в процессе работы системы.

Для FMEA конструкции при обнаружении отказов исследуют, с какой вероятностью, когда и где недостаток конструкции будет идентифицирован (с помощью анализа, моделирования, испытаний и т.д.). Для FMEA процесса при обнаружении отказов рассматривают, с какой вероятностью и где недостатки и несоответствия процесса могут быть идентифицированы (например, оператором при статистическом управлении процессом, в процессе контроля качества или на более поздних этапах процесса).

5.2.7 Условия компенсации отказа

Идентификация всех особенностей конструкции на данном уровне системы или других мер безопасности, которые могут предотвратить или уменьшить последствия видов отказа, является чрезвычайно важной. FMEA должен четко показать истинное действие этих мер безопасности в условиях конкретного вида отказа. Меры безопасности, препятствующие отказу, которые должны быть зарегистрированы в FMEA, включают в себя следующее:

a) резервированные объекты, которые допускают длительную работу, если один или несколько элементов отказали;

b) альтернативные средства работы;

c) мониторинг или сигнальные устройства;

d) любые другие методы и средства эффективной работы или ограничения ущерба.

В процессе проектирования функциональные элементы (аппаратные средства и программное обеспечение) могут быть неоднократно перестроены или переформированы, а также могут быть изменены их возможности. На каждой стадии необходимость анализа идентифицированных видов отказов и применения FMEA должна быть подтверждена или даже пересмотрена.

5.2.8 Классификация тяжести отказа

Тяжесть отказа является оценкой значимости влияния последствий вида отказа на функционирование объекта. Классификация тяжести отказа, зависящая от особенностей применения FMEA, разработана с учетом нескольких факторов:

- характеристики системы в соответствии с возможными отказами, особенностями пользователей или окружающей среды;
- функциональных параметров системы или процесса;
- любых требований заказчика, установленных в контракте;
- законодательных требований и требований безопасности;
- требований, связанных с гарантийными обязательствами.

В таблице 2 приведен пример качественной классификации тяжести последствий при выполнении одного из типов FMEA.

Таблица 2 — Иллюстративный пример классификации тяжести последствий отказа

Номер класса тяжести отказа	Наименование класса тяжести отказа	Описание последствия отказа для людей или окружающей среды
IV	Катастрофический	Вид отказа может привести к прекращению выполнения первичных функций системы и вызывает тяжелые повреждения системы и окружающей среды и/или гибель и тяжелые травмы людей
III	Критический	Вид отказа может привести к прекращению выполнения первичных функций системы и вызывает значительное повреждение системы и окружающей среды, но не представляет собой серьезной угрозы жизни или здоровью людей
II	Минимальный	Вид отказа может ухудшить выполнение функций системы без заметного повреждения системы или угрозы жизни или здоровью людей
I	Ничтожный	Вид отказа может ухудшить выполнение функций системы, но не вызывает повреждений системы и не создает угрозы жизни и здоровью людей

5.2.9 Частота или вероятность появления отказов

Частота или вероятность появления каждого вида отказа должна быть определена для оценки последствий или критичности отказов.

Для определения вероятности появления вида отказа, помимо опубликованной информации об интенсивности отказов, очень важно рассмотреть реальные условия функционирования каждого компонента (экологические, механические и/или электрические нагрузки), характеристики которого вносят свой вклад в вероятность появления отказа. Это необходимо, поскольку составляющие интенсивности отказов и, следовательно, интенсивность рассматриваемого вида отказа в большинстве случаев увеличиваются вместе с увеличением воздействующих нагрузок в соответствии со степенным или экспоненциальным законом. Вероятность появления видов отказов для системы можно оценивать с использованием:

- данных ресурсных испытаний;
- доступных баз данных об интенсивностях отказов;
- данных эксплуатационных отказов;
- данных об отказах аналогичных объектов или компонентов аналогичного класса.

Оценки вероятности появления отказа FMEA относят к определенному периоду времени. Обычно это гарантийный период или установленный срок службы объекта или продукции.

Применение частоты и вероятности появления отказа разъяснено ниже при описании анализа критичности.

5.2.10 Процедура анализа

Блок-схема, приведенная на рисунке 2, показывает общую процедуру анализа.

5.3 Анализ видов, последствий и критичности отказов (FMECA)

5.3.1 Цель анализа

Буква С, включенная в аббревиатуру FMEA, означает, что анализ вида отказов приводит также к анализу критичности. Определение критичности подразумевает использование качественной меры последствий видов отказа. Критичность имеет множество определений и способов измерения, большинству из которых присущ близкий смысл: воздействие или значимость вида отказа, который необходимо устранить или смягчить его последствия. Некоторые из этих способов измерения объяснены в 5.3.2 и 5.3.4. Цель анализа критичности состоит в качественном определении относительной величины каждого последствия отказа. Значения этой величины используют для установления приоритетности действий по устранению отказов или снижению их последствий на основе комбинаций критичности отказов и тяжести их последствий.

5.3.2 Риск *R* и значение приоритетности риска (*RPN*)

Одним из методов количественной оценки критичности является определение значения приоритетности риска [Risk Priority Number (*RPN*[1)])]. Риск в этом случае оценивают субъективной мерой тяжес-

[1)] Величина, характеризующая тяжесть последствий.

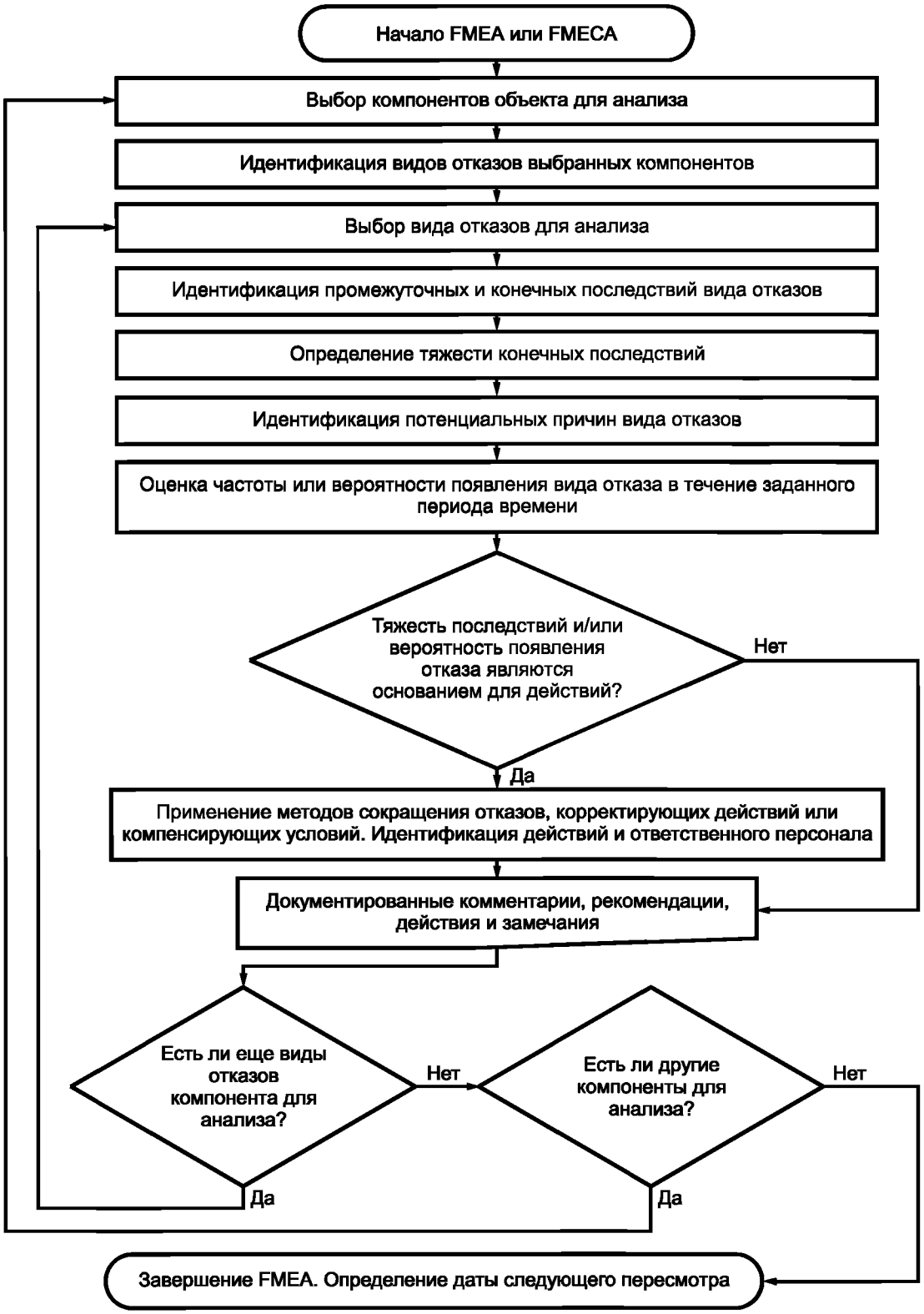

Рисунок 2 — Блок-схема анализа

ти последствий и вероятностью возникновения отказа в течение заданного периода времени (используемого для анализа). В некоторых случаях, когда этот способ неприменим, необходимо обратиться к более простой форме неколичественного FMEA.

В качестве общей меры потенциального риска R в некоторых типах FMECA используют величину

$$R = S\,P,$$

где S — значение тяжести последствий, т. е. степени влияния отказа на систему или пользователя (безразмерная величина);

P — вероятность появления отказа (безразмерная величина). Если она меньше 0,2, ее можно заменить значением критичности C, которое используют в некоторых количественных методах FMEA, описанных в 5.3.4 (оценка вероятности появления последствий отказа).

В некоторых применениях FMEA или FMECA дополнительно выделяют уровень обнаружения отказа для системы в целом. В этих случаях используют дополнительно значение обнаружения отказа D (также безразмерная величина) для формирования значения приоритетности риска RPN

$$RPN = SOD,$$

где O — вероятность появления отказа для заданного или установленного периода времени (эта величина может быть определена как ранг, а не фактическое значение вероятности появления отказа);

D — характеризует обнаружение отказа и представляет собой оценку шанса идентифицировать и устранить отказ до появления последствий для системы или заказчика. Значения D обычно ранжированы в обратном порядке по отношению к вероятности появления отказа или тяжести отказа. Чем выше значение D, тем менее вероятно обнаружение отказа. Более низкая вероятность обнаружения соответствует более высокому значению RPN и более высокой приоритетности вида отказа.

Значение приоритетности риска RPN можно использовать для установления приоритетов при сокращении видов отказа. Кроме значения приоритетности риска, для принятия решения о сокращении видов отказов учитывают, прежде всего, значение тяжести видов отказа, подразумевая, что при равных или близких значениях RPN в первую очередь это решение следует применять к видам отказов с более высокими значениями тяжести отказов.

Эти значения могут быть оценены в числовом виде с применением непрерывной или дискретной шкалы (конечное число заданных значений).

Затем виды отказов ранжируют в соответствии с их RPN. Высокий приоритет назначают для высоких значений RPN. В некоторых случаях последствия для видов отказов с RPN, превышающим установленный предел, являются неприемлемыми, в то время как в других случаях высокие значения тяжести отказа устанавливают независимо от значений RPN.

Различные типы FMECA используют различные шкалы значений для S, O и D, например от 1 до 4 или 5. Некоторые типы FMECA, например используемые в автомобильной промышленности для анализа конструкции и процесса производства, называемые DFMEA и PFMEA, назначают шкалу от 1 до 10.

5.3.3 Связь FMECA с анализом риска

Сочетание критичности и тяжести последствий характеризует риск, который отличается от обычно применяемых показателей риска меньшей строгостью и требует меньше усилий для оценки. Различия заключаются не только в способе прогноза тяжести последствий отказа, но также и в описании взаимодействий между вносящими вклад факторами с помощью обычной восходящей процедуры FMECA. Кроме того, FMECA обычно позволяет провести относительное ранжирование вкладов в совокупный риск, в то время как анализ риска для систем с высоким риском обычно ориентирован на приемлемый риск. Однако для систем с низким риском и низкой сложностью FMECA может быть экономически более эффективным и подходящим методом. Всякий раз, когда при выполнении FMECA обнаруживается вероятность последствий с высоким риском, более предпочтительным является использование вероятностного анализа риска [Probabilistic Risk Analysis (PRA)] вместо FMECA.

По этой причине FMECA не должен быть использован как единственный метод принятия решения о приемлемости риска конкретных последствий для системы с высоким риском или высокой сложностью, даже если оценка частоты и тяжести последствий основана на заслуживающих доверие данных. Это должно быть задачей вероятностного анализа риска, где больше влияющих параметров (и их взаимодействий) может быть принято во внимание (например, время выдержки, вероятность предотвращения последствий, скрытые отказы механизмов обнаружения отказов).

В соответствии с FMEA каждое идентифицированное последствие отказа относят к соответствующему классу тяжести. Частоту появления событий вычисляют на основе данных об отказах или оценивают для исследуемой составной части. Частота появления событий, умноженная на заданную наработку, дает значение критичности, которое затем применяют к шкале непосредственно, или, если шкала представляет собой вероятность появления события, определяют эту вероятность появления в соответ-

ствии со шкалой. Класс тяжести последствий и класс критичности (или вероятность появления события) для каждого последствия вместе составляют величину последствия. Можно выделить два основных метода оценки критичности: матрицу критичности и концепцию приоритетности риска *RPN*.

5.3.4 Определение интенсивности отказов

Если известны интенсивности отказов для видов отказов аналогичных объектов, определенные для внешних и эксплуатационных условий, аналогичных принятым для исследуемой системы, эти частоты событий могут быть непосредственно использованы в FMECA. Если имеются интенсивности отказов (а не видов отказов) для отличных от необходимых внешних и эксплуатационных условий, интенсивности видов отказов должны быть рассчитаны. При этом обычно используют следующее соотношение:

$$\lambda_i = \lambda_j \alpha_i \beta_i,$$

где λ_i — оценка интенсивности отказов i-го вида отказов (интенсивность отказов предполагается постоянной);

λ_j — интенсивность отказов j-го компонента;

α_i — отношение количества i-го вида отказов к общему количеству видов отказов, т. е. вероятность того, что объект будет иметь i-й вид отказа;

β_i — условная вероятность последствия i-го вида отказа.

Главным недостатком такого метода является неявное предположение о том, что интенсивность отказов постоянна и что многие используемые параметры получены на основе прогнозов или предположений. Это особенно важно в случае, когда для компонентов системы отсутствуют данные о соответствующих интенсивностях отказов, а имеется только расчетная вероятность отказа за установленное время работы с соответствующими нагрузками.

С помощью показателей, учитывающих изменения условий окружающей среды, нагрузок, технического обслуживания, данные об интенсивностях отказов, полученные в отличных от исследуемых условиях, могут быть пересчитаны.

Рекомендации по выбору значений этих показателей можно найти в соответствующих публикациях по надежности. Следует тщательно проверять правильность и применимость выбранных значений этих параметров для конкретной системы и ее эксплуатационных режимов.

В некоторых случаях, таких как количественный метод анализа, значение критичности вида отказа C_i (не связанное с общим значением «критичности», которое может принимать другое значение) используют вместо интенсивности отказов i-го вида отказов λ_i. Значение критичности связано с условной частотой отказа и временем эксплуатации и может быть использовано для получения более реалистичной оценки риска, соответствующего конкретному виду отказа, в течение заданного времени использования продукции.

$$C_i = \lambda_i t_j,$$

$$C_i = \lambda_j \alpha_i \beta_i t_j,$$

где t_j — время работы компонента в течение всего заданного времени исследований FMECA, для которого оценена вероятность, т. е. время активной работы j-го компонента.

Значение критичности для j-го компонента, имеющего m видов отказов, определяют по формуле

$$C_j = \sum_{i=1}^{m} \lambda_j \alpha_i \beta_i t_j.$$

Следует учесть, что значение критичности не связано с критичностью как таковой. Это лишь значение, вычисляемое в некоторых типах FMECA и представляющее собой относительную меру последствий вида отказа и вероятности его появления. Здесь значение критичности является мерой риска, а не мерой появления отказа.

Вероятность P_i появления отказа i-го вида за время t_j для полученной критичности:

$$P_i = 1 - e^{-C_i}.$$

Если интенсивности видов отказов и соответствующие значения критичности малы, то с грубым приближением можно утверждать, что для вероятностей появления меньше 0,2 (критичность равна 0,223) значения критичности и вероятности отказа очень близки.

В случае переменных интенсивностей отказов или частот появления отказа необходимо вычислять вероятность появления отказа, а не критичность, которая основана на предположении о постоянстве интенсивности отказов.

5.3.4.1 Матрица критичности

Критичность может быть представлена в виде матрицы критичности, как показано на рисунке 3. Следует иметь в виду, что не существует универсального определения критичности. Критичность должна быть определена аналитиком и принята руководителем программы или проекта. Определения могут существенно различаться для различных задач.

В матрице критичности, представленной на рисунке 3, предполагается, что тяжесть последствий увеличивается с увеличением ее значения. В этом случае IV соответствует наивысшей тяжести последствий (гибель человека и/или потеря функции системы, травмы людей). Кроме этого, предполагается, что на оси ординат вероятность появления вида отказа возрастает снизу вверх.

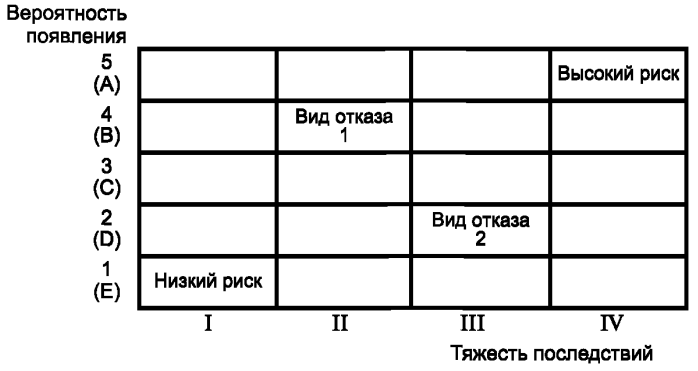

Рисунок 3 — Матрица критичности

Если самая высокая вероятность появления не превышает значения 0,2, то вероятность появления вида отказа и значение критичности приблизительно равны друг другу. Часто при составлении матрицы критичности применяют следующую шкалу:

- значение критичности 1 или E. Практически невероятный отказ, вероятность его появления изменяется в интервале: $0 \le P_i < 0{,}001$;
- значение критичности 2 или D. Редкий отказ, вероятность его появления изменяется в интервале: $0{,}001 \le P_i < 0{,}01$;
- значение критичности 3 или C. Возможный отказ, вероятность его появления изменяется в интервале: $0{,}01 \le P_i < 0{,}1$;
- значение критичности 4 или B. Вероятный отказ, вероятность его появления изменяется в интервале: $0{,}1 \le P_i < 0{,}2$;
- значение критичности 5 или A. Частый отказ, вероятность его появления изменяется в интервале: $0{,}2 \le P_i < 1$.

Рисунок 3 приведен только для примера. В других методах могут быть использованы для критичности и тяжести последствий другие обозначения и определения.

В примере, приведенном на рисунке 3, вид отказа 1 имеет более высокую вероятность появления, чем вид отказа 2, который имеет более высокую тяжесть последствий. Решение о том, какому виду отказа соответствует более высокий приоритет, зависит от вида шкалы, классов тяжести и частоты и используемых принципов ранжирования. Хотя для линейной шкалы вид отказа 1 (как обычно в матрице критичности) должен иметь более высокую критичность (или вероятность появления), чем вид отказа 2, могут быть ситуации, когда тяжесть последствий имеет абсолютный приоритет над частотой. В этом случае вид отказа 2 является более критичным видом отказа. Другой очевидный вывод состоит в том, что только виды отказа, относящиеся к одному уровню системы, можно обоснованно сравнивать в соответствии с матрицей критичности, поскольку виды отказа систем низкой сложности на более низком уровне обычно имеют более низкую частоту.

Как показано выше, матрица критичности (см. рисунок 3) может быть использована и качественно, и количественно.

5.3.5 Оценка приемлемости риска

Если требуемым результатом анализа является матрица критичности, может быть составлена схема распределения тяжести последствий и частот появления событий. Приемлемость риска определяют субъективно или руководствуются профессиональными и финансовыми решениями в зависимос-

ти от типа производства. В таблице 3 приведены некоторые примеры классов приемлемого риска и модифицированной матрицы критичности.

Таблица 3 — Матрица риска/критичности

Частота появления отказа	Уровни тяжести последствий			
	1 Ничтожный	2 Минимальный	3 Критический	4 Катастрофический
1 Практически невероятный отказ	Незначительные последствия	Незначительные последствия	Терпимые последствия	Терпимые последствия
2 Редкий отказ	Незначительные последствия	Терпимые последствия	Нежелательные последствия	Нежелательные последствия
3 Возможный отказ	Терпимые последствия	Нежелательные последствия	Нежелательные последствия	Неприемлемые последствия
4 Вероятный отказ	Терпимые последствия	Нежелательные последствия	Неприемлемые последствия	Неприемлемые последствия
5 Частый отказ	Нежелательные последствия	Неприемлемые последствия	Неприемлемые последствия	Неприемлемые последствия

5.3.6 Типы FMECA и шкалы ранжирования

Типы FMECA, описанные в 5.3.2 и широко используемые в автомобильной промышленности, обычно применяют для анализа проекта продукции, а также для анализа процессов производства этой продукции.

Методология анализа совпадает с описанными в общем виде FMEA/FMECA, кроме определений в трех таблицах для значений тяжести *S*, появления *O* и обнаружения *D*.

5.3.6.1 Альтернативное определение тяжести последствий

В таблице 4 приведен пример ранжирования тяжести последствий, которое обычно используют в автомобильной промышленности.

Таблица 4 — Тяжесть последствий вида отказов

Тяжесть последствий	Критерий	Ранг
Отсутствует	Нет последствий	1
Очень незначительная	Отделка (шумность) объекта не соответствует требованиям. Дефект замечают требовательные клиенты (менее 25 %)	2
Незначительная	Отделка (шумность) объекта не соответствует требованиям. Дефект замечают 50 % клиентов	3
Очень низкая	Отделка (шумность) объекта не соответствует требованиям. Дефект замечают большинство клиентов (более 75 %)	4
Низкая	Транспортное средство работоспособно, но система комфорта/удобства работает на ослабленном уровне, малоэффективна. Клиент испытывает некоторую неудовлетворенность	5
Умеренная	Транспортное средство/узел работоспособны, но система комфорта/удобства неработоспособна. Клиент испытывает дискомфорт	6
Высокая	Транспортное средство/узел работоспособно, но на сниженном уровне эффективности. Клиент очень неудовлетворен	7
Очень высокая	Транспортное средство/узел неработоспособны (потеря основной функции)	8
Опасная с предупреждением об опасности	Очень высокий уровень тяжести последствий, когда потенциальный вид отказа влияет на безопасность работы транспортного средства и/или вызывает несоответствие обязательным требованиям безопасности с предупреждением об опасности	9
Опасная без предупреждения об опасности	Очень высокий уровень тяжести последствий, когда потенциальный вид отказа влияет на безопасность работы транспортного средства и/или вызывает несоответствие обязательным требованиям без предупреждения об опасности	10

Примечание — Таблица заимствована из SAE J1739 [3].

Ранг тяжести последствий назначают для каждого вида отказа на основе влияния последствий отказа на систему в целом, ее безопасность, выполнение требований, целей и ограничений, а также вида транспортного средства как системы. Ранг тяжести указывают на листе FMECA. Определение ранга тяжести, приведенное в таблице 4, является точным для значений тяжести 6 и выше. Его следует применять в приведенной формулировке. Определение ранга тяжести от 3 до 5 может быть субъективным и зависит от особенностей задачи.

5.3.6.2 Характеристики появления отказа

В таблице 5 (также заимствованной из FMECA, используемой в автомобильной промышленности) приведены примеры качественных мер, характеризующих появление отказа, которые могут быть использованы в концепции *RPN*.

Таблица 5 — Виды отказа в соответствии с частотой и вероятностью появления

Характеристика появления вида отказа	Ранг *O*	Частота появления отказа	Вероятность
Очень низкая — отказ маловероятен	1	< 0,010 на 1000 транспортных средств/объектов	$\leq 10^{-5}$
Низкая — относительно мало отказов	2	0,1 на 1000 транспортных средств/объектов	10^{-4}
	3	0,5 на 1000 транспортных средств/объектов	$5 \cdot 10^{-4}$
Умеренная — отказы возможны	4	1 на 1000 транспортных средств/объектов	10^{-3}
	5	2 на 1000 транспортных средств/объектов	$2 \cdot 10^{-3}$
	6	5 на 1000 транспортных средств/объектов	$5 \cdot 10^{-3}$
Высокая — наличие повторных отказов	7	10 на 1000 транспортных средств/объектов	10^{-2}
	8	20 на 1000 транспортных средств/объектов	$2 \cdot 10^{-2}$
Очень высокая — отказ почти неизбежен	9	50 на 1000 транспортных средств/объектов	$5 \cdot 10^{-2}$
	10	> 100 на 1000 транспортных средств/объектов	$\geq 10^{-1}$

Примечание — См. AIAG [4].

В таблице 5 под «частотой» понимается отношение количества благоприятных случаев ко всем возможным случаям рассматриваемого события в течение выполнения стратегической задачи или срока службы. Например, вид отказа, которому соответствуют значения от 0 до 9, может привести к отказу одной из трех систем в течение периода выполнения задачи. Здесь определение вероятности появления отказов связано с исследуемым периодом времени. Рекомендуется указывать этот период времени в заголовке таблицы FMEA.

Лучшие методы могут быть применены, когда вероятность появления вычислена для компонентов и их видов отказов на основе соответствующих интенсивностей отказов для ожидаемых нагрузок (внешние эксплуатационные условия). Если необходимая информация недоступна, оценка может быть назначена, но при этом специалисты, выполняющие FMEA, должны иметь в виду, что значение появления отказа — это количество отказов на 1000 транспортных средств в течение заданного интервала времени (гарантийный период, срок службы транспортного средства и др.). Таким образом, это расчетная или оценочная вероятность появления вида отказа за исследуемый период времени. В отличие от шкалы тяжести последствий шкала появления отказов не линейна и не является логарифмической. Поэтому необходимо учитывать, что соответствующее значение *RPN* после вычислений оценок также нелинейно. Его необходимо использовать с особой осторожностью.

5.3.6.3 Ранжирование вероятности обнаружения отказа

Концепция *RPN* предусматривает оценку вероятности обнаружения отказа, т. е. вероятности того, что с помощью аппаратуры, процедур верификации, предусмотренных проектом, будут обнаружены возможные виды отказов за время, достаточное для предотвращения отказов на уровне системы в целом. Для применения FMEA процесса (PFMEA) это вероятность того, что у серии действий по контролю процесса есть возможность обнаружения и изоляции отказа прежде, чем он повлияет на последующие процессы или на готовую продукцию.

В частности, для продукции, которая может быть использована в нескольких других системах и областях применения, вероятность обнаружения бывает трудно оценить.

В таблице 6 приведен один из методов диагностики, используемых в автомобильной промышленности.

Таблица 6 — Критерии оценки обнаружения вида отказа

Характеристика обнаружения	Критерий — возможность обнаружения вида отказов на основе предусмотренных операций контроля	Ранг
Практически стопроцентно	Предусмотренный проектом контроль почти всегда обнаруживает потенциальную причину/механизм и следующий вид отказа	1
Очень хорошее	Очень высок шанс, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	2
Хорошее	Высокий шанс, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	3
Умеренно хорошее	Умеренно высокий шанс, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	4
Умеренное	Умеренный шанс, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	5
Слабое	Низкий шанс, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	6
Очень слабое	Очень низкий шанс, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	7
Плохое	Маловероятно, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	8
Очень плохое	Почти невероятно, что предусмотренный проектом контроль обнаружит потенциальную причину/механизм и последующий вид отказа	9
Практически невозможно	Предусмотренный проектом контроль не может обнаружить потенциальную причину/механизм и последующий вид отказа или контроль не предусмотрен	10

5.3.6.4 Оценка риска

Интуитивный метод, описанный выше, должен сопровождаться ранжированием приоритетности действий, направленных на обеспечение наивысшего уровня безопасности для заказчика (потребителя, клиента). Например, вид отказа с высоким значением тяжести, низкой интенсивностью появления и очень высоким значением обнаружения (например, 10, 3 и 2) может иметь намного более низкий *RPN* (в приведенном случае 60), чем вид отказа со средними значениями всех перечисленных величин (например, 5 в каждом случае), и, соответственно, *RPN* = 125. Поэтому часто используют дополнительные процедуры для гарантии того, что видам отказов с высоким рангом тяжести (например, 9 или 10) придано первостепенное значение и меры по их устранению приняты в первую очередь. В этом случае для решения следует руководствоваться еще и рангом тяжести, а не только *RPN*. Во всех случаях для принятия более обоснованного решения необходимо учитывать ранг тяжести наряду с *RPN*.

Значения приоритетности риска определяют также и в других методах FMEA, особенно в качественных методах.

Значения *RPN*, вычисленные в соответствии с вышеупомянутыми таблицами, часто используют для руководства при сокращении видов отказов. При этом следует учитывать предостережения 5.3.2.

RPN имеет следующие недостатки:

- промежутки в диапазонах значений: 88 % диапазонов пусты, только 120 из 1000 значений использованы;

- неоднозначность *RPN*: несколько комбинаций различных значений параметров приводят к одинаковым значениям *RPN*;

- чувствительность к небольшим изменениям: малые отклонения одного параметра оказывают большое влияние на результат, если другие параметры имеют бóльшие значения (например, $9 \cdot 9 \cdot 3 = 243$ и $9 \cdot 9 \cdot 4 = 324$, в то время как $3 \cdot 4 \cdot 3 = 36$ и $3 \cdot 4 \cdot 4 = 48$);

- неадекватная шкала: таблица появления отказов является нелинейной (например, отношение между двумя последовательными рангами может быть и 2,5, и 2);

- неадекватный масштаб *RPN*: разница в значениях для *RPN* может казаться незначительной, в то время как фактически является весьма существенной. Например, значения $S = 6$, $O = 4$, $D = 2$ дают *RPN* = 48, а значения $S = 6$, $O = 5$ и $D = 2$ дают *RPN* = 60. Второе значение *RPN* не вдвое больше, в то

время как фактически для *O* = 5 вероятность появления отказа вдвое больше, чем для *O* = 4. Поэтому исходные значения для *RPN* не следует сравнивать линейно;

- ошибочные выводы на основе сравнения *RPN*, поскольку шкалы являются порядковыми, а не относительными.

Анализ *RPN* требует осторожности и внимания. Правильное применение метода требует анализа значений тяжести, появления и обнаружения до формирования заключения и проведения корректирующих мер.

5.4 Отчет об анализе

5.4.1 Область применения и содержание отчета

Отчет по результатам FMEA может быть разработан как часть отчета о более широком исследовании или может быть самостоятельным документом. В любом случае отчет должен включать в себя обзор и подробные записи проведенного исследования, а также схемы и функциональные диаграммы структуры системы. Отчет должен также содержать список схем (с указанием их статуса), на которых основан FMEA.

5.4.2 Результаты анализа последствий

Должен быть подготовлен список последствий отказов для конкретной системы, исследуемой с помощью FMEA. В таблице 7 приведен типичный набор последствий отказов для стартера и электрической схемы двигателя автомобиля.

Таблица 7 — Пример последствий отказов для стартера автомобиля

Номер вида отказа	Последствие
1	Стартер не функционирует
2	Скорость вращения стартера меньше установленной
3	Стартер не захватывает зубчатый венчик маховика
4	Стартер включается преждевременно

Примечание 1 — Этот список является только примером. Каждая анализируемая система или подсистема будет иметь свой собственный набор последствий отказов.

Может потребоваться отчет о последствиях отказов для определения вероятности отказов системы, возникающих в результате перечисленных последствий отказов, и определения приоритетности корректирующих и предупреждающих действий. Отчет о последствиях отказов должен быть основан на перечне последствий отказов системы в целом и должен содержать детали видов отказов, влияющих на каждое последствие отказа. Вероятность появления каждого вида отказа вычисляют за установленный период времени функционирования объекта, а также для ожидаемых параметров использования и нагрузок. В таблице 8 показан пример обзора последствий отказов.

Таблица 8 — Пример вероятностей последствий отказов

Номер вида отказа	Последствие	Виды отказов, приводящие к последствию	Вероятность появления последствия отказа
1	Стартер не функционирует	1, 3, 7, 8, 9, 16, 21, 22	$8 \cdot 10^{-3}$
2	Скорость вращения стартера меньше установленной	6, 11, 12, 19, 20	$6 \cdot 10^{-4}$
3	Стартер не захватывает зубчатый венчик маховика	2, 4, 5, 10, 13	$1{,}1 \cdot 10^{-5}$
4	Стартер включается преждевременно	14, 15, 17, 18	$3{,}6 \cdot 10^{-7}$

Примечание 2 — Такая таблица может быть построена для различных качественных и количественных ранжирований объекта или системы.

Отчет должен также содержать краткое описание метода анализа и уровня, на котором он был проведен, используемые предположения и основные правила. Кроме того, он должен включать в себя перечни:

a) видов отказов, которые приводят к серьезным последствиям;

b) рекомендаций для проектировщиков, персонала технического обслуживания, планировщиков и пользователей;

c) изменений проекта, которые выполнены в результате FMEA;

d) последствий, которые устранены в результате общих изменений проекта.

6 Другие исследования

6.1 Отказ общей причины

Для анализа надежности недостаточно рассмотреть только случайные и независимые отказы, поскольку могут произойти отказы общей причины. Например, причиной нарушения функционирования системы или ее отказа может быть одновременное нарушение работы нескольких компонентов системы. Это может быть следствием ошибки в конструкции (неоправданное ограничение допустимых значений компонентов), воздействия окружающей среды (молния) или человеческой ошибки.

Наличие отказов общей причины [Common Cause Failure (CCF)] противоречит предположению о независимости видов отказов, рассматриваемых FMEA. Наличие CCF предполагает возможность появления более одного отказа одновременно или в пределах достаточно короткого промежутка времени и соответствующее появление последствий одновременных отказов.

Как правило, источниками CCF могут быть:

- конструкция (разработка программного обеспечения, нормирование);
- производство (недостатки партий компонентов);
- окружающая среда (электрические помехи, циклическое воздействие температуры, вибрация);
- человеческий фактор (неправильная работа или неправильные действия по техническому обслуживанию).

FMEA должен поэтому рассматривать возможные источники CCF при анализе системы, в которой использовано резервирование, или большое количество объектов для смягчения последствий отказа.

CCF — результат события, которое из-за логических зависимостей вызывает одновременное состояние отказа в двух или более компонентах (включая зависимые отказы, вызванные последствиями независимого отказа). Отказы общей причины могут происходить в идентичных составных частях с одинаковыми видами отказов и слабыми местами при различных вариантах сборки системы и могут быть резервированы.

Возможности FMEA для анализа CCF весьма ограничены. Однако FMEA — процедура последовательного изучения каждого вида отказа и связанных с ним причин, а также идентификации всех периодических испытаний, профилактического технического обслуживания и т. д. Этот метод позволяет исследовать все причины, которые могут вызвать CCF.

Полезно использовать комбинацию нескольких методов для предотвращения или смягчения последствий CCF (моделирование системы, физический анализ компонентов), в том числе: функциональное разнообразие, когда избыточные ветви или части системы, выполняющие одну и ту же функцию, неидентичны и имеют различные виды отказов; физическое разделение, позволяющее устранить влияние экологических или электромагнитных воздействий, вызывающих CCF, и т. д. Обычно FMEA предусматривает экспертизу предупреждающих CCF мер. Однако эти меры должны быть описаны в колонке замечаний рабочей таблицы для помощи в понимании FMEA в целом.

6.2 Человеческий фактор

Для предотвращения или сокращения некоторых человеческих ошибок необходимы специальные разработки. К таким мерам относится обеспечение механической блокировки железнодорожного сигнала и пароля для использования компьютера или поиска данных. Если такие условия в системе существуют, последствия отказа будут зависеть от вида ошибки. Некоторые виды человеческой ошибки должны быть исследованы с применением дерева неисправностей системы для проверки эффективности оборудования. Даже частичное внесение в список этих видов отказов полезно для идентификации недостатков конструкции и процедур. Идентификация всех видов человеческих ошибок, вероятно, невозможна.

Много отказов CCF основано на человеческих ошибках. Например, неправильное обслуживание идентичных объектов может нивелировать резервирование. Чтобы избежать этого, часто применяют неидентичные резервные элементы.

6.3 Ошибки программного обеспечения

FMEA, проводимый для аппаратных средств сложной системы, может иметь последствия для программного обеспечения системы. Таким образом, решения о последствиях, критичности и условных вероятностях, вытекающие из FMEA, могут зависеть от элементов программного обеспечения, их особенностей, последовательности и времени работы. В этом случае взаимосвязи между аппаратными средствами и программным обеспечением должны быть четко идентифицированы, поскольку последующее изменение или улучшение программного обеспечения может изменить FMEA и полученные на его основе оценки. Одобрение программного обеспечения и его изменений может быть условием для пересмотра FMEA и соответствующих оценок, например логика программного обеспечения может быть изменена для повышения безопасности за счет эксплуатационной надежности.

Сбои из-за ошибок или несоответствий программного обеспечения будут иметь последствия, значения которых должны быть определены при проектировании программного обеспечения и аппаратных средств. Установление таких ошибок или несоответствий и анализ их последствий возможны только ограниченно. Последствия возможных ошибок в программном обеспечении для соответствующих аппаратных средств должны быть оценены. Рекомендации по уменьшению таких ошибок для программного обеспечения и аппаратных средств часто являются результатом анализа.

6.4 FMEA и последствия отказов системы

FMEA системы может быть выполнен независимо от ее конкретного применения и может затем быть приспособлен к особенностям конструкции системы. Это относится к небольшим наборам, которые могут быть самостоятельно рассмотрены как компоненты (например, электронный усилитель, электрический двигатель, механический клапан).

Однако более типичной является разработка FMEA для конкретного проекта с конкретными последствиями отказов системы. Необходимо классифицировать последствия отказов системы, например: отказ предохранителя, устранимый отказ, неустранимый отказ, ухудшение выполнения задачи, невыполнение задачи, последствия для отдельных людей, группы или общества в целом.

Возможность учета в FMEA самых отдаленных последствий отказа системы зависит от конструкции системы и взаимосвязей FMEA с другими формами анализа, такими как дерево неисправностей, марковский анализ, сети Петри и т. п.

7 Применения

7.1 Использование FMEA/FMECA

FMEA — метод, который прежде всего приспособлен к исследованию отказов материала и оборудования и может быть применен к различным типам систем (электрических, механических, гидравлических и т.д.) и их комбинациям для частей оборудования, системы или проекта в целом.

FMEA должен включать в себя исследование программного обеспечения и действий человека, если они влияют на надежность системы. FMEA может быть исследованием процессов (медицинских, лабораторных, производственных, образовательных и т.п.). В этом случае его обычно называют FMEA процесса или PFMEA. При выполнении FMEA процесса всегда учитывают цели и задачи процесса и затем исследуют каждый этап процесса как основу неблагоприятных результатов для других этапов процесса или выполнения целей процесса.

7.1.1 Применение в пределах проекта

Пользователь должен определить, как и для каких целей использует FMEA. FMEA может быть использован самостоятельно или служить дополнением и поддержкой для других методов анализа надежности. Требования к FMEA следуют из необходимости понять поведение аппаратных средств и их значение для функционирования системы или оборудования. Требования к FMEA могут существенно меняться в зависимости от особенностей проекта.

FMEA поддерживает концепцию анализа проекта и должен быть применен как можно раньше при проектировании подсистем и системы в целом. FMEA применим ко всем уровням системы, но более подходит для низких уровней, характеризующихся большим числом объектов и/или функциональной сложностью. Важным является специальное обучение персонала, выполняющего FMEA. Необходимо тесное сотрудничество инженеров и проектировщиков системы. FMEA следует обновлять по мере продвижения проекта и изменения конструкции. В конце этапа проектирования FMEA используют для проверки конструкции и демонстрации соответствия разработанной системы установленным требованиям пользователя, требованиям стандартов, инструкций и обязательным требованиям.

Информация, полученная на основе FMEA, идентифицирует приоритеты для статистического управления производственным процессом, выборочного контроля и входного контроля в процессе производства и монтажа, а также для квалификационных, приемо-сдаточных, приемочных и пусковых испытаний. FMEA является источником информации для процедур диагностики, технического обслуживания при разработке соответствующих руководств.

При выборе глубины и способов применения FMEA к объекту или проекту важно рассмотреть цели, для которых необходимы результаты FMEA, согласованность по времени с другими действиями и установить требуемую степень компетентности и контроля нежелательных видов и последствий отказов. Это приводит к качественному планированию FMEA на указанных уровнях (система, подсистема, компонент, объект итеративного процесса проектирования и разработки).

Для обеспечения эффективности FMEA должно быть четко установлено его место в программе надежности, а также определены время, трудовые и другие ресурсы. Жизненно важно, чтобы FMEA не был сокращен для экономии времени и денег. Если время и деньги ограничены, FMEA должен быть сконцентрирован на тех частях конструкции, которые являются новыми или используют новые методы. Из экономических соображений FMEA может быть направлен на области, идентифицированные как критические другими методами анализа.

7.1.2 Применение к процессам

Для выполнения PFMEA необходимо следующее:

a) четкое определение цели процесса. Если процесс является сложным, цель процесса может противоречить общей цели или цели, связанной с продукцией процесса, продукцией серии последовательных процессов или этапов, продукцией отдельного этапа процесса, а также соответствующим частным целям:

b) понимание отдельных этапов процесса;

c) понимание потенциальных недостатков, характерных для каждого этапа процесса;

d) понимание последствий каждого отдельного недостатка (потенциального отказа) для продукции процесса;

e) понимание потенциальных причин каждого из недостатков или потенциальных отказов и несоответствий процесса.

Если процесс связан с продукцией более одного наименования, то его анализ может быть выполнен для отдельных типов продукции как PFMEA. Анализ процесса может также быть выполнен в соответствии с его этапами и потенциальными неблагоприятными результатами, которые приводят к обобщенному PFMEA независимо от конкретных типов продукции.

7.2 Преимущества FMEA

Некоторые из особенностей применения и преимущества FMEA перечислены ниже:

a) исключение дорогостоящих модификаций вследствие ранней идентификации недостатков конструкции;

b) идентификация отказов, которые при появлении по одному и в комбинации имеют недопустимые или существенные последствия, и определение видов отказов, которые могут иметь серьезные последствия для ожидаемой или требуемой функции.

Примечание 1 — Такие последствия могут включать в себя зависимые отказы;

c) определение необходимых методов повышения надежности конструкции (резервирование, оптимальные рабочие нагрузки, отказоустойчивость, выбор компонентов, пересортировка и т.д.);

d) обеспечение логической модели для оценки вероятности или интенсивности появления аномальных условий эксплуатации системы при подготовке к анализу критичности;

e) выявление проблемных зон безопасности и ответственности за качество выпускаемой продукции или ее несоответствие обязательным требованиям.

Примечание 2 — Часто для безопасности необходимы самостоятельные исследования, но пересечение неизбежно и поэтому в процессе исследования очень желательно сотрудничество;

f) разработка программы испытаний, позволяющей обнаруживать потенциальные виды отказов;

g) концентрация на ключевых вопросах управления качеством, анализа процессов контроля и изготовления продукции;

h) помощь в определении особенностей общей стратегии и графика профилактического технического обслуживания;

i) помощь и поддержка в определении критериев испытаний, планов испытаний и диагностических процедур (сравнительные испытания, испытания на надежность);

j) поддержка последовательности исключения дефектов конструкции и поддержка планирования альтернативных режимов работы и переконфигурации;

k) понимание проектировщиками параметров, влияющих на надежность системы;

l) разработка заключительного документа, содержащего доказательства предпринятых действий по обеспечению соответствия результатов проектирования требованиям технического задания при обслуживании. Это особенно важно в случае ответственности за качество выпускаемой продукции.

7.3 Ограничения и недостатки FMEA

FMEA чрезвычайно эффективен, если его используют для анализа элементов, которые вызывают отказ системы в целом или нарушение основной функции системы. Однако FMEA может быть трудным и утомительным для сложных систем, имеющих много функций и состоящих из различных наборов компонентов. Эти сложности увеличиваются при наличии многочисленных режимов эксплуатации, а также нескольких политик технического обслуживания и ремонта.

FMEA может быть трудоемким и неэффективным процессом при необдуманном применении. Исследования FMEA, результаты которых предполагается использовать в дальнейшем, должны быть определены. Проведение FMEA не должно быть включено в требования без предварительного анализа.

Осложнения, недоразумения и ошибки могут произойти при попытке охвата исследованиями FMEA нескольких уровней в иерархической структуре системы, если она предусматривает резервирование.

Взаимосвязи между людьми или группами видов отказов или причинами видов отказов не могут быть эффективно представлены в FMEA, так как главное предположение для этого анализа — независимость видов отказов. Этот недостаток становится еще более явным из-за взаимодействий программного обеспечения и аппаратных средств, когда предположение о независимости не подтверждается. Отмеченное справедливо для взаимодействия человека с аппаратными средствами и моделей этого взаимодействия. Предположение о независимости отказов не позволяет уделять должное внимание видам отказа, которые при совместном появлении могут иметь существенные последствия, тогда как каждый из них в отдельности имеет низкую вероятность появления. Взаимосвязи элементов системы легче исследовать, используя для анализа метод дерева неисправностей FTA (*ГОСТ Р 51901.5*).

FTA предпочтителен для применения в FMEA, поскольку ограничивается связями только двух уровней иерархической структуры, например идентификацией видов отказов объектов и определением их последствий для системы в целом. Эти последствия затем становятся видами отказов на следующем уровне, например для модуля, и т. д. Однако существует опыт успешного выполнения многоуровневых FMEA.

Кроме того, недостатком FMEA является его неспособность оценить общую надежность системы и таким образом оценить степень улучшения ее конструкции или изменений.

7.4 Взаимосвязь с другими методами

FMEA (или FMECA) может быть применен самостоятельно. Как системный индуктивный метод анализа FMEA чаще всего используют в качестве дополнения к другим методам, особенно дедуктивным, таким как FTA. На стадии проектирования часто бывает трудно решить, какой метод (индуктивный или дедуктивный) предпочесть, так как оба используют при выполнении анализа. Если для производственного оборудования и системы идентифицированы уровни риска, предпочтителен дедуктивный метод, но FMEA по-прежнему является полезным инструментом проектирования. Однако его следует применять в дополнение к другим методам. Это особенно справедливо, когда решения должны быть найдены в ситуациях с многократными отказами и цепочкой последствий. Метод, используемый вначале, должен зависеть от программы проекта.

На ранних стадиях проектирования, когда известны только функции, общая структура системы и ее подсистемы, успешное функционирование системы можно изобразить с помощью структурной схемы надежности или дерева неисправностей. Однако для составления этих систем к подсистемам должен быть применен индуктивный процесс FMEA. В этих обстоятельствах метод FMEA не является всеобъемлющим, но отражает результат в наглядной табличной форме. В общем случае анализа сложной системы с несколькими функциями, многочисленными объектами и взаимосвязями между этими объектами FMEA является необходимым, но недостаточным.

Анализ дерева неисправностей (FTA) является дополнительным дедуктивным методом анализа видов отказов и соответствующих им причин. Он позволяет прослеживать причины низкого уровня, приводящие к отказам высокого уровня. Хотя логический анализ иногда используют для качественного анализа последовательностей неисправностей, он обычно предшествует оценке частоты отказов высокого уровня. FTA позволяет моделировать взаимозависимости различных видов отказов в тех случаях, когда

их взаимодействие может привести к событию высокой тяжести. Это особенно важно, когда появление одного вида отказа вызывает появление другого вида отказа с высокой вероятностью и высокой тяжестью. Этот сценарий не может быть успешно смоделирован с применением FMEA, где каждый вид отказа рассматривают независимо и индивидуально. Один из недостатков FMEA — его неспособность анализировать взаимодействия и динамику возникновения вида отказа в системе.

FTA концентрируется на логике совпадающих (или последовательных) и альтернативных событий, вызывающих нежелательные последствия. FTA позволяет построить правильную модель анализируемой системы, оценки ее безотказности и вероятности отказа, а также позволяет оценить влияние улучшений проекта и уменьшения числа отказов конкретного вида на надежность системы в целом. Форма FMEA является более наглядной. Оба метода используются в общем анализе безопасности и надежности сложной системы. Однако если система базируется главным образом на последовательной логике с небольшим резервированием и многочисленными функциями, то FTA является слишком сложным способом представления логики системы и идентификации видов отказов. В таких случаях FMEA и метод структурной схемы надежности адекватны. В других случаях, когда предпочтителен FTA, он должен быть дополнен описаниями видов отказов и их последствий.

При выборе метода анализа необходимо руководствоваться в первую очередь специфическими требованиями проекта, не только техническими, но также требованиями к показателям времени, стоимости, эффективности и использования результатов. Общие руководящие принципы:

a) FMEA применим, когда требуется всестороннее знание характеристик отказа объекта;

b) FMEA более подходит для небольших систем, модулей или комплексов;

c) FMEA является важным инструментом исследований, разработок, проектирования или решения иных задач, когда недопустимые последствия отказов должны быть идентифицированы и найдены необходимые меры по их устранению или смягчению;

d) FMEA может быть необходим для объектов, при проектировании которых использованы новейшие достижения, когда характеристики отказов не могут быть известны из предыдущей эксплуатации;

e) FMEA более применим к системам, имеющим большое количество компонентов, которые связаны общей логикой отказов;

f) FTA является более подходящим для анализа видов многократных и зависимых отказов со сложной логикой и резервированием. FTA может быть использован на более высоких уровнях структуры системы, ранних стадиях проекта и в случае идентификации необходимости детального FMEA на более низких уровнях при углубленной проработке конструкции.

Приложение А
(справочное)

Краткое описание процедур FMEA и FMECA

А.1 Этапы. Обзор выполнения анализа

При проведении анализа должны были выполнены следующие этапы процедуры:

a) решение о том, какой метод — FMEA или FMECA необходим;
b) определение границ системы для анализа;
c) осознание требований и функций системы;
d) определение критерия отказа/работоспособности;
e) определение видов отказов и последствий отказов каждого объекта в отчете;
f) описание каждого последствия отказа;
g) составление отчета.

Дополнительные этапы для FMECA:

h) определение рангов тяжести отказов системы;
i) установление значений тяжести видов отказов объекта;
j) определение вида отказа объекта и частоты последствий;
k) определение частоты вида отказа;
l) составление матриц критичности для видов отказов объекта;
m) описание критичности последствий отказа в соответствии с матрицей критичности;
n) составление матрицы критичности для последствий отказа системы;
o) составление отчета для всех уровней анализа.

Примечание — Оценка частоты вида и последствий отказа в FMEA может быть выполнена с помощью этапов h), i) и j).

А.2 Рабочая таблица FMEA

А.2.1 Область применения рабочей таблицы

Рабочая таблица FMEA описывает детали анализа в табличной форме. Хотя общая процедура FMEA является постоянной, рабочая таблица может быть приспособлена к конкретному проекту в соответствии с его требованиями.

На рисунке А.1 приведен пример вида рабочей таблицы FMEA.

А.2.2 Головка рабочей таблицы

Головка рабочей таблицы должна включать в себя следующую информацию:

- обозначение системы как объекта в целом, для которой идентифицированы конечные последствия. Это обозначение должно быть совместимо с терминологией, используемой в блок-схемах, схемах и рисунках;
- период и режим эксплуатации, выбранные для анализа;
- объект (модуль, компонент или часть), исследуемый в этой рабочей таблице;
- уровень пересмотра, дата, имя аналитика, координирующего FMEA, а также имена основных членов команды, обеспечивающих дополнительную информацию для контроля документа.

А.2.3 Заполнение рабочей таблицы

Записи в столбцах «Объект» и «Описание объекта и его функций» должны идентифицировать тему анализа. Должны быть приведены ссылки на блок-схему или другие приложения, краткое описание объекта и его функции.

Описание способов отказа объекта приводят в столбце «Вид отказа». В пункте 5.2.3 приведены рекомендации по идентификации потенциальных видов отказов. Использование уникального идентификатора «Код вида отказа» для каждого уникального вида отказа объекта облегчит подведение итогов анализа.

Наиболее вероятные причины видов отказов перечисляют в столбце «Возможные причины отказа».

Краткое описание последствий вида отказа приводят в столбце «Локальные последствия отказа». Аналогичную информацию для объекта в целом приводят в столбце «Итоговые последствия отказа». Для некоторых исследований FMEA желательно оценить последствия отказа на промежуточном уровне. В этом случае последствия указывают в дополнительном столбце «Следующий более высокий уровень сборки». Идентификация последствий вида отказа рассмотрена в 5.2.5.

Краткое описание метода обнаружения вида отказа приводят в столбце «Метод обнаружения отказа». Метод обнаружения может быть реализован автоматически встроенным тестом, предусмотренным конструкцией, или может требовать применения диагностических процедур с привлечением персонала по эксплуатации и техническому обслуживанию. Важно идентифицировать метод обнаружения видов отказа для обеспечения выполнения корректирующих действий.

Особенности конструкции, которые смягчают последствия или сокращают количество отказов конкретного вида, например резервирование, должны быть отмечены в столбце «Условия компенсации отказа». Компенсация средствами технического обслуживания или действиями оператора также должна быть здесь указана.

В столбце «Класс тяжести отказа» указывают уровень тяжести, установленный аналитиками FMEA.

В столбце «Частота или вероятность появления отказа» указывают частоту или вероятность появления конкретного вида отказа. Масштаб частоты должен соответствовать ее значению (например, отказы за миллион часов, отказы за пробег в 1000 км и т.д.).

В столбце «Замечания» указывают наблюдения и рекомендации в соответствии с 5.3.4.

А.2.4 Замечания в рабочей таблице

Последний столбец рабочей таблицы должен содержать все необходимые замечания для разъяснения остальных записей. Возможные будущие действия, такие как рекомендации по улучшению конструкции, могут быть зарегистрированы и затем указаны в отчете. Этот столбец может также включать в себя следующее:

a) любые необычные условия;
b) последствия отказов резервного элемента;
c) описание критических свойств проекта;
d) любые замечания, расширяющие информацию;
e) ссылки на другие записи для последовательного анализа отказа;
f) существенные требования к техническому обслуживанию;
g) доминирующие причины отказов;
h) доминирующие последствия отказа;
i) принятые решения, например по анализу проекта.

FMEA

Конечный объект: Период и режим эксплуатации:			Объект: Пересмотр:					Подготовлен: Дата:			
Объект	Описание объекта и его функций	Вид отказа (неисправности)	Код вида отказа (неисправности)	Возможные причины отказа (неисправности)	Локальные последствия отказа (неисправности)	Итоговые последствия отказа (неисправности)	Метод обнаружения отказа	Условия компенсации отказа	Класс тяжести отказа	Частота или вероятность появления отказа	Замечания

Рисунок А.1 — Пример рабочей таблицы FMEA

Приложение В
(справочное)

Примеры исследований

В.1 Пример 1 — FMECA для электропитания автомобиля с вычислением *RPN*

На рисунке В.1 представлена небольшая часть обширного FMECA для автомобиля. Проанализированы электропитание и его связи с аккумуляторной батареей.

Цепь батареи включает в себя диод D1, конденсатор С9, соединяющий положительную клемму батареи с заземлением. Применен диод обратной полярности, что в случае соединения отрицательной клеммы батареи с корпусом защищает объект от повреждений. Конденсатор является фильтром электромагнитных помех. Если любая из этих частей замыкает на землю, батарея также замыкает на землю, что может привести к отказу батареи

Объект/Функция			Потенциальный вид отказа	Потенциальные последствия отказа		Ранг тяжести	Класс	Потенциальная причина/ механизм отказа	Точная(ые) причина(ы)/механизм отказа
Подсистема	Составная часть	Компонент		Локальные последствия	Итоговые последствия				
Электропитание									
	V1								
		D1	Короткое замыкание	Клемма батареи + замыкает на землю	Утечка батареи, поездка невозможна	10		Внутренний дефект компонента	Разрушение материала
		D1	Разрыв электрической цепи	Нет резервной защиты от обратного напряжения	Незаметные	2		Внутренний дефект компонента	Трещина в сварке или полупроводнике
		С9	Короткое замыкание	Клемма батареи + замыкает на землю	Утечка батареи, поездка невозможна	10		Внутренний дефект компонента	Разрушение диэлектрика или трещина
		С9	Разрыв электрической цепи	Нет фильтра электромагнитных помех EMI	Работа объекта не соответствует требованиям	2		Внутренний дефект компонента	Обнажение диэлектрика, утечка, пустота или трещина
		L1	Разрыв электрической цепи	Нет V1	Объект неработоспособен. Нет предупреждающей индикации	9		Внутренний дефект компонента	Разрушение материала
		R91	Разрыв электрической цепи	Нет напряжения для включения электрической цепи	Объект неработоспособен. Нет предупреждающей индикации	9		Внутренний дефект компонента	Трещина в сварке или материале

Рисунок В.1 — FMEA для части автомобильной

транспортного средства. Такой отказ, конечно, не имеет предупреждения. Отказ, при котором поездка невозможна, в автомобильной промышленности считают опасным. Поэтому для вида отказа обеих названных частей ранг тяжести *S* равен 10. Значения ранга появления *O* были вычислены на основе интенсивностей отказов частей с соответствующими нагрузками для работы транспортного средства и затем приведены к масштабу *O* для FMEA автомобиля. Значение ранга обнаружения *D* является очень низким, поскольку замыкание любой из частей сразу обнаруживается при тестировании объекта на работоспособность.

Отказ любой из вышеупомянутых частей не приводит к повреждению объекта, однако для диода нет защиты от изменения полярности. При отказе конденсатора, не фильтрующего электромагнитные помехи, возможны помехи для оборудования в транспортном средстве.

Если в катушке L1, расположенной между батареей и электрической цепью и предназначенной для фильтрации, имеется обрыв, объект неработоспособен, поскольку батарея отсоединена, и предупреждение не высветится. Катушки имеют очень низкую интенсивность отказов, поэтому ранг появления равен 2.

Резистор R91 передает напряжение батареи на коммутирующие транзисторы. При отказе R91 объект становится неработоспособным с рангом тяжести 9. Так как резисторы имеют очень низкую интенсивность отказов, ранг появления равен 2. Ранг обнаружения равен 1, так как объект не является работоспособным.

Ранг появления	Действия по предотвращению	Действия по обнаружению	Ранг обнаружения	*RPN*	Рекомендуемое действие	Ответственный и дата выполнения	Результаты действий				
							Предпринятые действия	Ранг	Ранг	Ранг	*RPN*
3	Выбор компонента более высокого качества и мощности	Оценочные и контрольные испытания на надежность	1	30							
3	Выбор компонента более высокого качества и мощности	Оценочные и контрольные испытания на надежность	2	12							
3	Выбор компонента более высокого качества и мощности	Оценочные и контрольные испытания на надежность	1	30							
2	Выбор компонента более высокого качества и мощности	Оценочные и контрольные испытания на надежность	1	4							
2	Выбор компонента более высокого качества и мощности	Оценочные и контрольные испытания на надежность	1	18							
2	Выбор компонента более высокого качества и мощности	Оценочные и контрольные испытания на надежность	1	18							

электроники с вычислением *RPN*

В.2 Пример 2 — FMEA для системы двигатель—генератор

Пример иллюстрирует применение метода FMEA к системе двигатель—генератор. Цель исследования ограничена только системой и касается последствий отказов элементов, связанных с электропитанием двигателя—генератора или любых других последствий отказов. Это определяет границы анализа. Приведенный пример частично иллюстрирует представление системы в виде блок-схемы. Первоначально выделено пять подсистем (см. рисунок В.2) и одна из них — система подогрева, вентиляции и охлаждения — представлена на более низких уровнях структуры по отношению к уровню, на котором было решено начать FMEA (см. рисунок В.3). Блок-схемы также показывают систему нумерации, используемую для ссылок в рабочих таблицах FMEA.

Для одной из подсистем двигателя—генератора показан пример рабочей таблицы (см. рисунок В.4), соответствующей рекомендациям настоящего стандарта.

Важной частью FMEA являются определение и классификация тяжести последствий отказов для системы в целом. Для системы двигатель—генератор они представлены в таблице В.1.

Таблица В.1 — Определение и классификация тяжести последствий отказов для системы двигатель—генератор в целом

Уровень	Характеристика тяжести отказа	Описание
5	Катастрофический	Отсутствие напряжения. Невозможность выполнения задачи
4	Критический	Снижение напряжения в системе. Невозможность выполнения задачи
3	Значительный	Отсутствие напряжения из-за принудительного отключения на период восстановления работоспособности
2	Минимальный	Временное снижение напряжения до восстановления работоспособности
1	Незначительный	Отсутствие потери или снижения напряжения

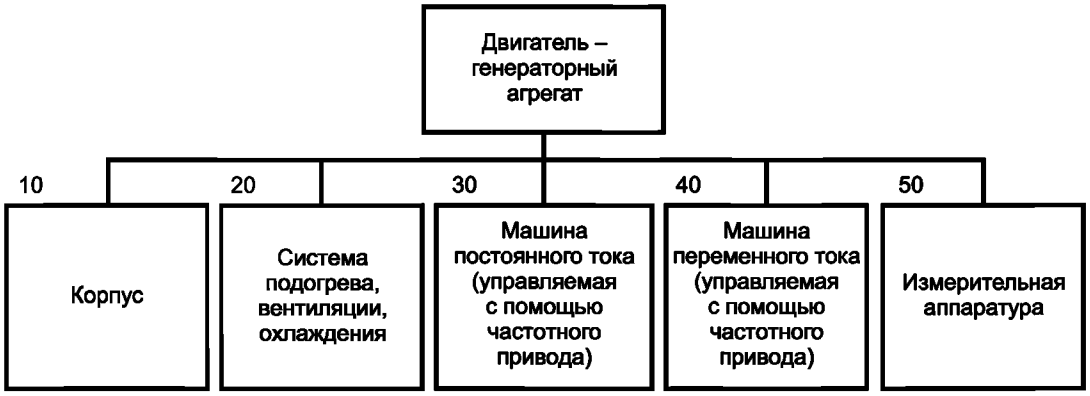

Рисунок В.2 — Диаграмма подсистем двигателя—генератора

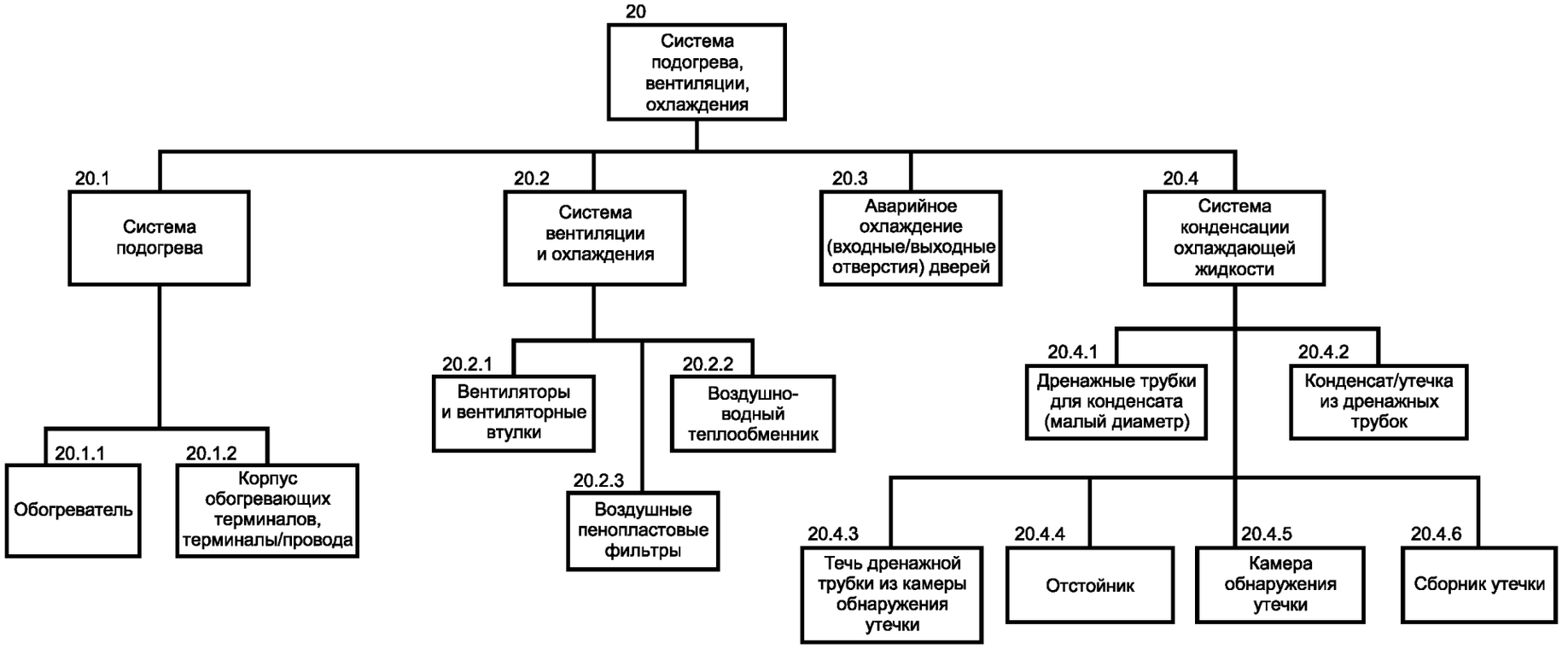

Рисунок В.3 — Диаграмма системы нагревания, вентиляции, охлаждения

Система 20 — Система подогрева, вентиляции и охлаждения													
Объект	Компонент	Функция	Вид отказа (неисправности)	Последствия отказа	Метод или признак обнаружения отказа	Резервирование	Интенсивность вида отказа по категориям качества					Замечания
							1	2	3	4	5	
20.1	Система подогрева (от 12 до 6 выключателей на каждом конце) только при неработающем механизме	Все										Примечание — Механизм может перегреться, если обогреватели не выключаются автоматически
20.1.1	Обогреватели	Нагрев	a) Перегорание обогревателя b) Короткое замыкание на землю из-за дефекта изоляции	Пониженное нагревание Отсутствие нагревания — возможна конденсация	a) Температура менее чем на 5 °С выше температуры окружающей среды b) Применение плавкого предохранителя или проверенного выключателя	Одно короткое замыкание на землю не должно приводить к отказу системы				1,2 0,3		Одно короткое замыкание на землю не должно приводить к отказу системы
20.1.2	Корпус обогревающих терминалов, кабель	Соединение с обогревателями	a) Перегревание терминала или кабеля одного/шести или всех обогревателей b) Короткое замыкание на землю терминалов (прослеживание)	Отсутствие или уменьшение нагревания, конденсация Отсутствие всего нагревания — конденсация	Температура менее чем на 5 °С выше температуры окружающей среды Проверенная поставка					0,5		
						Итого				2,0		

Рисунок В.4 — FMEA для системы 20

В.3 Пример 3 — FMECA для производственного процесса

FMECA процесса исследует каждый процесс изготовления рассматриваемого объекта. FMECA исследует то, что может произойти не так, как предусмотрено, и существующие меры защиты (в случае отказа), а также как часто это может происходить и как можно устранить подобные ситуации, модернизируя объект или процесс. Цель состоит в концентрации внимания на возможных (или известных) проблемах поддержки или достижения необходимого качества готовой продукции. Предприятия, собирающие сложные объекты, такие как легковые автомобили, хорошо знают о необходимости требовать от поставщиков компонентов выполнения такого анализа. При этом основные выгоды получают поставщики компонентов. Осуществление анализа заставляет выполнять повторную проверку нарушения технологии изготовления, а иногда и отказов, что приводит к затратам на улучшение.

Форма рабочей таблицы для FMECA процесса аналогична форме рабочей таблицы для FMECA продукции, но есть некоторые отличия (см. рисунок В.5). Мерой критичности является значение приоритетности действий (*APN*), очень близкое по смыслу к значению приоритетности риска (*RPN*), рассматриваемому выше. FMECA процесса исследует способы появления дефектов и несоответствий и варианты поставки заказчику в соответствии с процедурами управления качеством. FMECA не рассматривает отказы продукции при обслуживании, связанные с износом или ненадлежащим использованием.

Объект	Процесс	Вид отказа	Объект воздействия отказа	Потенциальное последствие	V	Потенциальная причина	Существующие средства управления	Существующие значения				Рекомендованное действие	Предпринятое действие	Пересмотренные значения			
								Occ	*Sev*	*Det*	*RPN*			*Occ*	*Sev*	*Det*	*APN*
01-01-01	Вставки	Неправильные размеры или углы изгиба плеча	1) a	Вставки без нагрузки на штамп. Снижение производительности		Недостатки производства или управления качеством	Изготовитель и планы статистического приемочного контроля	1	9	9	81	Анализ планов выборочного контроля. Изоляция дефектных комплектующих от годных поставок. Обучение сборщиков					
02			i) b	Разрегулированная вставка													
03			i) a	Неправильная толщина юбки, окружающей вставку													
04			iv) b	Снижение работоспособности													
05			iv) c	Сокращение ресурса													
01-02-01	Вставки	Недостаточный блеск никелевого покрытия	i) a	Коррозия. Отклонения на завершающей стадии			Визуальный контроль в соответствии с планом статистического приемочного контроля	5	6	1	30	Включить выборочный контроль для выполнения визуальной проверки на правильный блеск					
01-03-01	Вставки	Неадекватная оценка внешнего вида	i) a	Недостаточная металлическая выпрессовка. Неправильная толщина стенки. Отходы		Недостатки производства или управления качеством	Визуальный контроль в планах статистического приемочного контроля	2	8	6	96	Включить выборочный контроль для выполнения визуальной проверки на правильный блеск					
02			ii) a	При механической обработке обнаружены тонкие стенки. Отходы													
			iv) a	Сокращение ресурса													

Вид последствия:
последствия для промежуточного процесса;
последствия для конечного процесса;
последствия для сборки;
последствия для пользователя.

Вид критичности:
Occ = вероятность появления × 10;
Sev = тяжесть последствий по шкале 1—10;
Det = вероятность необнаружения до поставки заказчику × 10;
APN = значение приоритетного действия = *Occ* · *Sev* · *Det*.

Рисунок В.5 — Часть процесса FMECA для подвергнутого машинной обработке алюминиевого бруска

Приложение С
(справочное)

Перечень сокращений на английском языке, используемых в стандарте

FMEA — метод анализа видов и последствий отказов;
FMECA — метод анализа видов, последствий и критичности отказов;
DFMEA — FMEA, применяемый для анализа проекта в автомобильной промышленности;
PRA — вероятностный анализ риска;
PFMEA — FMEA, применяемый для анализа процесса;
FTA — анализ дерева неисправностей;
RPN — значение приоритетности риска;
APN — значение приоритетности действий.

Библиография

[1] ГОСТ 27.002—89 — Надежность в технике. Основные понятия. Термины и определения (Industrial product dependability. General principles. Terms and definitions)

[2] МЭК 60300-3-11:1999 (IEC 60300-3-11:1999) — Менеджмент надежности. Часть 3. Прикладное руководство. Раздел 11. Техническое обслуживание, ориентированное на надежность (Dependability management — Part 3-11: Application guide — Reliability centred maintenance)

[3] SAE J1739:2000 — Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery

[4] AIAG — Potential Failure Mode and Effects Analysis, Third Edition, 2001

УДК 362:621.001:658.382.3:006.354 ОКС 13.110 Т58

Ключевые слова: анализ видов и последствий отказов, анализ видов, последствий и критичности отказов, отказ, резервирование, структура системы, вид отказа, критичность отказа

Редактор *Л.В. Афанасенко*
Технический редактор *Л.А. Гусева*
Корректор *М.С. Кабашова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 10.04.2008. Подписано в печать 16.06.2008. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 4,65. Уч.-изд. л. 3,90. Тираж 478 экз. Зак. 690.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru