Утвержден и введен в действие
Приказом Ростехрегулирования
от 30 сентября 2005 г. N 236-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ РИСКА

РУКОВОДСТВО ПО ПРИМЕНЕНИЮ МЕТОДОВ АНАЛИЗА НАДЕЖНОСТИ

IEC 60300-3-1:2003
Dependability management. Part 3-1.
Application quide. Analysis techniques for dependability.
Guide on metodology
(MOD)

Risk management. Guide for application
of analysis techniques for dependability

ГОСТ Р 51901.5-2005
(МЭК 60300-3-1:2003)

Группа Т58

ОКС 13.110;
ОКСТУ 0027

Дата введения
1 февраля 2006 года

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 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) 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 30 сентября 2005 г. N 236-ст.

4. Настоящий стандарт является модифицированным по отношению к международному стандарту МЭК 60300-3-1:2003 "Управление надежностью. Часть 3-1. Руководство по применению. Методы анализа надежности. Руководство по методологии" (IEC 60300-3-1:2003 "Dependability management - Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology") путем внесения технических отклонений, объяснение которых приведено в разделе "Введение" к настоящему стандарту.

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

Изменения, введенные в настоящий стандарт по отношению к международному стандарту, обусловлены необходимостью наиболее полного достижения целей национальной стандартизации.

5. Введен впервые.

Введение

Настоящий стандарт входит в группу стандартов по анализу и оценке рисков и дополняет ГОСТ Р 51901-2002 "Управление надежностью. Анализ риска технологических систем". В стандарте приведено описание методов анализа надежности, которые могут использоваться для определения оценок вероятностных характеристик риска.

Методы анализа надежности, описанные в настоящем стандарте, могут быть использованы для прогнозирования, исследования и улучшения надежности, работоспособности и ремонтопригодности объекта.

Эти исследования проводят на стадиях концепции и определения, проектирования, разработки, эксплуатации и технического обслуживания на различных уровнях системы и в условиях разной детализации проекта. Методы могут быть использованы для сопоставления результатов анализа с установленными требованиями.

Методы могут быть использованы проектными организациями, службами материально-технического обеспечения и технического обслуживания для оценки частоты замены составных частей и планирования технического обслуживания. Эти оценки часто определяют главные элементы стоимости жизненного цикла продукции и должны быть использованы при оценке стоимости жизненного цикла и в сравнительных исследованиях.

Для получения достоверных результатов в процессе анализа должны быть рассмотрены все возможные воздействия на надежность системы со стороны: аппаратных средств, программного обеспечения, человеческого фактора и организационных действий.

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 обслуживания", который нецелесообразно применять в национальном стандарте из-за отсутствия принятых гармонизированных национальных стандартов. В соответствии с этим изменено содержание раздела 2. Кроме того, содержание стандарта дополнено Приложением С, содержащим пояснения применяемых в тексте английских сокращений.

1. Область применения

Настоящий стандарт содержит краткий обзор часто используемых методов анализа надежности. В стандарте приведены описания основных методов и указаны их преимущества и недостатки, входные данные и другие условия использования.

Настоящий стандарт является введением в методологию анализа надежности и содержит необходимую информацию для выбора метода.

2. Нормативные ссылки

Настоящий стандарт содержит ссылки на следующие стандарты:

ГОСТ 27.310-1995. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения

ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь

ГОСТ Р 51901.11-2005 (МЭК 61882:2001). Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство

ГОСТ Р 51901.14-2005 (МЭК 61078:1991). Менеджмент риска. Метод структурной схемы надежности

ГОСТ Р 51901.15-2005 (МЭК 61165:1995). Менеджмент риска. Применение марковских методов.

Примечание. При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования - на официальном сайте национального органа Российской Федерации по стандартизации 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 замененным

(измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3. Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1. Элемент, объект (item, entity): любая часть, компонент, устройство, подсистема, функциональный модуль, оборудование или система, которая может быть рассмотрена как самостоятельная единица.

Примечание. Элемент может представлять собой аппаратное средство, программное обеспечение или и то и другое и может, в отдельных случаях, включать людей.

3.2. Система (system): совокупность взаимосвязанных и взаимодействующих элементов.
[ГОСТ Р ИСО 9000-2001]

Примечания. 1. С точки зрения надежности система должна иметь:

a) определенную цель, выраженную в виде требований к функционированию системы;

b) заданные условия эксплуатации.

2. Система имеет иерархическую структуру.

3.3. Компонент (component): элемент, рассматриваемый на самом низком иерархическом уровне при анализе системы.

3.4. Распределение (allocation): процедура, применяемая при проектировании элемента и направленная на распределение требований качества элемента по его компонентам в соответствии с заданным критерием.

3.5. Отказ (failure): прекращение способности элемента исполнять требуемую функцию.

Примечания. 1. После отказа элемент становится неисправным.

2. Отказ является событием в отличие от неисправности, которая является состоянием.

3.6. Неисправность (fault): состояние элемента, характеризующееся неспособностью исполнять требуемую функцию, исключая период технического обслуживания, ремонта или других запланированных действий, а также из-за недостатка внешних ресурсов.

Примечание. Неисправность часто является результатом отказа элемента, но может существовать и без предшествующего отказа.

4. Основные процедуры анализа надежности

4.1. Общая процедура

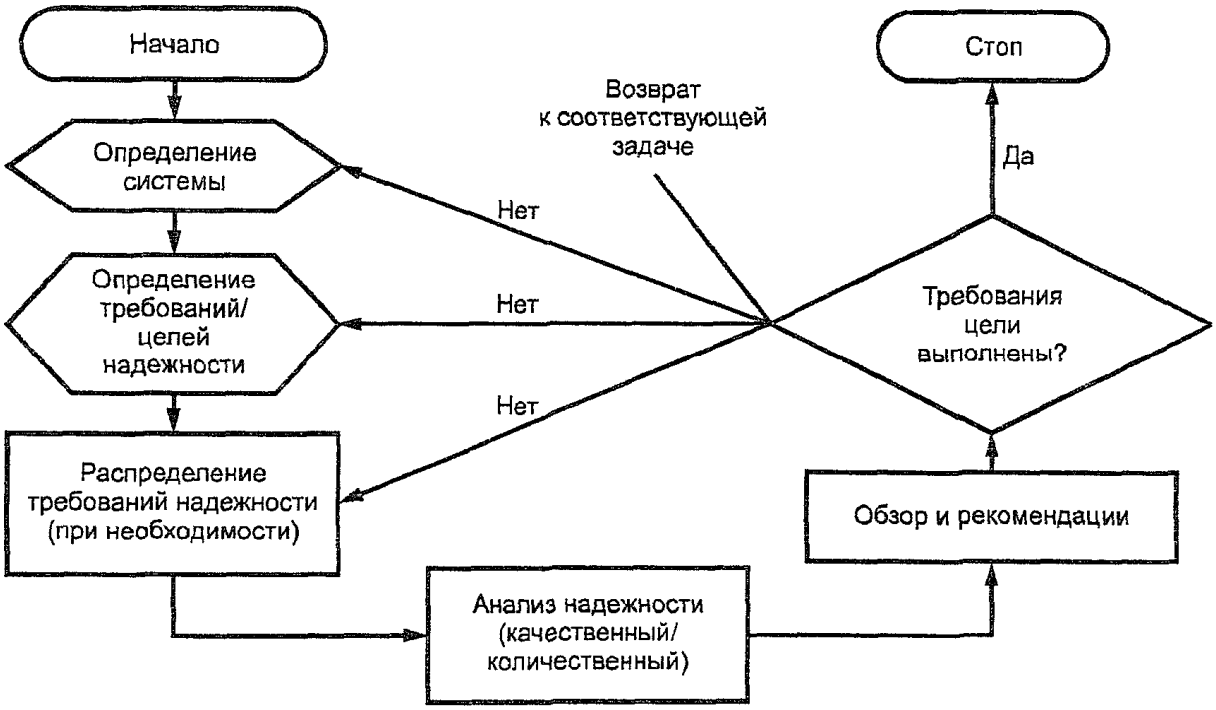


Рисунок 1. Общая процедура анализа надежности

Общая процедура анализа надежности представлена на рисунке 1 и состоит из следующих задач в порядке их применения:

a) Определение системы

Определение исследуемой системы, режимов и условий ее работы, функциональных связей, включая интерфейсы или процессы. Обычно результаты определения системы являются входом в процесс разработки системы.

b) Определение требований/целей надежности

Определение всех требований или целей надежности и работоспособности системы, а также характеристик и особенностей системы, режимов ее эксплуатации, условий окружающей среды и требований обслуживания. Определение отказа системы, критериев отказов и условий, основанных на функциональной спецификации системы, ожидаемой продолжительности и условий эксплуатации (циклограмма и время выполнения задания). При определении требований и целей надежности следует руководствоваться [1].

c) Распределение требований надежности

Распределение требований или целей надежности системы по различным подсистемам на ранней стадии проекта (при необходимости).

d) Анализ надежности

Анализ системы на основе методов надежности и соответствующих данных эффективности.

1) Качественный анализ:

- анализ функциональной структуры системы;
- определение режимов неисправностей системы и компонентов, механизмов отказов, причин и последствий отказов;
- определение механизма деградации, который может привести к отказу;
- анализ путей отказа/неисправности;
- анализ ремонтопригодности с учетом времени, метода изоляции и метода восстановления;
- определение адекватности методов диагностики неисправностей;
- анализ возможностей предотвращения неисправностей;
- определение стратегий технического обслуживания и ремонта.

2) Количественный анализ:

- разработка моделей надежности и/или эксплуатационной готовности;
- определение необходимых числовых данных;
- определение числовых оценок показателей надежности;
- проведение необходимого анализа критичности и чувствительности.

е) Исследования и рекомендации

Анализ выполнения целей требований надежности для рассматриваемого проекта и возможности их выполнения при использовании альтернативных проектов. Действия в этом направлении могут включать решение следующих задач:

- оценка улучшения надежности системы по результатам проектирования и производства (например, резервирование, снижение нагрузок, совершенствование стратегий технического обслуживания системы, контроля продукции и технологических процессов, системы менеджмента качества и материально-технической базы производства).

Примечание. Показатели надежности могут быть улучшены только в соответствии с проектом. Во многих случаях для повышения надежности необходимо усовершенствовать производственные процессы.

- исследование проекта системы и определение слабых мест и режимов критичности отказов компонентов;
- исследование проблем интерфейса системы, свойств и механизмов отказоустойчивости и т.д.;
- разработка альтернативных путей повышения надежности, например использование резервирования, контроля эффективности, обнаружения неисправностей, методов реконфигурации системы, процедур технического обслуживания, заменяемых компонентов, процедур восстановления;
- выполнение исследований по оценке стоимости и сложности альтернативных проектов;
- оценка влияния возможностей производственного процесса;
- оценка результатов и сравнение их с требованиями.

Примечание. Общая процедура объединяет некоторые элементы программы надежности, применимые для анализа надежности: спецификации надежности, анализ условий использования, разработка надежности, ремонтопригодности, человеческого фактора, моделирование надежности, анализ проекта и оценка продукции, анализ воздействия причин и анализ риска, анализ решений о заменах.

4.2. Методы анализа надежности

Методы, представленные в настоящем стандарте, относятся к двум основным группам:

- основные методы анализа надежности;
- общие технические методы, которые могут быть использованы как вспомогательные при проведении анализа надежности, а также при проектировании надежности.

Методы анализа надежности, используемые для решения общих задач анализа надежности, приведены в таблице 1, детальные характеристики методов приведены в таблице 2. Краткая характеристика методов приведена в Приложении А.

Таблица 1

Использование методов для решения
общих задач анализа надежности

Метод	Распределение требований/целей надежности	Качественный анализ	Количественный анализ	Рекомендации	Пункт Приложения А
Прогнозирование интенсивности отказов	Применим для последовательных систем без резервирования	Возможно применение для анализа стратегии технического обслуживания	Вычисление интенсивностей отказов и MTTF <*> для электронных компонентов и оборудования	Поддержка	A.1.1
Анализ дерева неисп-	Применим, если поведение системы зависит	Анализ комбинации неисправнос-	Вычисление показателей безотказности	Применим	A.1.2

равностей	от времени или последовательности событий	тей	работоспособности и относительного вклада подсистем в системы		
Анализ дерева событий	Возможен	Анализ последовательности отказов	Вычисление интенсивностей отказов системы	Применим	A.1.3
Анализ структурной схемы надежности	Применим для систем, у которых можно выделить независимые блоки	Анализ путей работоспособности	Вычисление показателей безотказности и комплексных показателей надежности системы	Применим	A.1.4
Марковский анализ	Применим	Анализ последовательности отказов	Вычисление показателей безотказности и комплексных показателей надежности системы	Применим	A.1.5
Анализ сети Петри	Применим	Анализ последовательности отказов	Подготовка описания системы для марковского анализа	Применим	A.1.6
Анализ режимов и последствий (критичности) отказов FME(C)A	Применим для систем, у которых преобладают единичные отказы	Анализ воздействия отказов	Вычисление интенсивностей отказов (и критичности) системы	Применим	A.1.7
Исследование HAZOP	Поддержка	Анализ причин и последствий отклонений	Не применим	Поддержка	A.1.8
Анализ человеческого фактора	Поддержка	Анализ воздействия действий эффективности человека на работу системы	Вычисление вероятностей ошибок человека	Поддержка	A.1.9
Анализ прочности и напряжений	Не применим	Применим как средство для предотвращения неисправности	Вычисление показателей безотказности для электромеханических компонентов	Поддержка	A.1.10
Табли-	Не применим	Возможен	Вычисление	Под-	A.1.11

ца истинности (анализ функциональной структуры)			показателей безотказности и комплексных показателей надежности системы	держка	
Статистические методы надежности	Возможен	Анализ воздействия неисправностей	Определение количественных оценок показателей безотказности с неопределенностью	Поддержка	A.1.12

<*> MTTF - средняя наработка до отказа.

Примечание. Слова-обозначения, принятые в таблице:
"применим" - метод рекомендован для решения задачи;
"возможен" - метод допускается использовать для решения задачи, учитывая, что он имеет некоторые недостатки по сравнению с другими методами;
"поддержка" - метод применим для некоторой части задачи и может использоваться для решения всей задачи только в комбинации с другими методами;
"не применим" - метод не допускается использовать для решения задачи.

Таблица 2

Характеристики методов анализа надежности

Метод	Подходит для сложных систем	Подходит для новых проектов	Количественный анализ	Подходит для комбинаций неисправностей	Подходит для обработки с учетом последовательности и зависимости событий	Может использовать зависимые события	Восходящий или нисходящий	Подходит для распределения надежности	Квалификация исполнителя	Применимость и унифицированность	Потребность в инструментах поддержки	Проверка правдоподобия результатов	Пригодность инструментальных средств	Обозначение стандарта
Прогнозирование интенсивности отказов	Нет	Да	Да	Нет	Нет	Нет	BU	Да	H	B	C	Да	B	[5]
Анализ дерева неисправностей (FTA)	Да	Да	Да	Да	Нет	Нет	TD	Да	C	B	C	Да	B	ГОСТ Р 51901.13
Анализ дерева событий (FTA)	NR	NR	Да	HR	Да	Да	BU	NR	B	C	C	Да	C	-
Анализ структурной схемы на-	NR	NR	Да	Да	Нет	Нет	TD	Да	H	C	C	Да	C	ГОСТ Р 51901.14

дежности (RBD)														
Марковский анализ	Да	Да	Да	Да	Да	Да	TD	Да	B	C	B	Нет	C	ГОСТ Р 51901.15
Анализ сети Петри	Да	Да	Да	Да	Да	Да	TD	Да	B	H	B	Нет	H	-
Анализ видов и последствий отказов (FMEA)	NR	NR	Да	Нет	Нет	Нет	BU	NR	H	B	H	Да	B	ГОСТ 27.310
Исследование HAZOP	Да	Да	Нет	Нет	Нет	Нет	BU	Нет	H	C	H	Да	C	ГОСТ Р 51901.11
Анализ надежности человеческого фактора (HRA)	Да	Да	Да	Да	Да	Да	BU	Нет	B	B	C	Да	C	-
Анализ нагрузок и напряжений	NA	NA	Да	NA	NA	Нет	NA	Нет	B	C	B	Да	C	-
Таблица истинности	Нет	Да	Да	Да	Нет	Нет	NA	Да	B	C	B	Нет	H	-
Статистические методы надежности	Да	Да	Да	Да	Да	Да	NA	NR	B	C	B	C	H	[6]

Примечание. Обозначения, принятые в настоящей таблице:
NR - может использоваться для анализа простых систем. Не рекомендуется использовать как автономный метод (только совместно с другими методами);
TD - нисходящий метод анализа;
BU - восходящий метод анализа;
NA - критерий не применим для этого метода;
B - высокий;
C - средний;
H - низкий.

Общие технические методы обычно включают:

- исследование ремонтопригодности по [2] и [3];
- анализ паразитных контуров схемы (A.2.1);
- анализ наихудшего случая (A.2.2);
- имитационное моделирование отклонений (A.2.3);
- разработку программного обеспечения по надежности (A.2.4);
- анализ конечных элементов (A.2.5);
- ограничение допустимых значений и выбор частей (A.2.6);
- анализ Парето (A.2.7);
- диаграмму причин и следствий (A.2.8);
- анализ отчета об отказах и систему корректирующих действий (A.2.9).

Следующие методы не выделены как самостоятельные, так как они являются модификацией упомянутых в таблице 1 методов анализа надежности:

- анализ причин/следствий - комбинация ETA и FTA;
- динамический FTA - расширение FTA, когда некоторые события представляются при помощи марковских моделей;
- функциональный анализ отказов - специальный вид FMEA;
- двоичные диаграммы решений, используемые главным образом для эффективного построения дерева неисправностей.

4.3. Распределение требований надежности

Определение требований надежности для подсистем является существенной частью проектирования системы. Цель распределения надежности - найти наиболее эффективную архитектуру системы, соответствующую требованиям надежности (технико-экономической

целесообразности). Распределение требований необходимо проводить для каждого показателя надежности. Поскольку методы распределения для всех показателей надежности одинаковы, далее в разделе использован термин "надежность".

Сначала (первый шаг) необходимо распределить требования надежности системы по подсистемам. При этом должны быть учтены сложность подсистем и опыт эксплуатации аналогичных подсистем. Если на начальном этапе проекта требования не выполнены, распределение и/или выполнение проекта необходимо повторить. Распределение требований надежности проводят с учетом анализа сложности, критичности, особенностей и условий эксплуатации системы.

Так как распределение требований надежности обычно проводят на раннем этапе проектирования, когда информация о системе отсутствует или ее очень мало, распределение необходимо периодически пересматривать.

Распределение требований по подсистемам и составным частям необходимо проводить на стадии определения. Это позволяет:

- проверить выполнение требований надежности для системы;
- установить в проекте выполнимые требования надежности для составных частей;
- установить четкие и поддающиеся проверке требования надежности для поставщиков.

Распределение требований надежности проводят в следующем порядке:

- анализируют систему и идентифицируют области, для которых разработан проект, а информация о значениях характеристик надежности доступна или может быть легко оценена;
- определяют соответствующие величины и их вклад в требования надежности системы. Разность между требованиями и фактическим уровнем надежности является частью требований надежности, которая должна быть распределена между другими составными частями системы.

Преимущества распределения требований надежности заключаются в том, что оно:

- обеспечивает путь совершенствования продукции за счет понимания соотношения между целями надежности системы и ее элементами (подсистемами, блоками, компонентами);
- рассматривает надежность наравне с другими характеристиками проекта, такими как эффективность и стоимость;
- определяет цели надежности для поставщиков;
- помогает оптимизировать надежность системы, поскольку рассматривает такие факторы как сложность, критичность, влияние условий эксплуатации.

Для распределения надежности существуют ограничения:

- часто предполагается, что элементы системы независимы, то есть отказ одного элемента не влияет на работу других элементов. Так как это предположение часто не выполняется, оно ограничивает область применения метода;
- распределение для систем с резервированием является более сложным. Для них рекомендуется использовать итеративные методы проверки выполнения целей надежности системы, например метод анализа дерева неисправностей.

4.4. Анализ надежности

4.4.1. Категории методов

Методы анализа надежности, описанные в Приложении А, классифицируют в соответствии с их главной целью по следующим категориям:

a) Методы для предотвращения неисправностей, например:

1) ограничение допустимых значений и выбор частей;

2) анализ прочности - напряжений.

b) Методы анализа архитектуры системы и распределения надежности. Например:

1) Восходящий метод (главным образом направленный на исследования последствий единичных неисправностей):

- анализ дерева событий (ETA);
- анализ видов и последствий отказов (FMEA),
- исследование опасности и удобства использования (HAZOP).

2) Нисходящие методы (исследующие последствия комбинаций неисправностей):

- анализ дерева неисправностей (FTA);
- марковский анализ;
- анализ сети Петри;
- таблица истинности (анализ функциональной структуры);
- анализ структурной схемы надежности (RBD).

c) Методы для оценки характеристик основных событий, например:

- прогнозирование интенсивности отказов;
- анализ надежности человеческого фактора (HRA);
- статистические методы надежности;
- программное обеспечение для проектирования надежности (SRE).

Методы различают также и по типу событий (зависимых или независимых), с которыми они работают. Результаты классификации перечисленных методов по этому признаку приведены на рисунке 2.

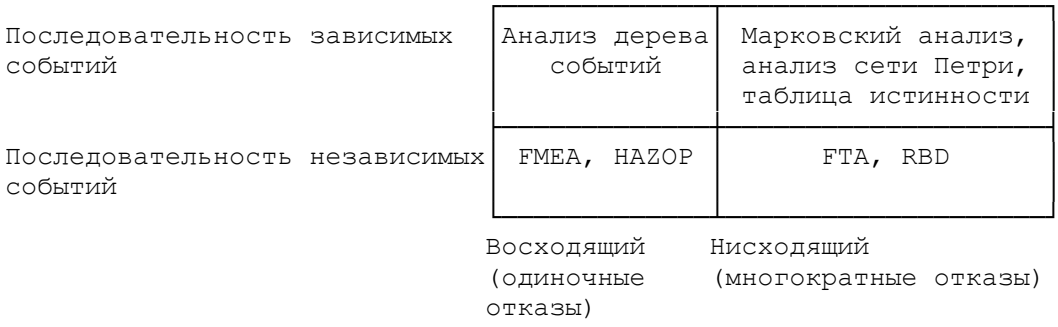


Рисунок 2. Схема классификации методов анализа надежности

Эти методы анализа применимы как для оценки характеристик качества, так и для оценок количественных характеристик при прогнозировании поведения системы в эксплуатации. Достоверность результата зависит от точности и правильности данных об основных событиях.

Однако ни один метод анализа надежности не может быть использован для всестороннего анализа реально существующих систем (аппаратных средств и программного обеспечения, систем со сложной функциональной структурой, систем с различными технологиями ремонта и технического обслуживания и т.д.). Для проведения анализа надежности сложных или многофункциональных систем, как правило, необходимо применять несколько дополнительных методов анализа.

На практике использование комбинаций нисходящего и восходящего анализов является весьма эффективным и позволяет обеспечить полноту анализа.

4.4.2. Восходящие методы

Начальным этапом любого восходящего метода является идентификация режимов отказов на соответствующем уровне. Для каждого режима отказа определяют его влияние на эффективность системы. Восходящий метод анализа надежности позволяет четко идентифицировать все режимы одиночных отказов, поскольку он опирается на списки частей системы или другие контрольные списки. На начальных этапах разработки анализ может быть качественным и иметь дело с функциональными отказами. Затем может применяться количественный анализ.

4.4.3. Нисходящие методы

На начальном этапе нисходящего метода определяют одиночное неблагоприятное событие или событие, обеспечивающее функционирование (успех) системы на самом высоком уровне (вершина событий). Затем идентифицируют и анализируют причины этого события на всех уровнях.

Нисходящий метод начинают с самого высокого уровня, то есть с анализа надежности в целом системы или подсистемы и последовательно спускаются на более низкий уровень.

Затем анализ проводят на следующем более низком уровне системы, идентифицируют все отказы и соответствующие режимы последствий. Этот процесс продолжают до тех пор, пока не достигнут самого низкого уровня. Нисходящий метод используют для оценки многократных отказов, включая последовательные зависимые отказы, при наличии неисправностей общей причины, а также для сложных систем.

4.5. Анализ технического обслуживания и ремонта

Эффективность ремонтируемой системы в большой степени зависит от ремонтопригодности системы, а также от стратегии и методов технического обслуживания и ремонта. При необходимости продолжительного функционирования системы эффективным мероприятием по обеспечению работоспособности системы является оценка влияния на надежность системы мероприятий по ее техническому обслуживанию и ремонту. Надежность является эффективным показателем функционирования в тех случаях, когда требуется обеспечение непрерывного функционирования

системы.

Ремонт системы в процессе эксплуатации без прерывания ее функционирования обычно возможен только для системы с избыточной структурой. В этом случае возможность восстановления или замены увеличивает показатели безотказности и работоспособности системы.

Обычно для оценки аспектов ремонта и технического обслуживания системы проводят специальный анализ по [2] - [4].

5. Выбор метода анализа надежности

Выбор метода анализа для программы надежности является очень индивидуальным и осуществляется объединенными усилиями экспертов по надежности и эксплуатации системы. Выбор должен быть сделан на ранних этапах разработки программы и исследован на применимость.

При использовании следующих критериев выбор методов может быть упрощен:

a) сложность системы. Сложные системы, например, включающие резервирование или другие особенности, обычно требуют более глубокого уровня анализа, чем простые системы;

b) новизна системы. Вновь разрабатываемая система требует более тщательного анализа, чем разработанная ранее;

c) качественный или количественный анализ. Действительно ли количественный анализ необходим?

d) единичные или многократные неисправности. Существенно ли влияние комбинации неисправностей или ими можно пренебречь?

e) поведение системы зависит от времени или последовательности событий. Имеет ли значение для анализа последовательность событий (например, система отказывает только в случае, если событию A предшествует событие B, но не наоборот) или поведение системы зависит от времени (например, ухудшение режимов работы после отказа или выполнения функции)?

f) возможность использования метода для зависимых событий. Зависят ли характеристики отказа или восстановления отдельного элемента системы от состояния системы в целом?

g) восходящий или нисходящий анализ. Обычно применение восходящих методов является более простым. Применение нисходящих методов требует осмысления и творческого подхода и имеет больше возможностей для ошибок;

h) распределение требований надежности. Может ли метод быть приспособлен к количественному распределению требований надежности?

i) квалификация исполнителя. Какой требуется уровень образования или опыта для правильного применения метода?

j) применимость. Например, регулирующая сторона или заказчик обычно применяет метод?

k) необходимость инструментальной поддержки. Нуждается ли метод в компьютерной поддержке или он может быть выполнен вручную?

l) проверки правдоподобия. Можно ли проверить правдоподобие результатов вручную? Если нет, являются ли инструментальные средства доступными?

m) работоспособность инструментальных средств. Действительно ли инструментальные средства доступны? Имеют ли эти инструментальные средства общий интерфейс с другими инструментальными средствами анализа, чтобы результаты могли многократно использоваться или передаваться?

n) стандартизация. Существует ли стандарт, устанавливающий требования к представлению его результатов?

В таблице 2 приведен краткий обзор различных методов анализа надежности, их характеристик и особенностей. Для полного анализа системы может потребоваться применение нескольких методов.

Приложение A
(справочное)

КРАТКОЕ ОПИСАНИЕ МЕТОДОВ АНАЛИЗА НАДЕЖНОСТИ

А.1. Основные методы анализа надежности

А.1.1. Прогнозирование интенсивности отказов

А.1.1.1. Описание и цель

Прогнозирование интенсивности отказов является методом, который применяют главным образом на ранних стадиях проектирования для оценки интенсивности отказов оборудования и системы. Он может быть использован также на стадии производства при необходимости улучшения количества продукции.

Для прогнозирования используют один из трех основных методов:

- метод прогнозирования интенсивности отказов в исходных условиях, называемый количественным анализом частей;

- метод прогнозирования интенсивности отказов в эксплуатационных режимах, называемый анализом напряжений частей;

- метод прогнозирования интенсивности отказов, использующий анализ подобия.

Выбор метода зависит от объема имеющейся информации о системе, а также от необходимой точности аппроксимации.

А.1.1.2. Прогнозирование интенсивности отказов в исходных условиях и прогнозирование интенсивности отказов в эксплуатационных режимах

В этих случаях необходимо знать количество и тип компонентов, входящих в систему, а также параметры эксплуатационных режимов, для которых проводится прогнозирование интенсивности отказов. Если параметры эксплуатационных режимов для компонентов совпадают с параметрами исходных условий, то записи об эксплуатационных режимах не делают. Однако, если параметры эксплуатационных режимов отличаются от параметров исходных условий, то принимают во внимание используемые условия и режимы для компонента (электрические, тепловые, окружающей среды и т.п.). Для этого должны быть использованы специально разработанные модели. Для точного прогноза необходима надежная база данных интенсивности отказов. В МЭК 61709 [5] даны рекомендации как установить интенсивность отказов в исходных условиях (этот стандарт не содержит данных об интенсивности отказов). Необходимые вычисления могут занять много времени, поэтому рекомендуется применять соответствующие программные средства.

Прогнозирование интенсивности отказов основано на следующих предположениях:

- компоненты соединены в системе последовательно (то есть отказ каждого компонента приводит к отказу системы);

- интенсивность отказов каждого компонента постоянна;

- отказы компонентов являются независимыми.

Эти предположения относительно исследуемой системы должны быть тщательно рассмотрены, так как ошибочное использование метода может привести к появлению опасных ошибок.

Предположение, что интенсивности отказов компонентов являются постоянными, сокращает количество вычислений, так как в этом случае интенсивность отказов системы является суммой интенсивностей отказов компонентов. Интенсивность отказов системы не всегда является значимой характеристикой надежности системы, поскольку не все отказы воздействуют на систему одинаково. Отказы диагностических элементов и некоторые режимы неисправностей могут не влиять на функционирование системы. В этом случае интенсивность отказов системы является лишь мерой количества корректирующих действий технического обслуживания, независимо от того, связаны они с отказами системы или нет.

Точность прогноза характеристик надежности системы зависит от доступных моделей отказов компонентов. Все вышеуказанное относится также к прогнозированию интенсивности отказов в эксплуатационных режимах.

А.1.1.3. Прогнозирование интенсивности отказов с использованием анализа подобия

Анализ подобия включает использование для прогнозирования надежности данных эффективности оборудования при эксплуатации для сравнения характеристик вновь разработанного оборудования с характеристиками оборудования-прототипа.

Сравнения характеристик аналогичного оборудования могут быть сделаны на уровне элемента, подсистемы или компонента. При этом используют одни и те же данные эксплуатации, но применяют различные алгоритмы и расчетные коэффициенты. Сопоставляемые элементы могут включать:

- условия эксплуатации окружающей среды (измеренные и заданные);

- характеристики проекта;

- процессы проекта;
- процессы обеспечения надежности;
- процессы производства;
- процессы технического обслуживания;
- компоненты и материалы.

Для каждого вышеупомянутого элемента необходимо сопоставлять все их характеристики. Например, условия эксплуатации и условия окружающей среды могут включать установившуюся температуру, влажность, температурные изменения, электрическую мощность, цикл режима работы, механическую вибрацию и т.д. Характеристики проектируемого оборудования могут включать количество компонентов, количество монтажных плат, схемы, размеры, массу, материалы и т.д.

Анализ подобия включает необходимые алгоритмы или расчетные методы для определения количества подобий и различий между исследуемым оборудованием и оборудованием-прототипом.

Анализ подобия элемента применяют в случае, когда оборудование-прототип имеет различия или недоступно для сравнения с вновь разработанным исследуемым оборудованием. Анализ подобия элемента - это структурированное сравнение элементов нового оборудования с подобными элементами ряда различных прототипов оборудования, для которых имеются данные надежности.

А.1.1.4. Достоинства:

- если имеются соответствующие данные, время и стоимость анализа будут очень небольшими;
- анализ адаптирован к ранним этапам проектирования и разработки, поскольку для него достаточно небольшого количества входной информации и данных;
- основная информация о надежности компонента получена на ранних этапах проектирования и разработки;
- метод адаптирован как к ручному, так и к компьютерному вычислениям;
- применение метода не требует специального обучения.

А.1.1.5. Ограничения:

- метод не применяют для систем с резервированием;
- из-за недостатка исходной информации уровень точности прогноза может быть низким, особенно для небольших подсистем и производств (для повышенной точности требуются большие выборки);
- оценка режимов и последствий отказов невозможна.

А.1.1.6. Стандарты

Применяют МЭК 61709 [5].

А.1.1.7. Пример для интегральной схемы (см. [5])

Для биполярной оперативной памяти интенсивность отказов в следующих исходных условиях $\lambda_{ref} = 10^{-7}$ ч$^{-1}$:

- температура окружающей среды: $\theta_{amb,ref}$ - 40 °С;
- самонагрев - 20 °С.

Каким будет значение интенсивности отказов при температуре окружающей среды $\theta_{amb,ref}$ = 70 °С с тем же значением самонагрева?

Шаг 1: Модель интенсивности отказов в эксплуатационных режимах определяют по формуле

$$\lambda = \lambda_{ref} \pi_T ,$$

где π_T - коэффициент температурного влияния.

Шаг 2: Из рисунка А.1 следует, что коэффициент температурного влияния π_T = 3,4.

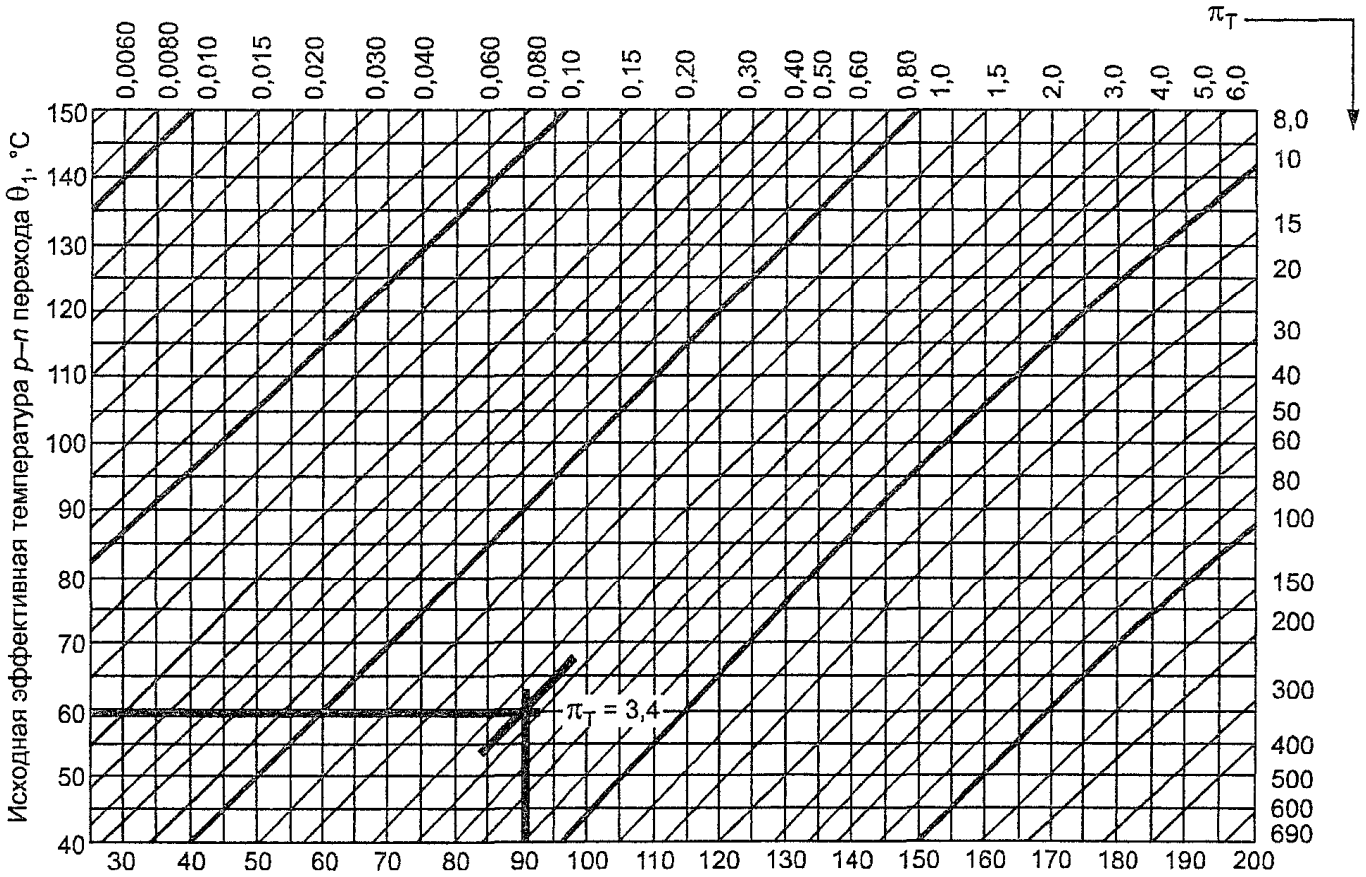

π_T
0,0060
0,0080
0,010
0,015
0,020
0,030
0,040
0,060
0,080
0,10
0,15
0,20
0,30
0,40
0,50
0,60
0,80
1,0
1,5
2,0
3,0
4,0
5,0
6,0
8,0
10
15
20
30
40
50
60
80
100
150
200
300
400
500
600
690
Исходная эффективная температура p–n перехода θ_1, °C
150
140
130
120
110
100
90
80
70
60
50
40
π_T = 3,4
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200

Рисунок А.1. Зависимость интенсивности отказов
от температуры

Используя значение исходной температуры и фактическую температуру, определяем:

$$\theta_1 = \theta_{amb,ref} + \Delta T_{ref} = 40\,°C + 20\,°C = 60\,°C;$$

$$\theta_2 = \theta_{amb} + \Delta T_{ref} = 70\,°C + 20\,°C = 90\,°C.$$

Шаг 3: Интенсивность отказов для θ_{amb} = 70 °С определяем по формуле, указанной для шага 1

$$\lambda = \lambda_{ref}\,\pi_T = 3,4 \cdot 10^{-7}\ \text{ч}^{-1}.$$

А.1.2. Анализ дерева неисправностей

А.1.2.1. Описание и цель

Анализ дерева неисправностей (FTA) является нисходящим методом анализа надежности продукции. Он предназначен для идентификации и анализа условий и факторов, которые вызывают или способствуют появлению нежелательного результата и влияют на эффективность, безопасность, экономичность и другие характеристики системы.

FTA может использоваться для построения модели прогнозирования надежности, а также при проведении альтернативных исследований на стадии проектирования продукции.

FTA применяют для определения количественных оценок, характеризующих причины неисправности. FTA является эффективным методом, который идентифицирует и оценивает режимы отказов и причины известных или предполагаемых воздействий.

FTA позволяет учесть известные неблагоприятные воздействия и находить соответствующие режимы и причины отказов. FTA способствует своевременному смягчению потенциальных режимов отказов и повышению надежности продукции на стадии проектирования.

FTA позволяет представить аппаратную и программную функциональные структуры системы, работает с основными событиями и является методом моделирования надежности. FTA учитывает сложные взаимодействия частей системы, моделируя их функциональные зависимости или зависимости отказов, события, вызывающие отказ, общие причины событий и позволяет сформировать общее представление о системе.

Для оценки показателей надежности и работоспособности системы с помощью FTA применяют такие методы, как Булевы сокращения и анализ набора вырезок. Основными исходными данными метода являются интенсивности отказов, интенсивности восстановления, вероятности появления режимов неисправностей для компонентов.

А.1.2.2. Применение

Анализ дерева неисправностей имеет двойное применение: как способ идентификации причины известного отказа и как метод анализа режима отказа, моделирования и прогнозирования надежности.

FTA используют для исследования потенциальных неисправностей, их режимов и причин для определения количественной оценки их вклада в отказ системы при проектировании. Дерево неисправностей создают, чтобы представить не только функции системы, но также и ее аппаратные средства, программное обеспечение и их взаимодействие. Если человек является частью системы, человеческие ошибки могут быть включены в FTA. Вероятность появления причин режимов неисправностей определяют с помощью технического анализа и затем используют для оценки величины их вклада в состояние полной неработоспособности системы. При этом допускают возможность изменений и повышения надежности. FTA позволяет моделировать надежность комбинации аппаратных, электронных и механических средств и программного обеспечения, а также их взаимодействие. Таким образом, FTA является мощным инструментом анализа надежности системы.

А.1.2.3. Ключевые элементы

Ключевые элементы дерева неисправностей:

- клапаны и события,

- наборы вырезок.

Клапаны представляют собой результат, а события - вход в клапан. Символически представление некоторых конкретных клапанов может изменяться в процессе решения разных задач. Однако представление основных клапанов довольно универсально.

Наборы вырезок представляют собой группы событий, возникновение которых вызывают отказ системы. Минимальные наборы вырезок содержат минимальное количество событий, которые необходимы для отказа системы. При удалении одного события отказ системы не происходит.

А.1.2.4. Достоинства:

- разработка может быть начата на ранних стадиях проектирования и затем разрабатываться более подробно одновременно с развитием проекта;

- идентифицирует и систематически регистрирует логические пути неисправности от их появления до основных причин при помощи Булевой алгебры;

- допускает простое преобразование логических моделей в соответствующие вероятностные характеристики.

А.1.2.5. Ограничения:

- позволяет представить события, зависящие от времени или последовательности их появления;

- имеет ограничения относительно реконфигурации системы и систем, функционирование которых зависит от их состояния.

Эти ограничения можно устранить, применяя FTA в комбинации с марковскими моделями, если марковские модели применяются для основных событий дерева неисправностей.

А.1.2.6. Пример

Дерево неисправностей аудиоусилителя изображено на рисунке А.2. Верхним уровнем дерева неисправностей системы для аудиоусилителя являются клапаны входа на клапан вершины (главные подсистемы).

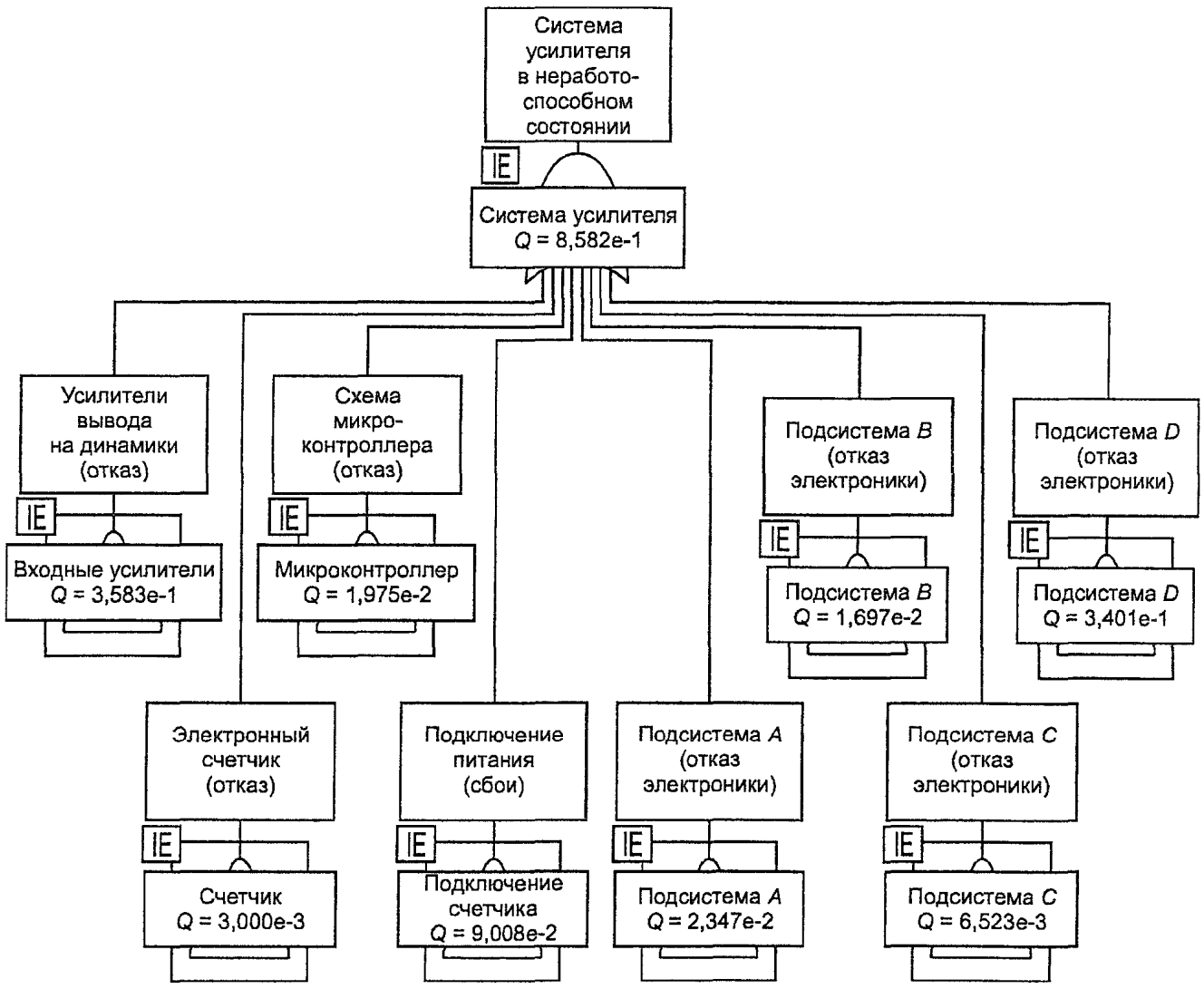


Рисунок А.2. Дерево неисправностей для аудиоусилителя

Наибольший вклад в общий отказ вносит ветвь дерева неисправностей, изображенная на рисунке А.3.

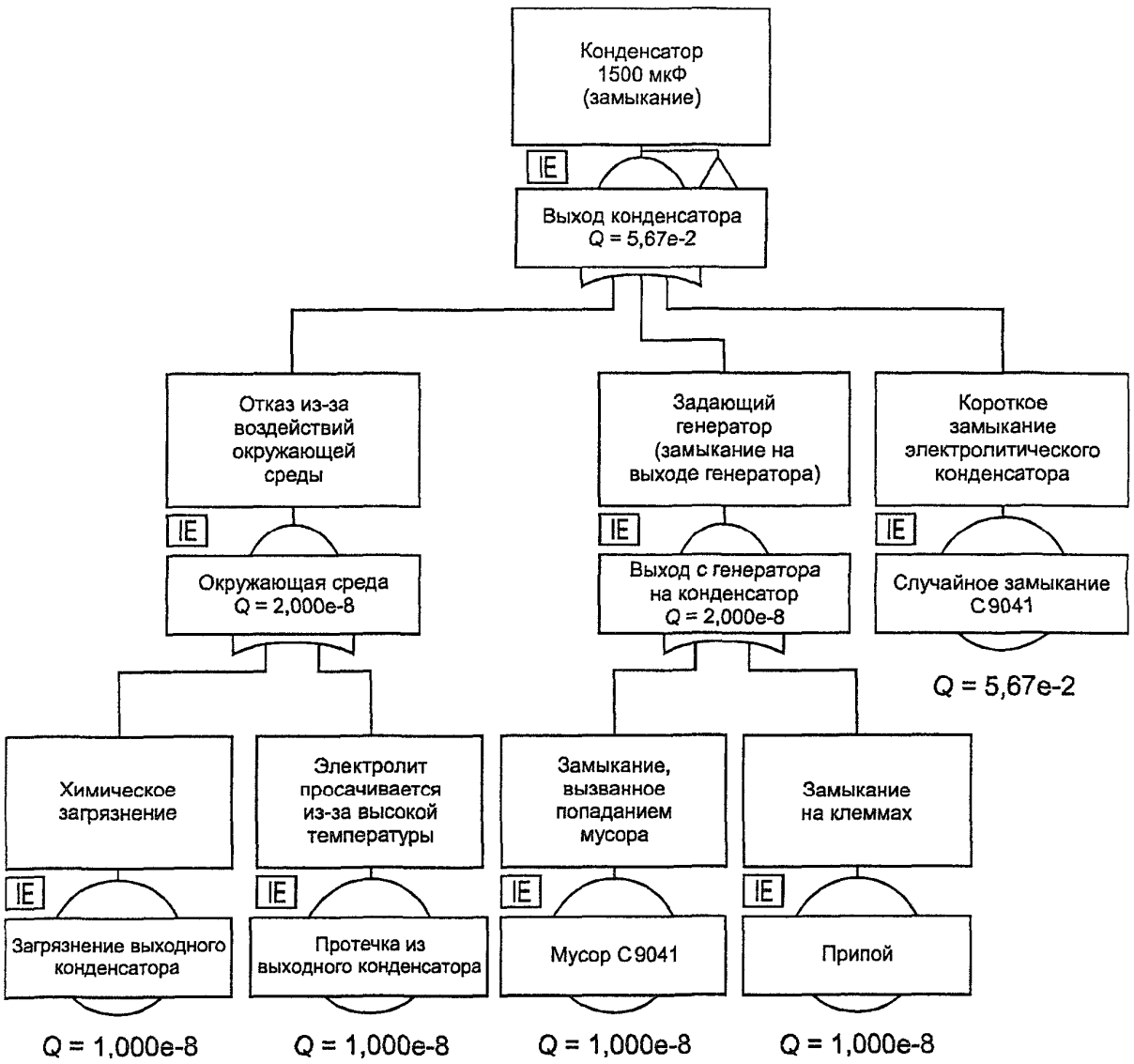
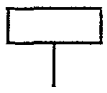
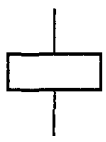
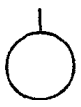
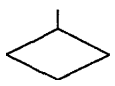
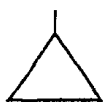


Рисунок А.3. Подсистема дерева неисправностей
(см. рисунок А.2)

При изображении дерева неисправностей используют символы, приведенные в таблице А.1.

Таблица А.1

Символы, используемые при изображении дерева неисправностей

Символ	Наименование символа	Описание символа
	Вершина событий	Вершина событий, соответствующая неисправности системы
	Промежуточное событие	Промежуточное событие, соответствующее неисправности более высокого уровня, чем события основного уровня
	Основное событие	Основное событие, для которого имеется информация о надежности
	Неразработанное событие	Часть системы, которая не разработана
	Клапан перехода	Клапан, указывающий, что эта часть системы разрабатывается в другой части или на другой странице диаграммы
	Клапан ИЛИ	Событие выхода происходит, если происходят все события входа одновременно
	Клапан И	Событие выхода происходит, если происходят все входные события одновременно

Цель данного анализа - найти наиболее вероятную причину отказа усилителя. В процессе анализа выяснилось, что самый высокий вклад в отказ усилителя вносит электролитический конденсатор, расположенный на выходе усилителя на динамик. Существует высокая вероятность короткого замыкания этого конденсатора. Это является следствием выбора конденсатора с более низким напряжением из-за его меньших габаритов. В результате понижение емкости этого конденсатора составило 90%. Короткое замыкание является только дополнительной причиной отказа конденсатора.

Обе причины привели к увеличению количества отказов конденсатора. Исходная интенсивность отказов электролитического конденсатора (1500 мкФ) не является низкой. Конденсатор был заменен на конденсатор с соответствующим напряжением, что уменьшило вероятность отказа усилителя за срок службы больше чем на 20%. В результате этого повысилась надежность системы.

В этом случае показатель неработоспособности системы Q, рассчитанный для заданного времени эксплуатации, представляет собой вероятность отказа системы F(t), так как ремонт не допускался.

В этом примере использовались стандартные клапаны, кроме клапанов подсистем, у которых треугольник указывает, что клапаны будут разработаны позже, а квадрат вокруг них указывает, что каждый из них показан на отдельной странице.

А.1.3. Анализ дерева событий

А.1.3.1. Описание и цель

Анализ дерева событий (ETA) распространяется на ряд возможных последствий реализации события или отказа системы. Эффективным может быть соединение дерева событий с деревом неисправностей. Корень дерева событий может быть вершиной дерева неисправностей. Эта комбинация иногда называется анализом причины и следствий, в котором FTA используют для анализа причин, а ETA - для анализа последствий реализации события. Чтобы оценить серьезность последствий, которые следуют за реализацией события, необходимо идентифицировать, исследовать и определить вероятность всех возможных последствий.

А.1.3.2. Применение

Анализ дерева событий применяют в тех случаях, когда необходимо исследовать все возможные пути формирования событий, последовательность их появления и наиболее вероятные результаты или последствия. После начального события может произойти несколько следующих событий/следствий. Вероятность, связанная с реализацией определенного пути (последовательности) событий, равна произведению условных вероятностей всех событий на этом пути.

А.1.3.3. Ключевые элементы

Ключевыми элементами применения ETA являются инициатор (первоначальное событие), последующие события и их последствия.

А.1.3.4. Преимущества

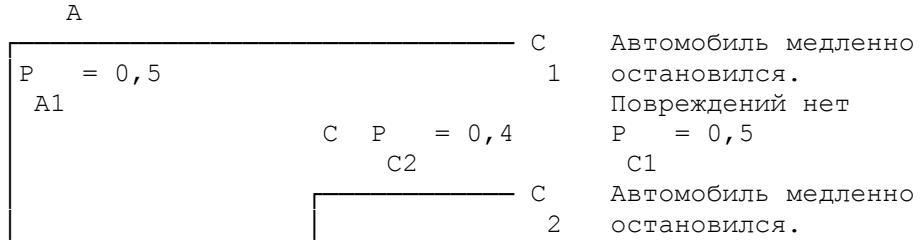
Главным преимуществом применения анализа дерева событий является возможность оценить последствия событий и таким образом способствовать снижению высокой вероятности неблагоприятного последствия. Анализ дерева событий является хорошим дополнением анализа дерева неисправностей. Анализ дерева событий может быть также использован при анализе режимов отказов. В этом случае анализ прослеживает возможные пути события (режимов отказа), чтобы определить вероятные последствия отказа.

А.1.3.5. Ограничения

Анализ дерева событий необходимо проводить с особой осторожностью при работе с условными вероятностями и независимыми событиями.

А.1.3.6. Пример

Пример анализа простого дерева событий приведен на рисунке А.4. В примере рассмотрено событие отказа автомобильной шины и приведено несколько возможных результатов.



A - без материального ущерба или травмы;
B - материальный ущерб, без травмы; C - повреждение автомобиля без другого материального ущерба.

Рисунок А.4. Дерево событий

А.1.4. Анализ структурной схемы надежности

А.1.4.1. Описание и цель

Метод анализа структурной схемы надежности (RBD) является методом анализа надежности системы. RBD является графическим изображением представления логической схемы системы через подсистемы и/или компоненты и позволяет изобразить пути успеха работоспособности системы в виде логических связей подсистем/компонентов.

А.1.4.2. Применение

Метод анализа RBD применяют на стадии определения продукции. Структурная схема надежности системы должна быть создана в начале разработки концепции. Разработка RBD должна начинаться сразу после завершения определения программы, как часть анализа требований, и непрерывно расширяться до более глубокого уровня детализации по мере увеличения данных для принятия решений.

А.1.4.3. Ключевые элементы

Для разработки RBD могут быть использованы следующие методы анализа:

- определение исправного состояния системы;

- разделение системы на функциональные блоки в соответствии с целями анализа надежности. Некоторые блоки могут представлять собой подсистемы, для которых могут быть разработаны свои RBD;

- проведение качественных исследований.

Количественные оценки по RBD проводят различными методами. В зависимости от типа структуры системы (с восстановлением или без восстановления) могут быть использованы простые Булевы методы, таблицы истинности и/или анализ путей и вырезок для прогнозирования показателей надежности и работоспособности системы, рассчитываемых на основе данных компонентов.

А.1.4.4. Достоинства:

- структурную схему надежности часто создают непосредственно по функциональной диаграмме системы. Это позволяет сократить количество конструктивных ошибок и/или систематическое описание функциональных путей системы;

- пригоден для многих типов конфигурации системы, включая параллельные, избыточные, резервные и альтернативные функциональные пути;

- пригоден для полного анализа вариантов при изменении параметров эффективности системы;

- позволяет получить простые логические модели путей функционирования и отказа системы (например, используя Булеву алгебру);

- пригоден для анализа вклада элементов в надежность системы;

- позволяет строить модели оценки вероятностных характеристик надежности и работоспособности системы;

- дает компактные результаты вероятностных характеристик для системы в целом.

А.1.4.5. Ограничения:

- не обеспечивает полный анализ неисправностей, то есть пути причина-следствие или следствие-причина не определяются;

- требует наличия вероятностной модели эффективности для каждого элемента диаграммы;

- не позволяет различать преднамеренные и непреднамеренные результаты, если аналитик не предусматривает для того специальных действий;

- направлен прежде всего на анализ работоспособности системы и не распространяется на сложные стратегии ремонта, технического обслуживания или общий анализ работоспособности;

- имеет те же ограничения, что и у методов, применяемых для анализа невосстанавливаемых систем.

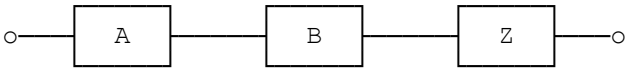
А.1.4.6. Стандарты

Применяют ГОСТ Р 51901.14.

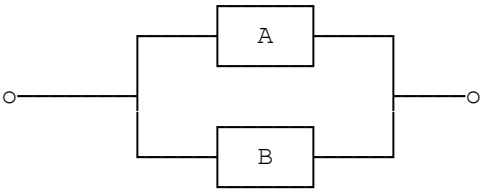
А.1.4.7. Пример

Простые RBD независимых блоков изображены на рисунке А.5.

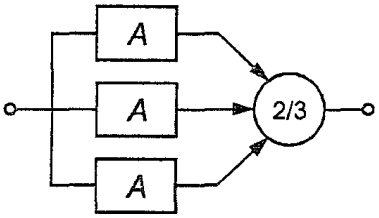
Последовательная модель



Параллельная модель (нагруженный резерв)



Модель m из n



Ненагруженный резерв

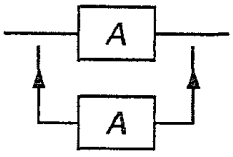


Рисунок А.5. RBD для независимых блоков

Более сложные модели, в которых один и тот же блок может появляться в схеме несколько раз, могут быть оценены при помощи:

- теоремы полной вероятности;

- Булевых таблиц истинности.

А.1.5. Марковский анализ

А.1.5.1. Описание и цель

Марковское моделирование - вероятностный метод, который учитывает статистическую зависимость отказов или характеристики ремонта отдельных компонентов для описания состояния системы. Следовательно, марковское моделирование может учитывать как воздействие независимых отказов компонентов, так и интенсивности перехода состояний под воздействием напряжений или других факторов. По этой причине марковский анализ применяют для оценки надежности функционально сложных систем со сложными стратегиями ремонта и технического обслуживания.

Метод основан на теории марковских процессов. Для прикладных задач надежности обычно используют гомогенную во времени марковскую модель, которая предполагает, что интенсивности переходов (отказ и ремонт) являются постоянными. Для этой модели применимы простые и эффективные численные методы решения и единственное ограничение его применения - размерность пространства состояний.

Представление поведения системы с помощью марковской модели требует определения всех возможных состояний системы, предпочтительно изображенных на диаграмме состояний и переходов. Кроме этого, должны быть определены (постоянные) интенсивности перехода из одного состояния в другое (интенсивности отказа или ремонта, интенсивности события и т.д.). Выходами марковской модели являются вероятности пребывания системы в данном наборе состояний (обычно эта вероятность является показателем качества работы системы).

А.1.5.2. Применение

Этот метод применяют в случае, когда интенсивность перехода (отказ или ремонт) зависит от состояния системы, нагрузки или структуры системы (например, резервирования), стратегии технического обслуживания или других факторов. В частности, структура системы (тип резервирования, запасные части) и стратегии технического обслуживания (количество ремонтных бригад) выявляют зависимости, которые не могут быть получены другими методами.

Пример - Прогнозирование характеристик надежности/работоспособности.

А.1.5.3. Ключевые элементы

Метод состоит из следующих ключевых элементов:

- определения пространства состояний системы;

- назначения интенсивностей перехода состояний (постоянных во времени);

- определения характеристик выхода (группировка состояний, которые приводят к отказу системы);

- разработки математической модели (матрицы интенсивностей переходов) и решений марковских моделей для использования подходящего пакета программ;

- анализа результатов.

А.1.5.4. Преимущества

Применение метода дает следующие преимущества:

- обеспечивает гибкую вероятностную модель для анализа поведения системы;

- может быть адаптирован к сложным избыточным конфигурациям, сложной стратегии технического обслуживания, сложным моделям обработки неисправностей (неустойчивые неисправности, скрытые неисправности, реконфигурации), деградационным режимам работы и общим причинам отказов;

- дает вероятностные решения для модулей, которые будут использованы в других методах, таких как методы структурной схемы надежности и дерева неисправностей;

- позволяет точно моделировать последовательность событий определенного вида или порядка появления.

А.1.5.5. Ограничения:

- с увеличением количества компонентов системы количество состояний экспоненциально возрастает, что приводит к росту трудоемкости анализа;

- модель может быть трудна для пользователей при построении и контроле и требует соответствующего программного обеспечения для анализа;

- числовые результаты можно получить только для постоянных интенсивностей переходов;

- некоторые показатели, такие как средняя наработка на отказ и средняя наработка до отказа, не могут быть получены непосредственно из марковской модели.

А.1.5.6. Стандарты

Применяют ГОСТ Р 51901.15.

А.1.5.7. Пример

Электронное оборудование (далее - модуль) содержит функциональную часть F и диагностическую часть D, изображенные на рисунке А.6. Под термином "диагностика" далее будут

подразумеваться части системы, которые выполняют наблюдения, контроль и отображают их результаты на дисплее (аппаратные средства, программное обеспечение, программируемое оборудование).

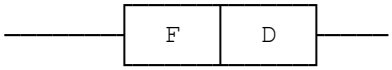


Рисунок А.6. Пример модуля

В данном примере используют также следующие термины с соответствующими определениями:

Дефект сигнала: неспособность диагностической части подавать сигнал о неисправности;

Неработоспособное состояние: состояние элемента, характеризуемое неисправностью или возможной неспособностью исполнять требуемую функцию в течение профилактического технического обслуживания;

Ложный сигнал: неисправность, обнаруженная встроенным тестовым оборудованием или другой схемой контроля, хотя в действительности неисправности нет;

Режим неисправности: одно из возможных состояний дефектного элемента для данной требуемой функции;

Доля неисправностей: доля неисправностей элемента, которая допускается в данных условиях;

Диагностика неисправности: действия, предпринятые для распознавания неисправности, локализации и идентификации причин;

Скрытая неисправность: существующая неисправность, которая еще не обнаружена;

Работоспособное состояние: состояние элемента, в котором он может исполнять требуемую функцию при наличии внешних ресурсов при необходимости.

На диаграмме изображают каждый функциональный блок в двух состояниях. Одно состояние соответствует работоспособному состоянию, а другое - неисправности (неработоспособное состояние). Модель двух состояний упрощает анализ надежности, но иногда не адекватно описывает реальные состояния системы, когда каждый функциональный блок имеет функциональную F и диагностическую D части, которые могут отказать. Такие ситуации рассматривают с помощью марковского анализа моделирования.

При применении марковского анализа вначале определяют пространство состояний системы. Определение состояния реального модуля и воздействие отказов функциональной и диагностической частей приведены в таблицах А.2 и А.3.

Таблица А.2

Состояния модуля

Обозначение состояния	Определение состояния
1	Правильная эксплуатация
2	Диагностическая ошибка; дефект сигнала
3	Функциональная неисправность, охваченная диагностикой
4	Функциональная неисправность, не охваченная диагностикой
5	Функциональная неисправность, не обнаруженная из-за отказа

	диагностики в режиме дефекта сигнала
6	Диагностическая ошибка; ложный сигнал

Таблица А.3

Воздействие отказов функциональной и диагностической частей

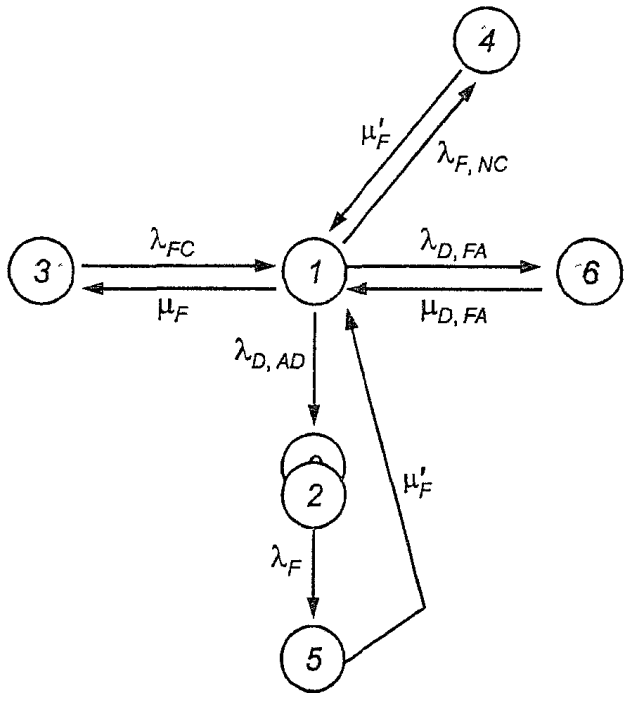
Состояние части F	Состояние части D	Обозначение состояния	Воздействие отказов
Работоспособное	Работоспособное	1	Корректная эксплуатация (состояние 1)
	Неисправность в режиме "ложный сигнал"	6	Есть сигнал. Часть F находится в работоспособном состоянии до тех пор, пока персонал по техническому обслуживанию не закончит ремонт. Если в части F нет избыточности, эксплуатацию этой части не прекращают во время ремонта (состояние 6)
	Неисправность в режиме "дефект сигнала"	2	Нет сигнала. Часть F находится в работоспособном состоянии (состояние 2) до тех пор, пока не откажет (состояние 5)
Неисправное	Работоспособное	3	Есть сигнал. Правильное распознавание неисправности (состояние 3)
	Неисправное	5	Последовательность событий, предшествующих этому состоянию: диагностическая неисправность

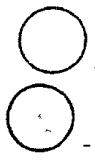
			(режим дефекта сигнала), подсистема приходит в состояние 2; функциональная неисправность; нет сигнала (состояние 5)
	Неизвестно	4	Необнаруживаемая неисправность (состояние 4)

На рисунке А.7 изображена диаграмма состояний и переходов. Она указывает на следующее:

- функциональная часть системы не может быть охвачена диагностикой; это означает, что отказ функциональной части не может быть обнаружен (состояние 4);

- диагностическая часть может подавать сигнал, когда он не нужен (состояние 6) или не может подавать сигнал, когда он нужен (состояния 2 и 5).




- работоспособное состояние;

- неработоспособное состояние

Рисунок А.7. Диаграмма состояний и переходов

Постоянные интенсивности перехода состояний указаны в таблице А.4.

Таблица А.4

Интенсивности перехода

Обозначение интенсивности перехода	Определение
λ_F	Интенсивность отказов функциональной части F
$\lambda_{F,C}$	Интенсивность отказов части F, обнаруживаемых с помощью диагностики
$\lambda_{F,NC}$	Интенсивность не обнаруживаемых с помощью диагностики отказов части F ($\lambda_F = \lambda_{F,C} + \lambda_{F,NC}$)
$\lambda_{D,AD}$	Интенсивность отказов части D в режиме дефекта сигнала
$\lambda_{D,AD}$	Интенсивность отказов части D в режиме ложного сигнала ($\lambda_D = \lambda_{D,AD} + \lambda_{D,FA}$)
μ_F	Интенсивность ремонта после неисправности, обнаруживаемой с помощью диагностики
μ'_F	Интенсивность ремонта после неисправности, обнаруживаемой с помощью диагностики
$\mu_{D,FA}$	Интенсивность ремонта после неисправности в режиме ложного сигнала

После построения диаграммы состояний и определения интенсивностей перехода коэффициент готовности можно рассчитать с помощью соответствующего пакета программ или провести параметрический анализ, рассматривающий разности интенсивностей перехода.

А.1.6. Анализ сети Петри

А.1.6.1. Описание и цель

Сеть Петри - графический метод представления и анализа сложных логических взаимодействий компонентов или событий в системе. Сеть Петри отражает такие сложные взаимодействия как конкуренция, конфликт, синхронизация, взаимное исключение и ограничение ресурса.

Статичная структура исследуемой системы может быть представлена графом сети Петри. Граф сети Петри состоит из трех примитивных элементов:

- мест (обычно изображаемых в виде кругов), которые представляют состояния системы;

- переходов (обычно изображаемых в виде линий), которые представляют события, после которых состояние системы изменяется;

- дуг (изображаемых в виде стрелок), которые подключают места к переходам, а переходы к местам и представляют логически допустимые подключения между состояниями и событиями.

Состояние допустимо в данной ситуации, если соответствующее место отмечено, по крайней мере, одним маркером, изображаемым в виде точки "•". Динамика системы представлена посредством движения маркеров в графе. Переход допускают, если его входные места содержат, по крайней мере, один маркер. Допускаемый переход может быть выполнен. При удалении перехода удаляют один маркер из каждого входного места и помещают один маркер в каждое место вывода. Правила постановки и удаления маркеров позволяют получить все достижимые маркировки, называемые набором достижимости сети Петри. Набор достижимости включает все состояния, в которые система может попасть из начального состояния.

Стандартные сети Петри не содержат понятия времени. Однако появилось много расширений в сети Петри, в которые добавлена синхронизация. Если интенсивность удаления (постоянная) действует при каждом переходе, динамика сети Петри может быть проанализирована посредством непрерывной марковской цепочки времен, пространство состояний которой изоморфно, с набором достижимости соответствующей сети Петри.

Сеть Петри может быть использована как язык высокого уровня для создания марковских моделей. Некоторые инструментальные средства анализа надежности основаны на этом методе.

Сети Петри обеспечивают также условия для моделирования.

А.1.6.2. Применение

Сеть Петри рекомендуется применять, когда должны быть учтены сложные логические взаимодействия (конкуренция, конфликт, синхронизация, взаимное исключение, ограничение ресурса), так как сеть Петри использует обычно более простой и естественный язык для описания марковской модели.

А.1.6.3. Ключевые элементы

Ключевой элемент сети Петри - описание структуры системы и ее динамического поведения с помощью примитивных элементов языка сети Петри (мест переходов, дуг и маркеров). Для применения элементов сетей Петри требуется использование специальных программ:

a) качественного анализа структуры;

b) количественного анализа (если постоянная интенсивность удаления назначена на переходы сети Петри, то количественный анализ может быть выполнен с помощью решения соответствующей марковской модели).

А.1.6.4. Достоинства

Сети Петри применяют в случаях, если необходимо представить сложные взаимодействия среди аппаратных или программных модулей, которые трудно описать другими методами.

Сети Петри являются хорошим средством разработки марковских моделей. Обычно описание системы посредством сети Петри требует значительно меньшего количества элементов, чем соответствующее представление.

Марковская модель автоматически может быть получена на основе сети Петри, а сложность процедуры аналитического решения будет скрыта от разработчика, который работает только на уровне сети Петри.

Кроме того, сети Петри позволяют проводить качественный анализ структуры, основанный только на свойствах графа. Этот структурный метод анализа является более дешевым, чем построение марковской модели, и обеспечивает необходимой информацией для ее проверки и утверждения.

А.1.6.5. Ограничения

Так как количественный анализ основан на разработке и решении соответствующей марковской модели, большинство ограничений те же, что и для марковского анализа.

Методология сети Петри требует использования программных средств, разработанных квалифицированными специалистами.

А.1.6.6. Пример

Устойчивая к ошибкам мультипроцессорная компьютерная система, структурная схема которой изображена на рисунке А.8, содержит две независимые подсистемы S_1 и S_2 с общей памятью МЗ.

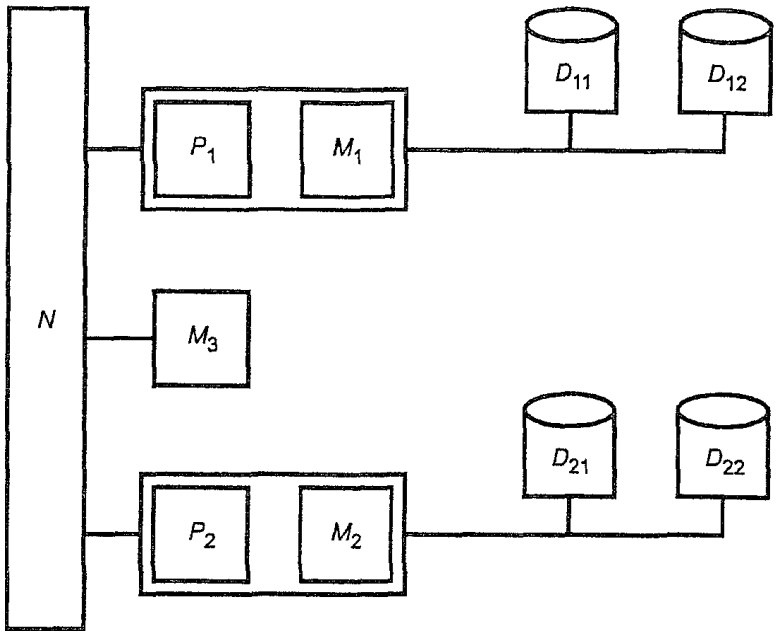


Рисунок А.8. Структурная схема мультипроцессора

Каждая подсистема S_i (i = 1; 2) состоит из одного процессора P, одной локальной памяти M и двух дисковых модулей D_{i1} и D_{i2}. Шина N соединяет эти две подсистемы и общую память.

Общая стохастическая сеть Петри системы, представленной на рисунке А.8, изображена на рисунке А.9.

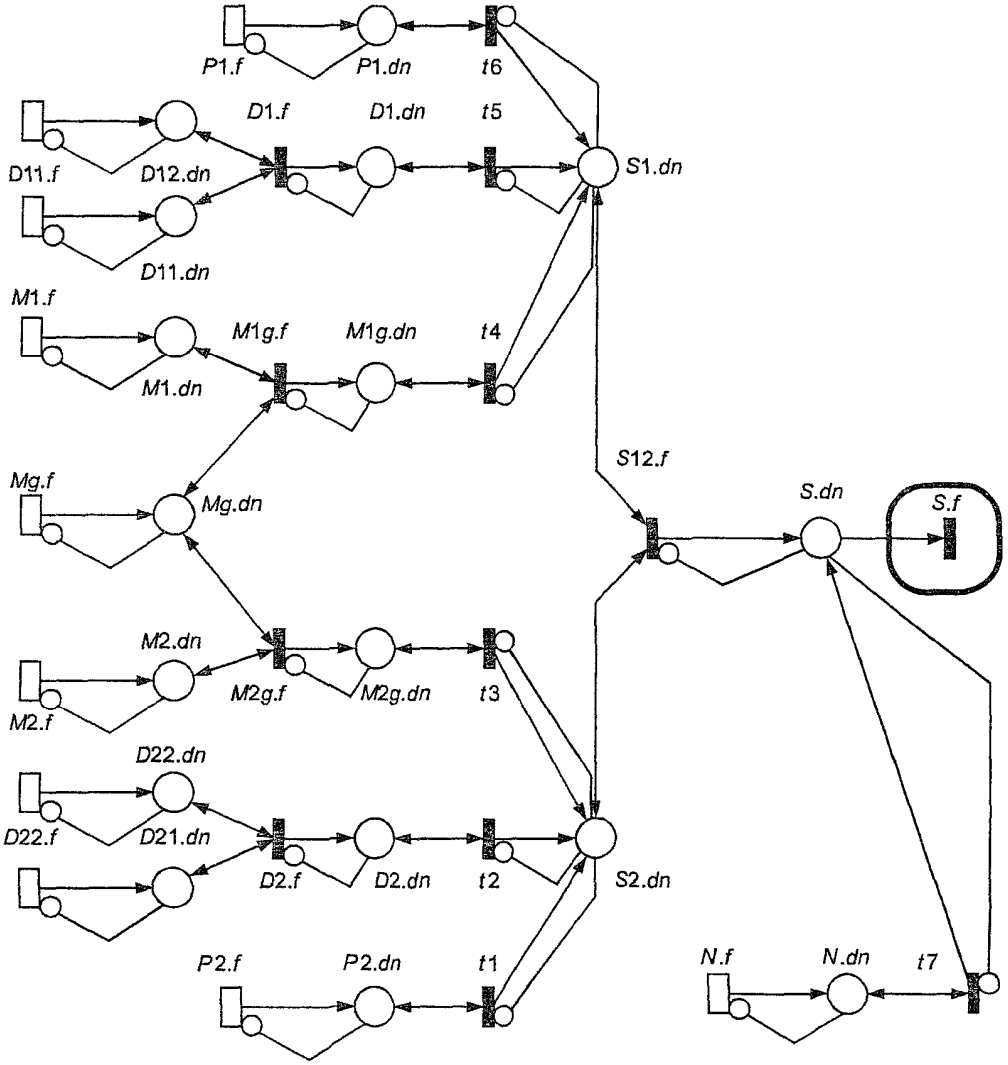


Рисунок А.9. Сеть Петри мультипроцессорной системы

Места со знаком "dn" соответствуют компонентам в неработоспособном состоянии.

Маркер "S.dn" отражает полный отказ системы.

Переходы со знаком "f" в обозначении соответствуют отказу компонента.

Такая маркировка сети Петри представляет мультипроцессор с компонентами, находящимися в работоспособном состоянии.

А.1.7. Анализ видов и последствий отказов

А.1.7.1. Описание и цель

Анализ видов и последствий отказов (FMEA) является восходящим методом анализа надежности, который обычно применяют для изучения материала, компонентов, отказов оборудования и их воздействий на следующий более высокий функциональный уровень системы. Итерации этих шагов (идентификация одиночных режимов отказов и оценка их воздействия на следующий более высокий уровень системы) заканчиваются идентификацией всех режимов единичных отказов системы. FMEA может быть использован для анализа систем, использующих технологии с простыми функциональными структурами отказов (электрические, механические, гидравлические, программные и т.д.). Анализ видов, последствий и критичности отказов (FMECA) расширяет FMEA, определяя количество последствий отказа через вероятности появления и серьезности последствий. Серьезность последствий оценивают в соответствии с заданной шкалой.

А.1.7.2. Применение

FMEA и FMECA обычно применяют в случаях, когда уровень риска выявляется на ранних уровнях разработки продукции. Их применяют для новых технологий, процессов, проектов или при изменениях условий окружающей среды, нагрузок или инструкций. FMEA или FMECA могут быть применены для компонентов или систем, которые представляют собой продукцию, процессы или производственное оборудование. Они также могут быть применены к системам программного обеспечения.

А.1.7.3. Ключевые элементы

FMEA или FMECA состоят из следующих этапов:

- идентификация требований к функционированию компонента системы;
- идентификация потенциальных видов, последствий и причин отказов;
- идентификация риска, связанного с видами и последствиями отказа;
- идентификация рекомендуемых действий для устранения или уменьшения риска;
- завершающие действия.

А.1.7.4. Достоинства:

- систематическая идентификация отношений причин и последствий;
- начальная индикация тех видов отказов, которые, возможно, могут быть критическими, особенно отказов, которые могут повторяться;
- идентификация результатов определенных причин или событий, которые являются важными;
- обеспечение порядка идентификации мер по снижению риска;
- возможность использования в предварительном анализе новых или неиспытанных систем или процессов.

А.1.7.5. Ограничения:

- объем выходных данных может быть большим, даже для относительно несложных систем;
- метод может стать сложным и неуправляемым, если нет четкой связи между причиной и последствиями;
- метод не предназначен для анализа временных последовательностей, процессов восстановления, условий окружающей среды, аспектов технического обслуживания и т.д.;
- первоначальная модель критичности усложняется за счет включения конкурирующих факторов.

А.1.7.6. Стандарты

Применяют ГОСТ 27.310.

А.1.7.7. Пример

Пример анализа видов и последствий отказов приведен в таблице А.5.

Таблица А.5

Пример FMEA

Уровень контрактов					Проект				Подготовлен			
Номер листа					Элемент				Одобрен			
Стадия задачи					Проблема				Дата			
порядковый номер	описание функции элемента	код отказа	вид отказа	возможные причины отказа	признак отказа	локальные последствия	воздействие на выход элемента	меры, предупреждающие отказ	класс опасности	интенсивность отказа	источник данных	рекомендуемые действия
1.1.1	Статор двигателя	1111	Разрыв цепи	Разрыв обмотки	Искрообразование	Низкая мощность	Отключение	Установить температурное реле на одну из фаз	4			-
		1112	Разрыв цепи	Обрыв соединений	Искрообразование	Низкая мощность	Отключение	Установить температурное реле на одну из фаз	3			-
		1113	Нарушение изоляции	Постоянная высокая температура, производственный дефект	Включение системы защиты	Перегрузка	Нет выхода	Ежегодная проверка температурного реле	4			-
		1114	Размыкание	Старение; обрыв	Включение	-	Нет выхода	Резервирование	3			Рекомендуется

			цепи термор езисто ром	соединен ия	системы защиты							резервное соединени е на внешний кожух
		1115	Размык ание цепи термор езисто ром	Включени е системы защиты	Включен ие системы защиты	Снижение запаса скорости срабатыван ия реле	Нет выхода при высокой нагрузке	Установить температурн ое реле	3			Рекоменду ется резервное соединени е на внешний кожух
1.1.2	Система охлаждения двигателя	1121	Неадек ватное охлажд ение	Блокировк а низкой разности давлений	Высокая температ ура статора	Быстро меняющаяс я температур а	Быстро изменяетс я температу ра статора	Установить температурн ое реле на статор	2			-
		1122	Утечка в атмосф еру	Неисправ ность трубопров ода	Температ ура двигател я	Неадекватн ое охлаждени е двигателя	Быстро меняющая ся температу ра двигателя	Проверка температурн ого реле через каждые 2 ч	2			-
		1122	Поступ ление из атмосф еры	Неисправ ность трубопров ода	Низкий выход	Попадание воздуха в систему	-	Проверка трубопровод а через каждые 2 ч	2			-
1.1.3	Поведение двигателя	1131	Неиспр авность прокла	Износ прокладки	Низкий уровень масла	Потеря масла	Нет воздейств ия, если	Ежедневные проверки наличия	3			-

			дки. Утечка				утечка несерьезная	утечек				

А.1.8. Исследование опасности и работоспособности

А.1.8.1. Описание и цель

Исследование опасности и работоспособности (HAZOP) - это детальный процесс идентификации проблем опасности и работоспособности, выполняемый группой специалистов. HAZOP предназначен для идентификации потенциальных отклонений от целей проекта, а также для экспертизы их возможных причин и оценки последствий.

В основе HAZOP лежит экспертиза с помощью управляющих слов. Основное назначение HAZOP - поиск отклонений от целей проекта, пожеланий проектировщика или требований спецификаций к функционированию системы, ее элементам и характеристикам. Чтобы облегчить экспертизу, систему делят на части таким образом, чтобы для каждой части была определена цель проекта, которая выражается через элементы, передающие особенности, присущие этой части и представляющие собой компоненты части.

Элементы могут быть дискретными шагами или стадиями в процедуре, отдельными сигналами и элементами оборудования в системе управления, оборудованием или компонентами в процессе или электронной системе и т.д.

Идентификация отклонений от целей проекта достигается в процессе опроса с помощью заданных управляющих слов. Управляющее слово должно стимулировать образное мышление, сосредоточивать исследование на конкретную цель и выявлять идеи и суждения, максимизируя полноту исследования. Управляющие слова и их значения приведены в таблицах А.6 и А.7.

Таблица А.6

Основные управляющие слова и их значения

Управляющее слово	Значение
НЕ ИЛИ НЕТ	Законченное отрицание целей проекта
БОЛЬШЕ	Увеличение количества
МЕНЬШЕ	Уменьшение количества
ТАКЖЕ, КАК	Качественное изменение/увеличение
ЧАСТЬ	Качественное изменение/уменьшение

ЗАМЕНА	Логическая противоположность целям проекта
ДРУГОЙ, ЧЕМ	Полная замена

Таблица А.7

Дополнительные управляющие слова, относящиеся ко времени,
порядку или последовательности действий

Управляющее слово	Значение
РАНО	Относится к времени
ПОЗДНО	Относится к времени
ПРЕЖДЕ	Относится к порядку или последовательности
ПОСЛЕ	Относится к порядку или последовательности

А.1.8.2. Применение

Исследование HAZOP применяют на поздних стадиях разработки проекта для экспертизы средств эксплуатации и при изменении этих средств. Лучшее время для выполнения исследований HAZOP - непосредственно перед завершением проекта.

А.1.8.3. Ключевые элементы:

- исследование HAZOP является творческим процессом;
- исследование опирается на систематическое применение управляющих слов для идентификации потенциальных отклонений от целей проекта и использование этих отклонений в дальнейшей работе членов группы для исследования возможных причин отклонений и их последствий;
- исследование проводят под руководством обученного и опытного лидера исследования, который должен гарантировать всестороннее логическое и аналитическое изучение системы;
- исследование проводят специалисты в различных областях знаний, обладающие необходимыми навыками и опытом;
- исследование проводят в атмосфере доброжелательности и откровенного обсуждения. После идентификации проблемы ее регистрируют для последующих оценок и выводов;
- решения по идентификации проблем регистрируют для дальнейшего рассмотрения лицами, ответственными за проект.

Исследования HAZOP состоят из четырех основных последовательных этапов, указанных на рисунке А.10.

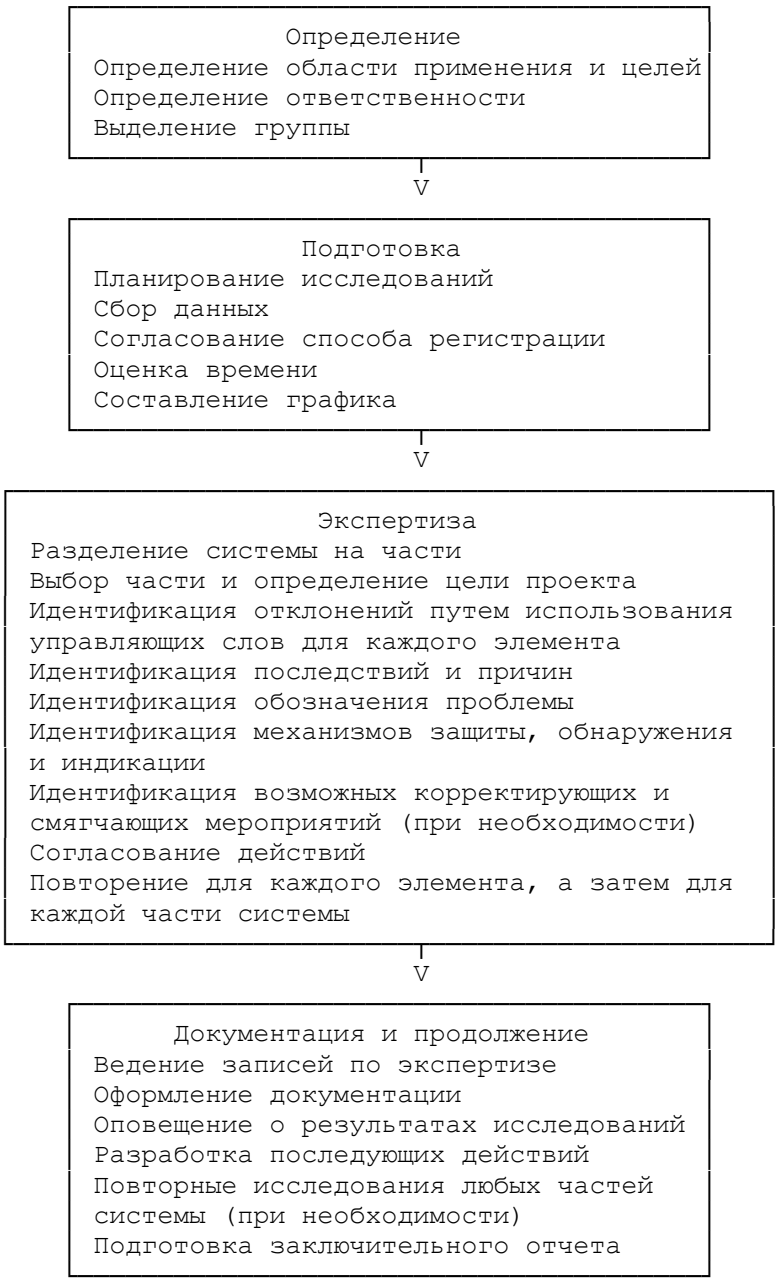


Рисунок А.10. Этапы исследования HAZOP

А.1.8.4. Достоинства:

- при исследовании используются навыки и знания группы экспертов, каждый из которых должен знать определенный аспект исследуемой системы;

- метод эффективен для обнаружения как причин, так и последствий отклонений на различных уровнях системы;

- метод применяют для анализа технологических процессов;

- результаты исследования имеют большое значение при определении необходимых корректирующих мероприятий.

А.1.8.5. Ограничения

Хотя исследования HAZOP чрезвычайно полезны в различных отраслях промышленности, они имеют ограничения, которые необходимо учитывать при рассмотрении вопроса о применении метода HAZOP:

- HAZOP рассматривает каждую часть системы и исследует воздействие отклонений на каждую часть. Иногда взаимодействие между частями системы является опасным. В этих случаях опасность должна исследоваться более подробно с применением таких методов, как метод дерева событий и анализ дерева неисправностей;

- при использовании любой другой методики идентификации опасностей или проблем работоспособности не может быть гарантии того, что все опасности или проблемы работоспособности идентифицированы. Поэтому исследование сложной системы не должно быть ограничено только исследованием HAZOP. Этот метод используют вместе с другими подходящими методами (например, анализом дерева неисправностей);

- существуют системы, тесно связанные между собой, в которых причины неисправности одной системы могут находиться в другой системе. Локальное совершенствование в этом случае не может устранить реальную причину и неисправность по-прежнему может возникать;

- успех исследования в большой степени зависит от способностей и опыта лидера исследования и взаимодействия между членами группы;

- метод HAZOP предназначен для исследования только частей системы, их элементов и характеристик, указанных в описании проекта. Действия и операции, которых нет в описании проекта не рассматривают.

А.1.8.6. Стандарты

Применяют ГОСТ Р 51901.11.

А.1.9. Анализ надежности человеческого фактора

А.1.9.1. Описание и цель

Анализ надежности человеческого фактора (HRA) является частью анализа человеческого фактора, который включает распределение функций, задач и ресурсов среди людей и машин и оценку надежности действий человека. Анализ человеческого фактора не является самостоятельной дисциплиной. В этом методе используются такие дисциплины как психология, физиология, социология, медицина и проектирование.

Специфическая цель анализа человеческого фактора состоит в том, чтобы оценить факторы, которые могут воздействовать на надежность действий человека при эксплуатации системы (анализ надежности человеческого фактора). Надежность человека необходима для успешной работы системы "человек - машина" в условиях воздействия различных факторов. Эти факторы могут быть внутренними (напряжение, эмоциональное состояние, обучение, побуждения и опыт) или внешними (часы работы, среда, действия диспетчеров, процессов, аппаратных средств).

А.1.9.2. Применение

Влияние человеческого фактора должно быть определено на всех стадиях разработки системы от проекта до обучения, эксплуатации и демонтажа. Метод применим для рассмотрения системы в целом (включая управление при эксплуатации) и взаимодействия отдельных работников при эксплуатации системы.

При решении любой задачи, выполняемой человеком, возникает возможность возникновения человеческой ошибки. После идентификации этих задач необходимо идентифицировать вероятные ситуации возникновения человеческих ошибок. Метод HRA является методом FMEA для задач, связанных с человеческим фактором.

Часто для решения этих задач используют анализ дерева событий. Дерево событий отражает информацию анализа задачи и определяет схему количественной оценки комбинации отказов.

А.1.9.3. Ключевые элементы

Типичными элементами анализа надежности человеческого фактора являются:

- описание персонала, условий его работы и выполняемых задач;

- анализ интерфейсов "человек - машина";

- анализ эффективности функций оператора;

- эффективность анализа ошибки человека при выполнении заданных функций;

- документирование результатов.

А.1.9.4. Достоинства

Анализ неудач и несчастных случаев показывает, что надежность человеческого фактора является ключевым моментом надежности системы "человек - машина". Если учитывать человеческий фактор, прогноз надежности системы может быть ложным.

А.1.9.5. Ограничения

Проведение анализа надежности человеческого фактора системы требует глубокого знания параметров эффективности действий человека.

Если необходимые данные отсутствуют, количественный анализ должен быть основан на экспертной оценке вероятностей человеческих ошибок.

Анализ человеческого фактора редко является частью разработки надежности системы и иногда

сложно убедить руководителей проекта начать анализ человеческого фактора или анализ надежности человека.

А.1.9.6. Пример

Рассмотрим систему, для запуска которой используют ключ (например, поезд). Предположим, что этот ключ должен быть заменен на электронную карту (по любой причине). Аналогичное решение используется в нескольких разновидностях автоматических кассовых аппаратов. Необходимо оценить влияние этого изменения на работоспособность системы (относительно прежнего решения). Оценку проводят поэтапно.

Этап 1. Рассматривают поведение водителя в конкретных условиях работы и его взаимодействие с системой при запуске поезда. Задача человека состоит в том, чтобы ввести карту и код для подтверждения своей личности.

Этап 2. Проводят распознавание кода. Интерфейс известен из опыта эксплуатации кассовых аппаратов. Он состоит из читающего устройства, дисплея и числовой клавиатуры для введения личного кода.

Этап 3. Определяют задачи:

а) ввод карты;

б) ввод правильного кода.

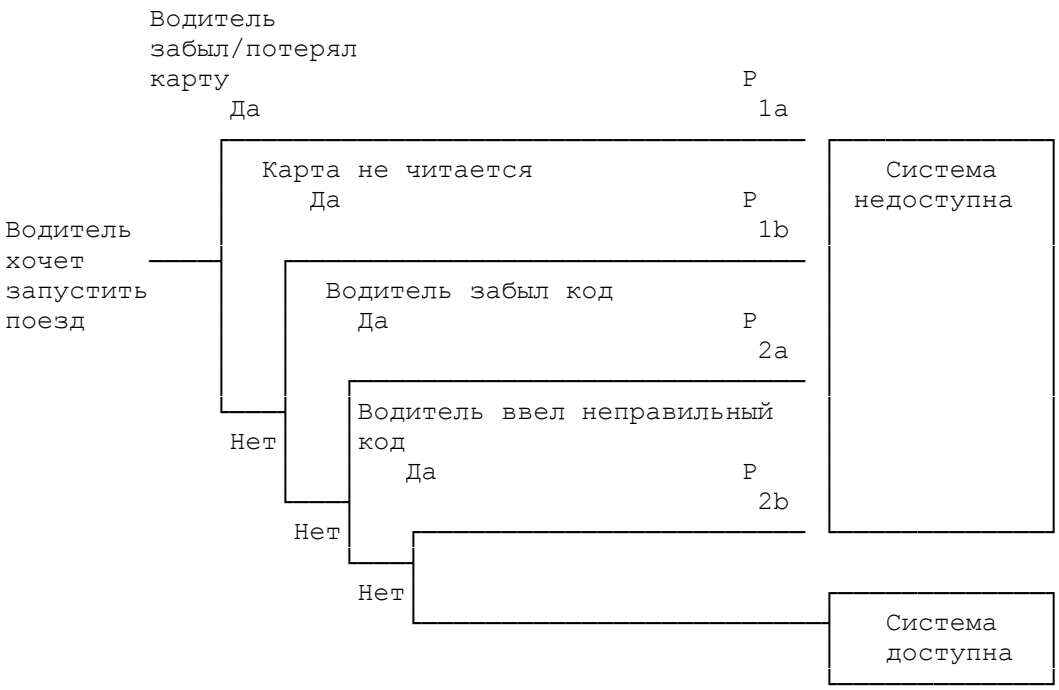
Этап 4. Возможные человеческие ошибки приведены в таблице А.8.

Таблица А.8

Возможные человеческие ошибки

Задача этапа 3	Человеческая ошибка	Причина	Мера предупреждения
a)	1) Водитель забыл или потерял карту	Неправильный способ хранения карты	Установленные способы хранения или футляр для карты, который удобен для водителя
		Невнимательность водителя	Проверки наличия карт у водителя (или напоминание перед началом работы). Обеспечение водителя резервными картами
	2) Карта находится в условиях, которые делают ее нечитаемой	Неправильный способ хранения карты	Проверки наличия карт у водителя (или напоминание перед началом работы). Обеспечение водителя резервными картами
		Неправильное обращение с картой	Обучение обращению с картой. Регулярные проверки способов хранения. Обеспечение водителей бесконтактными картами как альтернативный проект (рентабельность которого должна проверяться)
b)	1) Водитель забыл код	Плохая память	Обучение или как альтернатива: водитель выбирает код сам (номер, который является более простым для запоминания) вместо назначения кода системы
	2) Водитель ввел неправильный код	Ошибка при вводе кода	Обеспечение возможности, как минимум, одного повторного набора кода. Дизайн клавиатуры должен быть эргономичным для сокращения ошибок (например, клавиши не должны быть слишком маленькими, должны быть легко читаемыми, клавиатура должна давать подтверждение (сигнал), когда код набран и т.д.)

Эта информация также может быть представлена в виде дерева событий (рисунок А.11)



Параметр:	Значение:	Замечание:
	-4	
P 1a	10	Водитель знает, что должен быть внимателен и аккуратен при работе с картой, обеспечивать надлежащее хранение карты и выполнять необходимые проверки.
	-4	
P 1b	10	Необходим футляр для карты.
	-4	
P 2a	10	Водителю позволили выбрать свой код: он знает последствия, например, задержка поезда.
	-2	
P 2b	10	Эргономично разработанная клавиатура, но ошибки при наборе кода возможны.

Рисунок А.11. Человеческие ошибки,
изображенные в виде дерева событий

Для дерева событий могут быть заданы вероятности каждого перехода. Однако даже в этом примере точные данные или модели не могут быть получены. Несмотря на то, что некоторые данные могут быть получены из эксплуатации кассовых аппаратов, необходимо помнить, что условия работы в рассматриваемом случае могут быть совсем иными. В данном примере вероятность неработоспособного состояния является суммой вероятностей всех событий дерева.

Результатом человеческой ошибки является вероятность неработоспособного состояния, которая составляет приблизительно 0,01 за поездку и является недопустимой. Если водитель может сделать вторую попытку ввода кода после ошибочного набора, то вероятность ошибки равна $P_{2b} \cdot P_{2b} = 10^{-4}$. Таким образом, общая оценка вероятности ошибки составляет 0,0004 за поездку (четыре из 10000 поездов опоздают), которая является приемлемой. Разрешение большего количества попыток ввода кода могло бы снизить эту вероятность до 0,0003, но это решение может быть недопустимо с точки зрения безопасности.

А.1.10. Анализ прочности и напряжений

А.1.10.1. Описание и цель

Анализ прочности и напряжений определяет способность компонента или элемента

противостоять электрическим и механическим воздействиям окружающей среды или другим напряжениям, которые могут быть причиной отказа. Этот анализ определяет физические последствия воздействия на компоненты, а также механические или физические свойства компонента. Вероятность отказа компонента прямо пропорциональна прикладываемым напряжениям. Определенные отношения напряжений к прочности компонента определяют надежность компонента.

А.1.10.2. Применение

Анализ прочности и напряжений используют прежде всего при определении надежности или эквивалентной интенсивности отказов компонентов. Кроме того, его используют при исследовании физики отказа и определении вероятностного режима отказа компонента, вызванного определенной причиной.

Структурная надежность компонента, то есть его способность выдерживать электрические или другие напряжения, зависит от его прочности или несущей способности. В этом случае надежность является вероятностной мерой эффективности компонента. Определение этой несущей способности включает неопределенность, поэтому ее выражают случайной величиной; прикладываемое напряжение по этой же причине тоже представляют случайной величиной. Пересечение зон неопределенности этих случайных величин, представленных соответствующими распределениями, характеризует вероятность того, что напряжение превысит прочность, то есть вероятность появления отказа.

Оценки напряжений, прочности и результирующая надежность частей определяются вторыми моментами и зависят от дисперсий случайных величин, характеризующих ожидаемые напряжения и прочность. Часто задача упрощается до сравнения одной переменной напряжения с соответствующей характеристикой прочности компонента.

В общем случае прочность и напряжение должны быть описаны функцией эффективности или функцией состояния, которая представляет множество характеристик проекта. Положительное значение этой функции соответствует безопасному состоянию, а отрицательное - состоянию отказа.

А.1.10.3. Ключевые элементы

Ключевые элементы включают детальное знание составляющих материалов компонента и конструкции, а также других исследуемых свойств и соответствующих методов моделирования ожидаемых напряжений.

А.1.10.4. Достоинства

Анализ прочности и напряжений позволяет получить точное представление о надежности компонента, как функции процессов, приводящих к отказу. Метод позволяет учесть изменения проекта, а также изменчивости прикладываемых напряжений и их взаимную корреляцию. В результате метод обеспечивает более глубокое понимание воздействий сложных напряжений и лучше отображает физику отказа компонента, поскольку позволяет учесть воздействие различных факторов (механических, условий окружающей среды), включая их взаимодействие.

А.1.10.5. Ограничения

В случае сложных напряжений и особенно, когда имеется взаимодействие или корреляция между ними, решение задачи может быть очень сложным, требующим применения специальных программных средств. Другим недостатком анализа являются возможные ошибки в предположениях о распределениях случайных величин, которые могут привести к ошибкам при решении задачи.

А.1.10.6. Пример

Простым примером применения анализа прочности и напряжений является воздействие силы на уплотнительное кольцо, когда критерием отказа является утечка через кольцо. Для вычисления вероятности появления этого отказа была определена средняя сила F_0, вызывающая утечку, которая была рассчитана по результатам внутренних и внешних измерений, при определении геометрии кольца и исследования свойств его материала. Предполагалось, что и напряжение, и сила подчиняются нормальному распределению, стандартное отклонение которого составляет одну десятую от величины среднего. Вероятность отказа рассчитана по формуле

$$P_F = \Phi\left[\frac{F - F_0}{\sqrt{\sigma_F^2 + \sigma_{F_0}^2}}\right] = 1,9 \times 10^{-6}.$$

Пример изображен на рисунке А.12.

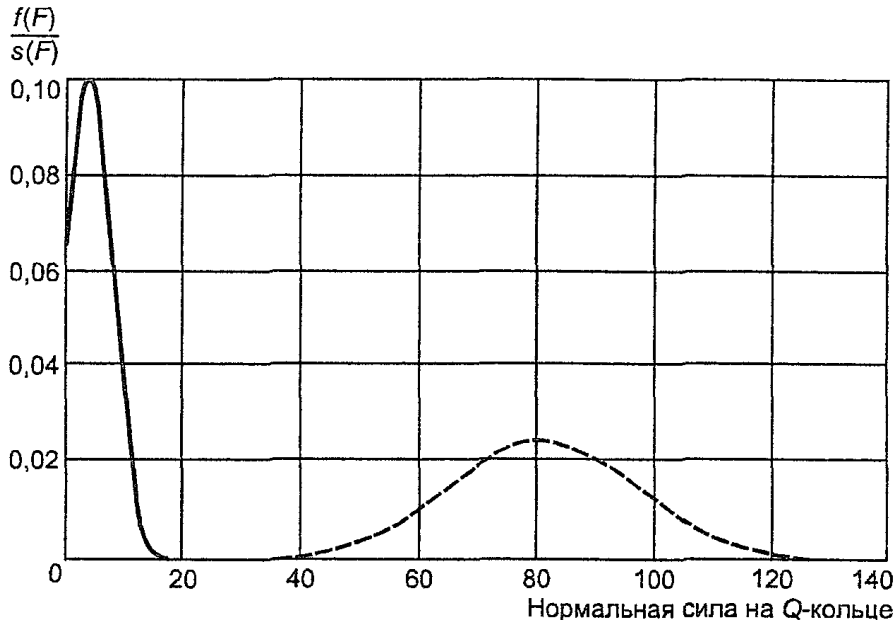


Рисунок А.12. Пример применения критерия прочности напряжений

А.1.11. Таблица истинности

А.1.11.1. Описание и цель

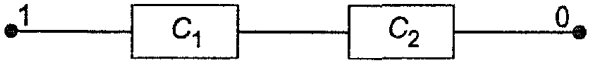
Основой метода таблицы истинности (ТТМ) является анализ функциональной структуры. Его применяют при разработке электрических и электронных систем. Метод заключается в составлении списка всех возможных комбинаций состояний (работоспособное состояние, неработоспособное состояние) компонентов системы и изучении их последствий.

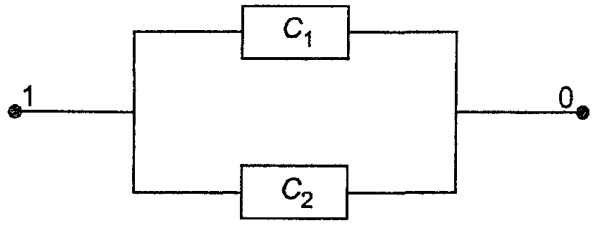
А.1.11.2. Применение

Начальные этапы применения метода совпадают с начальными этапами FMECA. Режимы отказов компонентов, а также их неработоспособные состояния должны быть идентифицированы. Каждый компонент характеризуется работоспособным состоянием и состоянием отказа. Таким образом, состояние системы является комбинацией состояний компонентов, каждый из которых находится в работоспособном или неработоспособном состоянии.

По результатам анализа последствий всех составляющих векторов состояний компонентов разрабатывают таблицу. Все отказы системы, таким образом, идентифицированы. Результаты отображают в таблице, называемой "таблицей истинности", где "0" обозначает работоспособное состояние, а "1" - неработоспособное состояние. Исследование каждого вектора состояний должно также включать анализ отказа (или неисправности) для идентификации вероятных общих причин отказа.

Вероятность неработоспособного состояния системы рассчитывают на основе вычисления вероятности появления каждого вектора неработоспособного состояния системы. Это возможно, когда компоненты независимы. На рисунке А.13 представлена таблица истинности для двух простых систем.

Система	Таблица истинности		
	C_1	C_2	0
	0	0	0
	0	1	1
	1	0	1
	1	1	1



C_1	C_2	0
0	0	0
0	1	0
1	0	0
1	1	1

Рисунок А.13. Таблица истинности для двух простых систем

Метод ТТМ позволяет определить все возможные комбинации работоспособных и неработоспособных состояний компонентов. Таким образом, он является наиболее строгим теоретическим методом. Для получения необходимых комбинаций таблицу истинности можно сократить Булевым методом, но его может быть трудно применить к сложной системе, так как число состояний может быстро стать очень большим.

А.1.11.3. Стандарты

Применяют ГОСТ Р 51901.14.

А.1.11.4. Пример

Система, представленная на рисунке А.14, состоит из главного пути сигнала К и альтернативного пути сигнала Е. Альтернативный путь не действует при функциональном резервировании. Выключатель U не находится на пути сигнала. Необходимо определить коэффициент готовности системы.

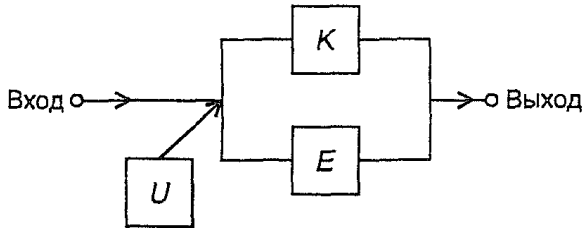


Рисунок А.14. Пример применения метода ТТМ

Пример таблицы истинности, в которой "0" обозначает работоспособное состояние, а "1" - неработоспособное состояние, приведен в таблице А.9.

Таблица А.9

Пример таблицы истинности

Обозначение состояния системы	K	E	U	$P(S\|A_i)$	$P(A_i)$	$P(S\|A_i)P(A_i)$
A_1	0	0	0	1	$a\ a\ a$ K E U	$1a\ a\ a$ K E U
A_2	0	1	0	1	$a\ (1-a)a$ K E U	$1a\ (1-a)a$ K E U

A 3	1	0	0	1	(1 - a)a a K E U	1(1 - a)a a K E U
A 4	1	1	0	0	(1 - a)(1 - a)a K E U	0
A 5	0	0	1	1	a a (1 - a) K E U	1a a (1 - a) K E U
A 6	0	1	1	1	a (1 - a)(1 - a) K E U	1a (1 - a)(1 - a) K E U
A 7	1	0	1	0,5	(1 - a)a (1 - a) K E U	0,5(1 - a)a (1 - a) K E U
A 8	1	1	1	0	(1 - a)(1 - a)(1 - a) K E U	0

Примечание. В состоянии А7 функция системы зависит от того, в положении К или Е находится выключатель. Поэтому вероятность состояния А7 принята равной 0,5.

Если случайные события, приводящие к состояниям A_1, ..., A_n, не появляются попарно, то вероятность P_s в соответствии с теоремой полной вероятности рассчитывают по формуле

$$P_s = \sum_{i=1}^{n} P(S \mid A_i) P(A_i),$$

где $P(S \mid A_i)$ - вероятность того, что система функционирует в состоянии A_i,

$P(A_i)$ - вероятность того, что система находится в состоянии A_i.

Подставляя коэффициенты готовности a вместо вероятностей P, получаем:

$$P_S = a_S = [a_K a_E a_U] + [a_K (1 - a_E) a_U] + [(1 - a_K) a_E a_U] + [a_K a_E (1 - a_U)] + \\ + [a_K (1 - a_E)(1 - a_U)] + [0,5(1 - a_K) a_E (1 - a_U)].$$

Таким образом,

$$a_S = a_K + 0,5(1 - a_K) a_E (1 - a_U).$$

А.1.12. Статистические методы оценки вероятности безотказной работы

А.1.12.1. Описание и цель

Безотказность является свойством, которое можно определить с помощью показателей безотказности. Показатели безотказности являются вероятностными характеристиками и требуют применения статистических методов.

Статистические методы могут быть использованы для определения количественной оценки показателей безотказности, включая:

- оценку и прогнозирование показателей безотказности продукции;
- оценку характеристик материалов в течение гарантийного срока эксплуатации или в процессе проектирования продукции;
- прогнозирование гарантийных затрат;
- оценку последствий предложенного изменения проекта;
- оценку выполнения требований технического регулирования и заказчика;
- наблюдение за продукцией в процессе ее эксплуатации для получения информации о причинах отказов и методах повышения безотказности продукции;
- сравнение компонентов, изготовленных на двух и более предприятиях с применением

различных материалов и эксплуатируемых в различных условиях.

Для применения статистических методов необходимо собрать соответствующие данные, которые зависят от решаемой задачи. Данные, используемые для анализа безотказности, должны представлять собой информацию об эффективности работы элементов, которые могут отказать (например, в условиях эксплуатации). Тип данных зависит от типа исследуемого элемента. Например, основными данными для устройств краткого действия являются количество испытуемых элементов и количество неотказавших элементов. Основными данными для невосстанавливаемых элементов являются наработки до опасных событий (для системы). Основные данные для восстанавливаемых элементов - наработки в процессе срока службы элемента. Обычно не все элементы отказывают за период наблюдений. Поэтому наработку до отказа фиксируют только для отказавших элементов, а продолжительность наблюдений - для неотказавших элементов. Такие данные называют цензурированными. Их обработка достаточно сложна и зависит от целей исследования надежности и особенностей элемента.

В дополнение к основным данным в статистический анализ может включаться информация о факторах, влияющих на безотказность для оценки их воздействия на эффективность.

Руководство по сбору данных о надежности по данным эксплуатации приведено в МЭК 60300-3-2 [7], а руководство по условиям испытаний на надежность и принципам статистической проверки гипотез - в МЭК 60300-3-5 [6].

В статистических методах используют только количественные данные. Данные о надежности, соответствующие предыдущим испытаниям или эксплуатации, могут быть ограниченными, но полезными для оценки надежности. Поэтому данные предыдущих испытаний или эксплуатации могут быть использованы вместе с количественными данными для оценки надежности на основе байесовских методов.

Байесовские методы позволяют объединять данные из различных источников. Они включают разработку модели показателя надежности и последующее использование доступных данных для описания априорного распределения. Априорное распределение описывает неопределенность параметров модели или параметров надежности. Априорное распределение должно охватывать все доступные данные, например, данные о надежности элементов в процессе их изготовления, данные о возможностях процессов производства и данные последних испытаний. Объединение всех данных в одно априорное распределение может быть использовано для анализа и решения сложных задач.

Байесовские методы формируют систему определения оценок, в которой оценки показателей надежности могут изменяться по мере поступления новых данных. Априорное распределение совместно с первоначальной моделью надежности позволяет построить апостериорное распределение, на основе которого определяют модифицированную оценку показателя надежности. Например, начальная оценка надежности в процессе разработки проекта может быть модифицирована по мере поступления данных испытаний. Неопределенность оценок может быть определена количественно в виде верхних и/или нижних границ показателей надежности.

Байесовские методы могут быть использованы для объединения данных различных уровней системы, например, модуля и его компонентов.

А.1.12.2. Применение

В зависимости от решаемой задачи используют различные модели надежности. Например, для описания срока службы используют экспоненциальное распределение или распределение Вейбулла, для случайных процессов - степенную модель, кроме того, используют модели повышения надежности, деградации, технического обслуживания и др.

С помощью классических или байесовских методов для каждого вида моделей могут быть получены необходимые оценки с соответствующей областью неопределенности.

А.1.12.3. Ключевые элементы

Классические статистические методы надежности обычно состоят из следующих этапов:

- идентификация модели надежности, которую необходимо использовать для решения задачи;
- идентификация данных, необходимых для определения параметров модели надежности;
- объединение используемых данных;
- оценка параметров статистической модели на основе классических методов;
- определение оценок показателей на основе построенной модели;
- повторение перечисленных этапов при необходимости получения новой оценки показателей надежности.

Байесовские методы надежности состоят из следующих этапов:

- идентификация модели надежности, используемой для решения задачи;

- идентификация данных, необходимых для определения параметров модели надежности;

- объединение отдельных данных в соответствующее априорное распределение;

- объединение априорного распределения с моделью и получение апостериорного распределения;

- определение необходимых оценок на основе апостериорного распределения;

- повторение вышеупомянутых этапов при необходимости определения новых оценок показателей надежности.

А.1.12.4. Достоинства

Преимущества всех статистических методов:

- могут объединять данные из различных источников;

- могут быть получены оценки показателей надежности с областью неопределенности;

- оценки показателей надежности могут быть модифицированы по мере поступления новых данных.

Кроме того, для байесовских методов:

- отдельные технические данные могут быть объединены с предыдущими данными об отказах;

- оценки показателей надежности могут быть получены даже на ранних этапах создания изделия, когда информации о наблюдениях очень мало.

А.1.12.5. Ограничения

Для всех статистических методов характерны трудности при:

- определении соответствующей функциональной модели, используемой для принятия решений;

- структурировании данных, необходимых для анализа.

Кроме того, для байесовских методов:

- выявление необходимых отдельных технических данных может быть сложным;

- построение априорного распределения может представлять трудную задачу;

- модифицированная оценка показателей надежности (по апостериорному распределению) не определяется прямым расчетом.

А.2. Выбранные методы поддержки

А.2.1. Анализ паразитных контуров

А.2.1.1. Описание и цель

Анализ паразитных контуров (SCA) представляет собой компьютеризированный подход к поиску скрытых путей, приводящих к выполнению нежелательной функции или невыполнению желательной функции без использования информации об отказах. Скрытый путь может состоять из проводов, частей, программных интерфейсов и источников энергии. Имеется шесть типов условий появления паразитных контуров:

- ложные метки;

- ложные индикаторы;

- ошибки в рисунках и чертежах;

- ложные пути;

- неправильная синхронизация;

- ошибки при выборе базовых значений параметров;

- объединения по проектированию.

А.2.1.2. Применение

Анализ паразитных контуров используют для обнаружения условий скрытых путей, приводящих к незапланированным режимам работы. SCA широко используют в космических системах и разработках, а также на промышленных предприятиях атомной энергетики.

А.2.1.3. Ключевые элементы

SCA состоит из следующих этапов:

- экспертиза путей (или функций);

- появление нежелательных путей.

А.2.1.4. Достоинства

SCA способствует сокращению ошибок в проекте и человеческих ошибок в системе.

А.2.1.5. Ограничения:

- нет достаточного количества специалистов по анализу паразитных контуров с применением программного обеспечения;

- требуются крупномасштабные компьютерные системы.

А.2.2. Анализ наихудшего случая

А.2.2.1. Описание и цель

Анализ наихудшего случая (WCA) представляет собой нестатистический способ определения возможности снижения эффективности системы на основе изучения всех комбинаций, заданных в спецификации пределов для параметров системы.

А.2.2.2. Применение

Главным образом WCA применяют на стадии разработки и проектирования для системы, состоящей из нескольких компонентов. Например, любой механизм, схема или сеть могут быть рассмотрены как система. Характеристики эффективности и параметры работоспособности компонентов могут влиять на характеристики эффективности системы. Их представляют в виде комбинаций математических выражений или логических функций.

А.2.2.3. Ключевые элементы

WCA состоит из следующих этапов:

- идентификация системы и ее компонентов;

- идентификация математической или логической функции для описания эффективности системы и ее параметров, описывающих эффективность компонентов;

- идентификация допустимых пределов изменения параметров системы;

- анализ характеристик эффективности системы для всех комбинаций параметров системы из допустимой области;

- проверка соответствия результатов заданной в спецификации эффективности системы;

- идентификация рекомендуемых действий для изменения проекта системы;

- завершающие действия;

- документирование аналитических процессов и заключительных результатов.

А.2.2.4. Достоинства:

- проектировщик может быть уверен, что система имеет высокую надежность при любых характеристиках компонентов, если они не выходят за границы требований спецификации;

- нет необходимости в сложной математической обработке;

- аналитические результаты, как правило, являются точными.

А.2.2.5. Ограничения:

- необходимо знать все математические и логические соотношения между параметрами;

- для получения достоверных аналитических результатов необходимо рассмотреть все компоненты системы;

- аналитические результаты не являются оптимальными.

А.2.3. Имитационное моделирование

А.2.3.1. Описание и цель

Имитационное моделирование состоит из набора статистических подходов, необходимых для проверки и определения возможности снижения эффективности системы при различных комбинациях параметров системы в пределах требований спецификации. Имеются два типовых метода моделирования: метод момента и метод Монте Карло. Первый метод основан на линейном приближении функции параметров проекта с помощью рядов Тейлора. При этом используют номинальные значения, предусмотренные проектом. Второй метод основан на моделировании статистическими методами, когда каждый параметр проекта выбирают случайным образом в соответствии с заданным распределением вероятностей.

А.2.3.2. Применение

Имитационное моделирование используют вместе с методом наихудшего случая для системы, состоящей из нескольких компонентов, главным образом, на стадии ее проектирования и разработки. Например, любой механизм, схема или сеть могут быть рассмотрены как система. Характеристики эффективности компонентов, а также параметры системы могут влиять на характеристики эффективности системы. Метод Монте Карло часто применяют в процессе автоматизированного проектирования системы.

А.2.3.3. Ключевые элементы

Имитационное моделирование обычно состоит из следующих этапов:

а) общие элементы:

- идентификация системы и ее компонентов,

- идентификация функции эффективности системы, выраженной через эффективность

компонентов или параметры проекта,

- идентификация допустимых пределов изменений параметров системы;

b) метод момента:

- построение линейного приближения функции эффективности системы с помощью рядов Тейлора,

- идентификация номинальных значений и дисперсий параметров проекта,

- идентификация номинального значения и дисперсии эффективности системы, рассчитанной на основе параметров проекта;

c) метод Монте Карло:

- идентификация распределения вероятностей для каждого параметра проекта,

идентификация компьютерного генератора случайных чисел для параметров проекта, основанных на данном распределении вероятностей,

- идентификация распределения вероятностей, его среднего и дисперсии для описания работы системы при моделировании;

d) общие элементы:

- проверка соответствия результатов требованиям спецификации по эффективности системы,

- определение рекомендуемых действий для изменения конфигурации системы и ее перепроектирования,

- завершающие действия,

- документирование аналитических процессов и заключительных результатов.

A.2.3.4. Достоинства:

a) метод момента:

- проектировщик может быть уверен, что система имеет установленную надежность, если для возможных изменений характеристик компонентов аналитические результаты дают значения характеристик системы в пределах, установленных в спецификации,

- аналитические результаты обеспечивают более точную интервальную оценку, чем WCA;

b) метод Монте Карло:

- проектировщик может быть уверен, что система имеет установленную надежность, если для возможных изменений характеристик компонентов, аналитические результаты дают значения характеристик системы в пределах, установленных в спецификации,

- метод применяют при автоматизированном проектировании,

- может быть смоделировано любое распределение вероятностей,

- полученные результаты обычно близки к оптимальным значениям,

- нет необходимости в математических вычислениях.

A.2.3.5. Ограничения:

a) метод момента:

- необходимы математические модели, пригодные для дифференцирования,

- для получения достоверных аналитических результатов должны быть учтены все компоненты системы,

- необходима сложная математическая обработка,

- в качестве распределения вероятностей используется нормальное распределение;

b) метод Монте Карло:

- для моделирования необходимы математические модели,

- для получения достоверных аналитических результатов должны быть рассмотрены все компоненты системы,

- моделируется большое количество копий системы.

A.2.4. Разработка надежности программного обеспечения

A.2.4.1. Описание и цель

Целью разработки надежности программного обеспечения (SRE) является прогнозирование надежности программного обеспечения на основе статистических методов. Проблема заключается в том, что программное обеспечение не отказывает, а выдает заранее определенные правильные или ошибочные результаты для данных входа. Поэтому в основе SRE лежит предположение, что программное обеспечение действует не случайным образом, а конфигурация системы и вид операции (например, входные данные) могут рассматриваться как случайные условия.

A.2.4.2. Применение

SRE применяют в процессе испытаний при принятии решения о прекращении испытаний

(решение, что критерий приемки выполнен) или для прогнозирования надежности при эксплуатации. Обычно данные отбирают в группах, например, количество отказов за указанное время, поскольку очень трудно получить реальные наработки для отказов.

Большинство прикладных программ основаны на предположении, что программная ошибка может быть описана негомогенным процессом Пуассона. Это означает, что программные ошибки происходят в статистически независимые моменты времени. Наработки подчиняются экспоненциальному распределению, а интенсивность отказов изменяется во времени. Обычно используют убывающую интенсивность отказов. Это означает, что ошибки, как только они выявлены, эффективно устраняются без введения новых ошибок. Главная цель SRE заключается в том, чтобы определить форму функции интенсивности отказов и оценить ее параметры по наблюдаемым данным. Как только функция интенсивности отказов определена, могут быть найдены такие показатели надежности как:

- общее количество отказов;
- количество остающихся отказов;
- время до следующего отказа;
- остаточное время испытаний (до принятия решения);
- максимальное количество отказов (относительно срока службы).

Другие подходы принимают во внимание архитектуру программного обеспечения, его функциональные модули, модель их взаимодействия и т.п. (например, марковский анализ). Затем данные отбирают и определяют оценки для модулей.

А.2.4.3. Ключевые элементы:

- определение показателей надежности и целей;
- определение используемой модели надежности программного обеспечения;
- отбор данных об отказах;
- валидация модели;
- прогноз показателей надежности по данным.

А.2.4.4. Достоинства:

- программное обеспечение может быть рассмотрено при прогнозировании надежности;
- цели и критерии испытаний могут быть определены и проконтролированы.

А.2.4.5. Ограничения:

- сбор данных о надежности программного обеспечения может быть трудным, так как качество результатов определяется качеством собранных данных;
- нет подхода для выбора функций интенсивности отказов. Имеется искушение выбрать модель интенсивности отказов, которой данные соответствуют больше всего вместо априорного выбора модели;
- теоретическая основа негомогенного процесса Пуассона намного слабее, чем в случае прогнозирования надежности аппаратных средств.

А.2.5. Анализ конечных элементов

А.2.5.1. Описание и цель

Анализ конечных элементов представляет собой расчетный компьютерный метод анализа воздействия нагрузок, прикладываемых к физическим элементам. Нагрузки могут быть механическими, тепловыми, электромагнитными или их комбинациями. В этом случае обычно решаемая задача слишком сложна для классических методов.

Данный метод существенно отличается от классических методов описанием исследуемого объекта. Для описания объекта используют бесконечно малые элементы. Континуум исследуемого объекта описывается дифференциальными уравнениями в частных производных. Для анализа конечных элементов объект разделен на простые блоки, находящиеся во взаимодействии, называемые элементами. Элементы характеризуются функциями формы. Все вместе они формируют геометрическую модель. Элементы взаимодействуют в узлах. Информация передается от элемента к элементу только через общие узлы. Внутри элемента используется интерполяция. Таким образом, воздействия на элемент описываются через центральные смещения.

А.2.5.2. Применение

Анализ конечных элементов является эффективным методом прогнозирования последствий и режимов отказов сложных структур. Он может быть использован для решения задач различных типов, включая анализ механических напряжений, вибраций, жидких потоков, передачи тепла, электромагнитных полей и т.п.

А.2.5.3. Ключевые элементы:

- выбор наиболее подходящих конечных элементов для моделирования объекта;
- деление объекта на элементы и определение свойств элементов;
- составление матричного представления взаимодействия с учетом степени свободы узлов;
- определение граничных условий и применяемых нагрузок;
- решение набора алгебраических уравнений, соответствующих матрице, для расчета центральных смещений;
- вычисление исследуемых физических параметров, например, напряжений вибрации и т.п.

А.2.5.4. Достоинства

Метод анализа конечных элементов может быть использован:

- для анализа упругих и неупругих воздействий;
- для выполнения статических и динамических исследований;
- для анализа элементов неправильной формы с большим количеством граничных условий и из различных материалов;
- для оптимизации проекта;
- для оценки и валидации надежности.

А.2.5.5. Ограничения:

- необходимость проведения высокого уровня специализированной технической экспертизы;
- легко исказить или неправильно истолковать результаты.

А.2.6. Выбор и ограничение частей

А.2.6.1. Описание и цель

Части выбирают на основе двух критериев: надежности части и способности части противостоять ожидаемым условиям окружающей среды и рабочим нагрузкам при использовании в системе. Выбор части зависит от требуемой надежности части, а также ее механических и/или электрических характеристик и условий, в которых часть должна безотказно работать.

Характеристики каждого электронного или механического компонента (активного или пассивного) должны быть нормированы, чтобы гарантировать, что его температурные, конструктивные и другие свойства (механические или другие) адекватны условиям эксплуатации. Эту задачу решают следующими этапами:

a) проводят оценку увеличения температуры (внутри корпуса). Если это не требуется, определяют самую неблагоприятную температурную ситуацию;

b) изучают требования к условиям окружающей среды для других изделий (климатические и динамические);

c) сравнивают результаты для этапов, указанных в перечислениях a) и b), по отношению к спецификациям для определения способности каждого компонента выдерживать тепловые и другие условия.

Части должны быть выбраны в соответствии с требованиями надежности. Так как система в целом тоже должна соответствовать требованиям надежности, ключевые части системы, то есть части, которые являются необходимыми для функционирования системы с установленной эффективностью, должны быть выбраны таким образом, чтобы была обеспечена их работоспособность.

Ограничение части означает снижение для нее допустимых воздействий нагрузок при эксплуатации и со стороны окружающей среды. Это способствует снижению вероятности отказа при эксплуатации.

При сравнении номинального усилия с ожидаемым напряжением должен быть предусмотрен запас, который рассчитывают на основе критериев и методов инженерного анализа. Этот запас обеспечивает необходимую надежность части при возникновении режимов неисправности.

А.2.6.2. Применение

Выбор частей, соответствующих ожидаемым условиям эксплуатации, и обеспечение необходимой надежности должны применяться при решении любой задачи надежности. Ограничение части должно быть неотъемлемой частью проектирования, поскольку ненадлежащим образом уменьшенные нагрузки на часть могут быть причиной ненадежности системы.

А.2.6.3. Ключевые элементы

Ключевыми элементами данного метода являются:

- информация об условиях эксплуатации и хранения;
- информация о надежности части в условиях эксплуатации;
- рекомендации по уменьшению нагрузок, подготовленные на основе исследования надежности

системы в целом и применения лучших методов проектирования.

А.2.6.4. Достоинства

Преимуществом метода является достижение необходимой надежности изделия.

А.2.6.5. Ограничение

Ограничение метода касается ситуации, когда нет информации о надежности части ни в базе данных, ни у изготовителя части. Это ограничение распространяется и на снижение допустимых нагрузок для части, когда рекомендации по снижению допустимых нагрузок включают рекомендации по надежности. Если рекомендации по снижению допустимых нагрузок являются следствием требований надежности, существует опасность чрезмерного снижения нагрузок.

А.2.7. Анализ Парето

А.2.7.1. Описание и цель

Анализ Парето является одним из семи основных инструментальных средств управления качеством (листы проверки, диаграммы Парето, диаграммы Исикавы, диаграммы последовательности операций, гистограммы, графики рассеивания и контрольные карты). Эти инструментальные средства находят применение при разработке надежности. Принцип Парето устанавливает, что небольшое подмножество проблем происходит намного чаще, чем все остальные ("полезное большинство"). Этот принцип можно сформулировать следующим образом: "20% причин вызывают 80% проблем".

Цель анализа Парето состоит в том, чтобы сосредоточить усилия на тех проблемах, которые имеют самый высокий потенциал для улучшения и помогают в распределении ресурсов, чтобы использовать их там, где они наиболее эффективны.

Диаграмма Парето является одним из наиболее часто используемых инструментальных средств улучшения. С помощью диаграммы определяют относительную важность проблемы в наглядной форме. Кроме того, диаграмма помогает предотвращать "смещение проблемы", когда ее "решение" устраняет одни проблемы, но усугубляет другие. С помощью диаграммы можно учесть воздействие изменения проекта на эффективность изделия путем управления изменениями следующим образом:

- путем разделения главной причины на категории ("высшую полосу" делят на подпункты в соответствующей диаграмме Парето);
- до и после анализа (новые полосы Парето изображают рядом с оригиналом Парето, показывая воздействия изменений);
- путем замены источника данных (данные, собранные по той же проблеме, но из различных источников (система/оборудование, расположение, заказчик и т.д.), отображаются рядом с диаграммой Парето);
- путем изменения измерений (используют те же самые характеристики, но измеренные другим способом).

А.2.7.2. Применение

Анализ Парето может быть использован на всех стадиях программы надежности, от концепции и определения, проектирования и разработки, производства и инсталляции до эксплуатации и технического обслуживания.

А.2.7.3. Ключевые элементы

Для эффективного применения анализа Парето требуется следующее:

- решить, о какой проблеме Вы хотите больше знать (то есть об отказах или их причинах);
- выбрать причины или проблемы, которые необходимо отслеживать, сравнивать и ранжировать (с помощью существующих данных, мозгового штурма, экспериментов);
- выбрать наиболее значимый параметр для измерений, например, частота или цена;
- выбрать период времени для исследований;
- составить список исследуемых данных, расположив их в порядке убывания;
- вычислить общее количество всех элементов и процентный вклад каждого элемента;
- начертить гистограмму, нанося категории на горизонтальную линию, а частоты (или затраты) на вертикальную линию;
- изобразить общую кривую, если это возможно;
- нанести на диаграмму соответствующие обозначения;
- интерпретировать результаты.

А.2.7.4. Достоинства:

- эффективное графическое представление анализа проблемы;
- анализ очень прост и не требует много времени и усилий;
- может быть использован для принятия решений как в технических, так и в других областях.

А.2.7.5. Ограничения:

- анализ Парето служит инструментом для улучшения обзора данных. Исследование причин проблемы должно проводиться экспертами, использующими любые необходимые методы;

- к анализу должны привлекаться опытные специалисты.

А.2.8. Диаграмма причин и следствий

А.2.8.1. Описание и цель

Диаграмма причин и следствий называется диаграммой Исикавы (в честь ее создателя) или диаграммой рыбного скелета (из-за ее формы). Диаграмма обеспечивает наглядное представление списка идентифицированных и систематизированных возможных причин проблем или факторов, необходимых для обеспечения работоспособного состояния или отказа системы.

Диаграмма эффективна при изучении процессов и ситуаций, а также при планировании. Она позволяет легко увидеть отношения между факторами. Диаграмма причин и следствий обычно создается методом мозгового штурма. В результате диаграмму часто изображают вручную на бумаге. Однако существуют пакеты программ, пригодных для составления диаграммы.

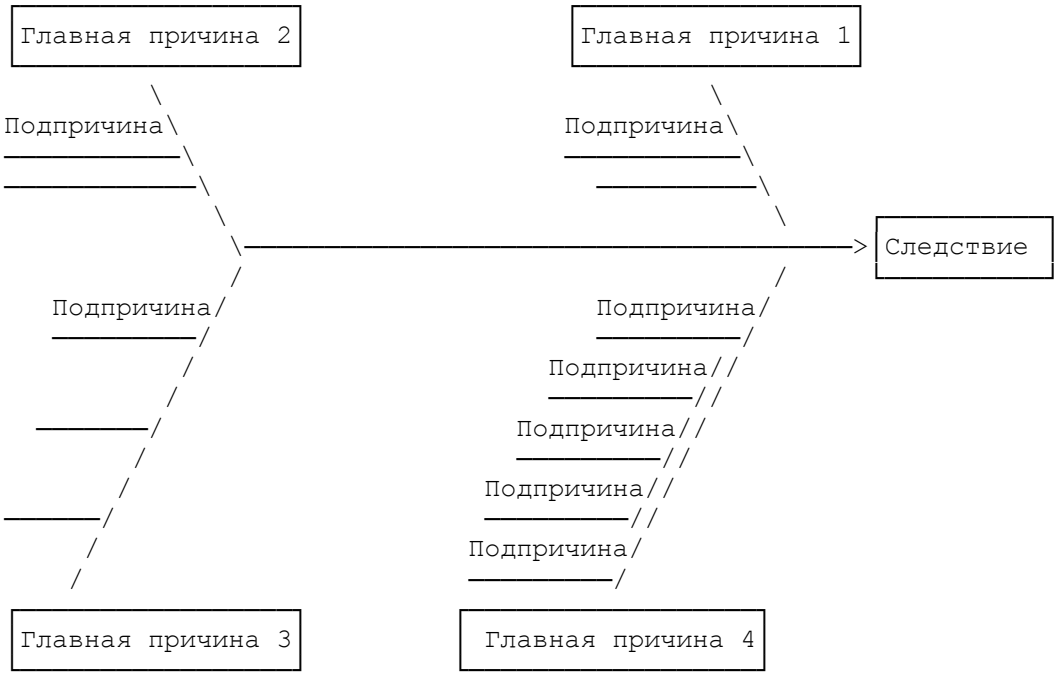


Рисунок А.15. Диаграмма причин и следствий

Основные этапы построения диаграммы:

1) определение воздействий;

2) идентификация главных причин;

3) идентификация вторичных причин;

4) идентификация наиболее вероятных вторичных причин.

Примечание. Для второго этапа часто используют метод 4М: человек, машины, методы, материалы. Могут также использоваться другие главные причины, например, шаги процесса.

А.2.8.2. Применение

Диаграмму используют при исследованиях на стадии проектирования и анализа последствий отказов, обнаруженных при эксплуатации.

А.2.8.3. Ключевые элементы:

- следствия должны быть понятны;

- установленные причины должны соответствовать следствиям;

- соответствующий выбор вторичных причин помогает сбалансировать структуру дерева (скелета);

- поскольку реальные причины должны опираться на данные и факты, эта информация должна быть доступной;

- компоненты системы, которые становятся слишком сложными или остаются слишком

простыми, должны иметь указание на то, что структура должна быть улучшена.

А.2.8.4. Достоинства:

- помогает работе специалистов в различных областях знаний;
- обеспечивает визуальное отображение причин и их структуры;
- результаты могут использоваться как входные данные для FMEA или анализа неисправностей.

А.2.8.5. Ограничения:

- отсутствуют количественные исследования;
- правильный выбор главных и вторичных причин зависит от опыта группы;
- метод не распространяется на многократные последствия.

А.2.9. Анализ отчета об отказах и система корректирующих действий

А.2.9.1. Описание и цель

Анализ отчета об отказах и система корректирующих действий (FRACAS) представляют собой систему закрытого цикла для идентификации, оценки и своевременного устранения последствий отказа. Отказы, появляющиеся в процессе испытаний и оценки, документируются. Данные собираются на нескольких уровнях. Используется система для прослеживания, анализа, последующей идентификации проблем части, ошибок в проекте, недостаточной квалификации персонала и неточностей процесса, требующих корректирующих действий. После определения причин отказа необходимо провести разработку корректирующих действий, эффективность которых проверяют до их выполнения.

А.2.9.2. Применение

FRACAS проводят сразу же, как только появляется возможность работы с аппаратными средствами и программным обеспечением. Весь персонал, участвующий в испытаниях и оценке, несет ответственность за документирование отказов. Отказы проверяют и по возможности локализуют.

Группа исследований FRACAS анализирует данные для определения значимости проблем и проблем, требующих корректирующих действий. В группе должны быть специалисты всех дисциплин, связанных с возможными проблемами.

Исследования отказов проводят на уровне, необходимом для определения корректирующих действий по устранению проблемы. Проверка эффективности корректирующих действий включает заключение группы о предотвращении повторных отказов.

А.2.9.3. Ключевые элементы:

- форма отчета соответствует исследуемым системе и процессу;
- база данных для документирования всех действий, связанных с анализом и решением проблем;
- группа специалистов по необходимым дисциплинам;
- механизм для прослеживания решения проблем.

А.2.9.4. Достоинства:

- могут быть использованы данные, собранные для разных условий эксплуатации и окружающей среды;
- применяют при проектировании, производстве и техническом обслуживании;
- способствует повышению надежности;
- могут быть использованы данные прошлых проектов и может быть источником данных для будущих проектов.

А.2.9.5. Ограничения:

- предотвращает повторение проблемы;
- результаты зависят от квалификации персонала, участвующего в испытаниях, оценке и регистрации отказов;
- в большинстве случаев не пригоден для объединения данных числовых оценок.

Приложение В
(справочное)

СВЕДЕНИЯ О СООТВЕТСТВИИ ССЫЛОЧНЫХ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

НАЦИОНАЛЬНЫМ СТАНДАРТАМ, ИСПОЛЬЗОВАННЫМ В НАСТОЯЩЕМ СТАНДАРТЕ В КАЧЕСТВЕ НОРМАТИВНЫХ ССЫЛОК

Обозначение ссылочного национального стандарта	Обозначение и наименование ссылочного международного стандарта и условное обозначение степени его соответствия ссылочному национальному стандарту
ГОСТ 27.310-1995	МЭК 60812:1985. Методы анализа надежности систем. Метод анализа видов и последствий отказа (NEQ)
ГОСТ Р 51901.14-2005 (МЭК 61078:1991)	МЭК 61078:1991. Методы анализа общей надежности. Метод блок-схемы надежности (MOD)
ГОСТ Р 51901.15-2005 (МЭК 61165:1995)	МЭК 61165:1995. Применение марковских методов (MOD)
ГОСТ Р 51901.11-2005 (МЭК 61882:2001)	МЭК 61882:2001. Исследование опасности и работоспособности (HAZOP). Руководство по применению (MOD)
ГОСТ Р ИСО 9000:2001	ИСО 9000:2000. Системы менеджмента качества. Основные положения и словарь (IDT)

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

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

Приложение С
(справочное)

ПЕРЕЧЕНЬ
СОКРАЩЕНИЙ НА АНГЛИЙСКОМ ЯЗЫКЕ,
ИСПОЛЬЗУЕМЫХ В ТЕКСТЕ СТАНДАРТА

Сокращение	Расшифровка сокращения на английском языке	Определение сокращения
FTA	Fault tree analysis	Анализ дерева неисправностей
ETA	Event tree analysis	Анализ дерева событий
HAZOP	Hazard and operability study	Исследование опасности и работоспособности
FMEA	Failure mode and effects analysis	Анализ режимов и последствий отказов
SRE	Software reliability engineering	Разработка программного обеспечения по надежности
FMECA	Failure mode, effects and criticality analysis	Анализ режимов, последствий и критичности отказов
FRACAS	Failure reporting analysis and corrective action	Анализ отчета об отказах и система корректирующих действий
RDB	Reliability block diagrams	Анализ структурной схемы надежности

HRA	Human reliability analysis	Анализ человеческого фактора

БИБЛИОГРАФИЯ

[1] МЭК 60300-3-4:1996 (IEC 60300-3-4:1996). Управление общей надежностью. Часть 3. Руководство по применению. Раздел 4. Руководство по установлению требований к общей надежности в технических условиях

(Dependability management. Part 3. Application guide. Section 4. Guide to the specification of dependability requirements)

[2] МЭК 60300-3-10:2001 (IEC 60300-3-10:2001). Управление общей надежностью. Часть 3-10. Руководство по применению. Ремонтопригодность

(Dependability management. Part 3-10. Application guide-Maintainability)

[3] МЭК 60706-2:1990 (IEC 60706-2:1990). Электрооборудование. Руководство по ремонтопригодности. Часть 2. Раздел 5. Изучение вопроса ремонтопригодности на этапе проектирования оборудования

(Guide on maintainability of equipment. Part 2. Section Five. Maintainability studies during the design phase)

[4] МЭК 60706-1:1982 (IEC 60706-1:1982). Электрооборудование. Руководство по ремонтопригодности. Часть 1. Разделы 1, 2 и 3. Введение, требования и программа ремонтопригодности

(Guide on maintainability of equipment. Part 1. Sections One, Two and Three. Introduction, requirements and maintainability programme)

[5] МЭК 61709:1996 (IEC 61709:1996). Компоненты электронные. Надежность. Стандартные условия для интенсивности отказов и нагрузочные модели для преобразования

(Electronic components. Reliability. Reference conditions for failure rates and stress models for conversion)

[6] МЭК 60300-3-5:2001 (IEC 60300-3-5:2001). Управление общей надежностью. Часть 3-5. Руководство по применению. Условия испытаний на надежность и принципы статистической проверки гипотез

(Dependability management. Part 3-5. Application guide. Reliability test conditions and statistical test principles)

[7] МЭК 60300-3-2:1993 (IEC 60300-3-2:1993). Управление общей надежностью. Часть 3. Руководство по применению. Раздел 2. Сбор данных по общей надежности с места эксплуатации

(Dependability management. Part 3. Application guide. Section 2. Collection of dependability data from the field).