ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61165— 2019

Надежность в технике

ПРИМЕНЕНИЕ МАРКОВСКИХ МЕТОДОВ

(IEC 61165:2006, Application of Markov techniques, IDT)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 5 сентября 2019 г. № 635-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61165:2006 «Применение марковских методов» (IEC 61165:2006 «Application of Markov techniques», IDT).

Международный стандарт разработан Техническим комитетом ТС 56.

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

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

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов, указанных в библиографии настоящего стандарта, соответствующие им национальные стандарты, сведения о которых приведены в приложении ДБ

5 ВЗАМЕН ГОСТ Р 51901.15—2005 (МЭК 61165:1995)

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Обозначения и сокращения 3
5 Общие положения 5
6 Предположения и ограничения 6
7 Взаимосвязь с другими методами анализа 6
8 Построение диаграммы состояний 7
9 Анализ 8
10 Документирование результатов 11
Приложение А (справочное) Основные математические соотношения, используемые в марковских методах 12
Приложение В (справочное) Пример построения диаграммы состояний 14
Приложение С (справочное) Пример анализа некоторых показателей безотказности, готовности, ремонтопригодности и безопасности для системы типа «1 из 2» с активным резервом 18
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 22
Приложение ДБ (справочное) Сведения о соответствии ссылочных международных стандартов, указанных в библиографии настоящего стандарта, национальным стандартам 23
Библиография 24

Введение

Марковские методы являются методами анализа безотказности, готовности, ремонтопригодности и безопасности. Обзор других, применимых для этих целей, методов и их ключевых характеристик представлен в МЭК 60300-3-1.

В настоящем стандарте представлены основные термины и обозначения, используемые в марковских методах, приведено описание основных правил разработки, представления и применения марковских методов, а также указаны предположения и ограничения для использования данного подхода.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежность в технике

ПРИМЕНЕНИЕ МАРКОВСКИХ МЕТОДОВ

Dependability in technics. Application of Markov techniques

Дата введения — 2019—12—01

1 Область применения

В настоящем стандарте установлено руководство по применению марковских методов для моделирования и анализа систем, а также определения оценок показателей безотказности, готовности, ремонтопригодности и безопасности систем.

Настоящий стандарт применяется во всех отраслях промышленности, где необходим анализ работы системы, функционирование которой может быть представлено совокупностью состояний и переходов между ними. Применение установленных в настоящем стандарте марковских методов предполагает, что интенсивности перехода — это не зависящие от времени константы. Подобные марковские методы называют однородными.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

IEC 60050(191):1990, International Electrotechnical Vocabulary (IEV) — Chapter 191: Dependability and quality of service (Международный электротехнический словарь. Глава 191. Надежность и качество услуг)

IEC 60300-3-1, Dependability management — Part 3-1: Application guide — Analysis techniques for dependability — Guide on methodology (Менеджмент надежности. Часть 3-1. Руководство по применению. Методы анализа надежности. Руководство по методологии)

IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения)

3 Термины и определения

В настоящем стандарте использованы термины и определения по МЭК 60050(191):1990, а также следующие термины и определения.

Примечание — При применении настоящего стандарта для анализа безопасности могут быть использованы термины, приведенные в стандартах серии МЭК 61508.

3.1 **система** (system): Совокупность взаимосвязанных и взаимодействующих элементов.
[ИСО 9000, 3.2.1]

Примечание 1 — В контексте надежности для системы определена цель в виде заданных функций, условий функционирования (использования) и установленных границ.

Примечание 2 — Структура системы может быть иерархической.

Издание официальное

3.2 **элемент** (element): Объект, у которого в рамках данного рассмотрения не выделены составные части.

Примечание — Обычно предполагают, что элемент может существовать только в двух состояниях: работоспособном или неработоспособном (см. 3.4 и 3.5). Для удобства в настоящем стандарте используется термин «состояние элемента».

3.3 **состояние системы** $X(t)$ (system state): Конкретная комбинация состояний элементов.

Примечание — $X(t)$ — состояние системы в момент времени t. Существуют другие факторы, оказывающие влияние на состояние системы (например, режим функционирования).

3.4 **работоспособное состояние** (up state): Состояние объекта (системы или элемента), в котором объект способен выполнять требуемую функцию.

Примечание — Система может иметь несколько различных работоспособных состояний (например, состояние полного выполнения установленных функций и состояние ухудшения работоспособности).

3.5 **неработоспособное состояние** (down state): Состояние объекта (системы или элемента), в котором объект не способен выполнять требуемую функцию.

Примечание — Система может иметь несколько различных неработоспособных состояний.

3.6 **опасность** (hazard): Потенциальный источник получения травм или вреда здоровью людей или материального ущерба.

[МЭК 61508-4, 3.1.2, модифицировано]

3.7 **опасный отказ** (dangerous failure): Отказ, который может привести к тому, что система, связанная с безопасностью, перейдет в опасное состояние или в состояние невыполнения заданной функции.

[МЭК 61508-4, 3.6.7, модифицировано]

Примечание 1 — Возможность появления опасного отказа зависит от структуры системы.

Примечание 2 — В некоторых случаях в качестве синонима термина «опасный отказ» используют термин «небезопасный отказ».

3.8 **безопасный отказ** (safe failure): Отказ, который не приводит систему, связанную с безопасностью, в опасное состояние или в состояние невыполнения заданной функции.

[МЭК 61508, модифицировано]

3.9 **переход** (transition): Изменение одного состояния системы на другое.

Примечание — Как правило, переход является результатом отказа или восстановления. Также причиной перехода могут быть: ошибка человека, внешние события, перенастройка программного обеспечения и т. п.

3.10 **вероятность перехода** $P_{ij}(t)$ (transition probability): Условная вероятность перехода из состояния i в состояние j в течение периода времени $(s, s + t)$ при условии, что в момент времени s (левая граница временного промежутка) системы находится в состоянии i.

Примечание 1 — Формально $P_{ij}(s, s + t) = P(X(s + t) = j \mid X(s) = i)$. Если марковский процесс однороден по времени, то $P_{ij}(s, s + t)$ не зависит от s и обозначается $P_{ij}(t)$.

Примечание 2 — Для неприводимого марковского процесса (например, если каждое состояние может быть достигнуто из другого состояния) имеет место соотношение $P_{ij}(\infty) = P_j$, где P_j — асимптотическая стационарная или установившаяся вероятность состояния j.

3.11 **интенсивность перехода** q_{ij} (transition rate): Предел, если он существует, отношения условной вероятности перехода из состояния i в состояние j в течение периода времени $(t, t + \Delta t)$, к Δt при Δt, стремящемся к нулю, и при условии, что система находилась в состоянии i в момент времени t.

Примечание — В данном случае также используют обозначения p_{ij} и c_{ij}.

3.12 **начальное состояние** (initial state): Состояние системы в момент времени $t = 0$.

Примечание — Как правило, система начинает функционирование в момент времени $t = 0$ из работоспособного состояния, в котором все элементы системы функционируют, и переходит в конечное неработоспособное состояние через другие работоспособные состояния, в которых система имеет меньшее количество функционирующих элементов.

3.13 **поглощающее состояние** (absorbing state): Состояние, из которого переходы невозможны.

3.14 **восстанавливаемая система** (restorable system): Система, содержащая элементы, которые могут быть восстановлены после отказа до работоспособного состояния; отказ элемента не обязательно вызывает отказ системы.

Примечание — В данном случае также используют термин «ремонтируемая система».

3.15 **невосстанавливаемая система** (non-restorable system): Система, диаграмма состояний которой содержит переходы только по направлению к состоянию отказа системы.

Примечание — В данном случае также используют термин «неремонтируемая система».

4 Обозначения и сокращения

4.1 Обозначения для диаграммы состояний и переходов

Марковские методы графически представляют с помощью диаграмм состояний или диаграмм интенсивностей переходов.

В настоящем стандарте использованы представленные ниже обозначения и сокращения. При необходимости могут быть использованы другие обозначения.

4.1.1 Знак состояния

Состояние изображают в виде круга или прямоугольника.

Примечание — Для четкости неработоспособные состояния могут быть выделены жирными линиями, цветом или штриховкой.

4.1.2 Описание состояния

Описание, расположенное внутри знака состояния и представленное в виде слов или алфавитно-цифровых символов, определяющих комбинации отказавших и функционирующих элементов, характеризующих это состояние.

4.1.3 Обозначение состояния

Число или буква в круге расположены рядом со знаком состояния или при отсутствии описания состояния внутри знака состояния без него.

Примечание — Состояние часто изображают в виде круга с числом, обозначающим состояние.

4.1.4 Стрелка перехода

Стрелка указывает направление перехода (как результата отказа или восстановления). Интенсивность перехода записывают рядом со стрелкой перехода.

4.2 Другие обозначения и сокращения

Обозначения показателей безотказности, готовности, ремонтопригодности и безопасности соответствуют обозначениям, приведенным в МЭК 60050 (191). Приведенные ниже ссылки с числом 191 указывают на раздел МЭК 60050 (191). В настоящем стандарте представлены следующие обозначения и сокращения:

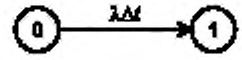
Обозначение/ сокращение	Термин	Ссылка
$R(t)$	— вероятность безотказной работы	
	Примечание — Для вероятности безотказной работы используют также более общее обозначение $R(t_1,t_2)$.	
DFR	— интенсивность опасного отказа	МЭК 61508
	Примечание — В контексте безопасности для DFR обычно используют обозначение HR (интенсивность возникновения опасности, интенсивность отказа).	
MTTF	— средняя наработка до отказа	191-12-07
MTTFF	— средняя наработка до первого отказа[1)]	191-12-06

[1)] *MTTFF* является частным случаем *MTTF*.

Обозначение/ сокращение	Термин	Ссылка
MTTFH	— средняя наработка до возникновения первой опасной ситуации	
PFD	— вероятность отказа по запросу	МЭК 61508
	Примечание — Для заданного времени *t* *PFD* соответствует $\sum_j P_j(t)$ — $\sum_j \sum P_j(t)$ по всем неработоспособным состояниям *j*	
$\lambda(t)$	— интенсивность отказов (мгновенная)	191-12-02
$\mu(t)$	— интенсивность восстановлений	
	Примечание — В 191-13-02 $\mu(t)$ используют для обозначения интенсивности ремонта.	
$A(t)$	— коэффициент готовности (мгновенный)	191-11-01
$U(t)$	— коэффициент неготовности (мгновенный)	191-11-02
A	— асимптотический или стационарный коэффициент готовности	
	Примечание — Стационарный коэффициент готовности имеет то же числовое значение, что и асимптотический коэффициент готовности.	
MUT	— средняя продолжительность работоспособного состояния	191-11-11
MDT	— средняя продолжительность неработоспособного состояния	191-11-12
$P_i(t)$	— вероятность того, что система находится в состоянии *i* в момент времени *t*	
P_i	— асимптотическая и стационарная вероятность того, что система находится в состоянии *i* в момент времени *t*	
Δt	— малый интервал времени	
$P_{ij}(t)$	— вероятность перехода из состояния *i* в состояние *j* в момент времени *t*	
q_{ij}	— интенсивность перехода из состояния *i* в состояние *j*, и $i \neq j$	
	Примечание — q_i представляет собой интенсивность перехода из состояния *i*: $q_i = \sum_{j \neq i} q_{ij}$	

4.3 Пример

На рисунке 1 показана диаграмма вероятностей перехода за период времени (t, $t + \Delta t$), где t произвольно, а Δt мало, для невосстанавливаемой системы, состоящей из одного элемента, с постоянной интенсивностью отказов λ.



0 — работоспособное состояние системы. 1 — неработоспособное состояние системы

Рисунок 1 — Диаграмма вероятностей перехода в период времени (t, $t + \Delta t$), где t произвольно, а Δt мало, для невосстанавливаемой системы, состоящей из одного элемента с постоянной интенсивностью отказов λ

$\lambda \Delta t$ — условная вероятность перехода системы из состояния 0 в состояние 1 за малый период времени (t, $t + \Delta t$) при условии, что система находилась в состоянии 0 в момент времени t. Для

упрощения записи величину Δt часто опускают, при этом диаграмма вероятностей перехода, представленная на рисунке 1, принимает вид диаграммы интенсивностей перехода, приведенной на рисунке 2.

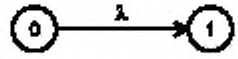


Рисунок 2 — Диаграмма состояний для невосстанавливаемой системы, состоящей из одного элемента

На рисунке 2 и далее по тексту термин «диаграмма состояний» использован как эквивалентный термину «диаграмма интенсивностей перехода».

5 Общие положения

При применении марковских методов диаграммы состояний используют для представления функционирования системы, для которой могут быть вычислены показатели безотказности, готовности, ремонтопригодности и безопасности. Это позволяет моделировать поведение системы во времени. В настоящем стандарте систему рассматривают как набор элементов, каждый из которых может существовать только в одном из двух состояний: неработоспособном или работоспособном. Система в целом, однако, может существовать в различных состояниях, каждое из которых определяется специфической комбинацией работоспособного и неработоспособного состояний ее элементов. Таким образом, в момент отказа или восстановления элемента система переходит из одного состояния в другое. Обычно эту модель называют моделью дискретных состояний с непрерывным временем.

Марковские методы особенно подходят для исследования систем: с резервированием, отказ которых зависит от наличия последовательности событий; со сложной стратегией технического обслуживания и ремонта. Например, это системы с приоритетами восстановлений или множественными групповыми восстановлениями, с проблемами очередей и ограничения ресурсов для восстановления. При построении модели необходимо, чтобы модель адекватно отражала функционирование реальной системы по отношению к стратегии и политике ее технического обслуживания и ремонта. В частности, должны быть рассмотрены подходящие экспоненциальные распределения времени восстановления. Следует отметить, что при моделировании восстанавливаемых систем с резервированием при ограничении возможностей ремонта за счет свойства отсутствия памяти реальное время ремонта может быть завышено (см. рисунок В.9 приложения В).

Главным преимуществом применения марковских методов анализа с учетом предположений и ограничений, описанных в разделе 6, является то, что могут быть смоделированы стратегии технического обслуживания и ремонта, например приоритеты восстановления отдельных элементов. Кроме того, в модели может быть рассмотрен порядок возникновения многократных отказов. Необходимо отметить, что другие методы анализа надежности, например анализ дерева неисправностей (FTA) и метод структурной схемы надежности (RBD), как описано в МЭК 61025 и МЭК 61078, соответственно, не позволяют учесть сложные стратегии технического обслуживания и ремонта, хотя они могут иметь специальные вентили, изображаемые особыми знаками (динамические вентили), для идентификации подобных ситуаций. Анализ таких вентилей следует проводить отдельно с помощью марковских и других методов, включая полученные результаты в анализ дерева неисправностей и RBD.

Несмотря на то что марковские методы с теоретической точки зрения являются гибкими и универсальными, при решении трудных практических задач необходимы специальные меры предосторожности. Главная проблема заключается в том, что количество состояний и возможных переходов системы быстро возрастает с ростом количества элементов системы. В случае большого количества состояний и переходов возрастает вероятность ошибок и искажений. Для того чтобы уменьшить эту вероятность, предпочтительно использовать некоторые правила составления диаграммы. Кроме того, применяемые расчетные методы могут быть достаточно сложными и требовать специальных компьютерных программ и/или помощи экспертов в области прикладной математики.

Кроме того, методы марковского анализа подходят для моделирования стратегий технического обслуживания и ремонта и дают возможность графически отображать события отказа/восстановления, что также является ценной характеристикой метода. Процесс чередования отказа/восстановления представлен переходами от одного знака состояния к другому, вместе составляющими диаграмму состояний системы.

Количество возможных состояний конечно, и сумма всех вероятностей состояний равна единице. В любой момент времени система может находиться исключительно в одном из состояний, представленных на диаграмме состояний. Из практических соображений состояния с очень низкой вероятностью допускается исключать из модели функционирования системы, в этом случае сумма вероятностей всех оставшихся состояний будет лишь приближенно равна единице.

Описанные методы моделирования могут быть также применены к системам, в которых определенные или все элементы являются невосстанавливаемыми. Очевидно, что систему с невосстанавливаемыми элементами можно рассматривать как специальный случай системы с восстанавливаемыми элементами, у которых интенсивности восстановления равны нулю (или время восстановления бесконечно).

6 Предположения и ограничения

Правила разработки диаграммы состояний (см. 8.2), установленные в настоящем стандарте, применимы во всех случаях (кроме правила h). Однако описание расчетных методов приведено только для случая, когда интенсивности отказов и восстановлений для всех элементов исследуемой системы постоянны во времени. Предположение о постоянстве интенсивности отказов приемлемо для элементов многих систем до наступления их износа (однако это предположение также должно быть обосновано), предположение о постоянстве интенсивности восстановлений должно быть обосновано в том случае, если среднее время восстановления не является пренебрежимо малой величиной по сравнению с соответствующим значением средней наработки до отказа. Оценки в общем случае, когда интенсивности отказов или интенсивности восстановлений не постоянны во времени, в настоящем стандарте не рассмотрены.

Из сделанных предположений следует, что будущее состояние системы зависит только от существующего состояния системы и не зависит от того, как система достигла этого состояния. Необходимо гарантировать, что данное свойство отсутствия памяти марковских моделей является достаточной аппроксимацией реального процесса изменения состояния системы (см. 8.1). Особое внимание следует уделять моделированию влияния отказов по общей причине, которые могут привести систему в некоторое возможное промежуточное состояние (см. рисунок В.4 приложения В).

Обычные предположения для каждого элемента рассматриваемой системы следующие:

- интенсивность отказов λ и интенсивность восстановлений μ являются постоянными (не зависят от времени);
- вероятность перехода из состояния i в состояние j за малый период времени $(t, t + \Delta t)$ при условии, что в момент времени t система находилась в состоянии i, равна $q_{ij}\,\Delta t$, где q_{ij} — сумма интенсивностей отказов и восстановлений соответствующих элементов.

Примечание — Теоретически ограничения, связанные с постоянством интенсивностей отказов и восстановлений, могут быть преодолены путем расширения пространства состояний, так как многие неэкспоненциальные распределения наработки до отказа или для времени восстановления могут быть аппроксимированы суммой экспоненциальных распределений. Каждое из этих экспоненциальных распределений моделируют как дополнительное состояние, являющееся аналогом памяти для наработки до отказа или для времени восстановления. Однако данный подход, обычно называемый фазовой концепцией или концепцией дополнительных состояний, не получил широкого практического применения.

7 Взаимосвязь с другими методами анализа

7.1 Общие положения

Марковские методы могут быть использованы для моделирования событий и состояний совместно с другими методами моделирования, в особенности когда этим методам не достает возможностей марковских методов, например способности описывать переходы состояний системы в зависимости от времени или состояния. Результат совместного применения нескольких методов часто называют гибридной моделью.

Подробный анализ методов моделирования приведен в МЭК 60300-3-1. Всестороннее описание гибридных моделей, использующих марковские диаграммы состояний, представлено в МЭК 61078 и МЭК 61025. Ниже приведено общее описание гибридных моделей.

7.2 Анализ дерева неисправностей FTA

Анализ дерева неисправностей — метод, используемый для определения оценки вероятности отказа в заданный момент времени *t* при помощи булевой алгебры. Данный метод не отражает зависимости от времени и состояний. Для анализа подобных зависимостей внутри метода FTA возможно применение новых вентилей, для которых используют особые марковские модели (рассматриваемые отдельно), не включаемые в основную схему FTA. Эти вентили называют динамическими вентилями (такие как PRIORITY AND, SEQUENTIAL INHIBIT или SPARE)[1]. Каждый из них может быть заменен основным событием, вероятность реализации которого вычисляют при помощи марковских методов. Полученную модель часто называют гибридным или динамическим FTA.

Как статические, так и динамические вентили FTA могут быть смоделированы при помощи марковских методов. Однако особое внимание следует уделять свойству независимости событий в марковской модели и в FTA. В дереве неисправностей части, исследуемые при помощи марковских методов по предположению должны быть независимыми ветвями.

7.3 Метод структурной схемы надежности RBD

Метод структурной схемы надежности RBD, как и FTA, основан на применении булевой логики и, таким образом, имеет те же ограничения, что и FTA.

Метод RBD позволяет выделять блоки RBD, для которых необходимо использовать марковские методы. Выделенные блоки должны формировать цепь с одним входом и одним выходом; при этом цепь не должна содержать блоки, ранее дублированные. Руководство по применению данного метода представлено в МЭК 61078.

7.4 Сети Петри

Сети Петри — это графический метод представления и анализа сложных логических взаимодействий элементов системы.

В частности, такой класс сетей Петри, как общие стохастические сети Петри (GSPN), имеет эквивалентные марковским методам возможности моделирования. Сети Петри можно рассматривать как естественное неявное представление явного представления марковской модели. Сети Петри могут быть преобразованы в марковскую модель. Так модели GSPN, содержащие сложные взаимодействия, часто могут быть описаны более просто и более простыми диаграммами при использовании марковских методов. В вычислительных целях сети Петри преобразуют в соответствующую марковскую модель. Для практических вычислений, как правило, используют программное обеспечение.

8 Построение диаграммы состояний

8.1 Предварительные требования

До начала анализа системы необходимо решить следующие общие задачи:

a) Определить цель анализа. Это может быть анализ одного или нескольких из следующих показателей:

- вероятность безотказной работы;
- частота опасных событий;
- средняя наработка до первого отказа;
- асимптотический коэффициент готовности;
- вероятность того, что система откажет при поступлении запроса на ее функционирование (для системы, которая не используется непрерывно);
- другие установленные показатели.

Также необходимо определить единицы измерений.

b) Определить характеристики системы и граничные условия анализа.

Для этого необходимо ответить на вопросы, подобные следующим:

Какие важные свойства моделируемой системы?

Каким образом данные характеристики могут быть подтверждены или, по крайней мере, проверена их правдоподобность?

[1] Вентили «И с приоритетами», «Последовательные блокировки» или «Резерв».

Система является восстанавливаемой (после отказа) или невосстанавливаемой?

Необходимо ли описывать изменение состояния системы в зависимости от времени?

Какова неопределенность исходных данных, например интенсивностей отказов и восстановлений и/или характеристик отказов по общей причине?

Каковы необходимые точность или уровень доверия результатов?

Если некоторые свойства реальной системы не важны для модели, то следует это обосновать.

c) Убедиться в том, что марковский метод является наиболее подходящим методом анализа для поставленной задачи. Выбор метода должен быть основан на целях анализа и свойствах системы, а не наоборот; в противном случае свойства системы будут смоделированы не в полном объеме. В частности, предположения и ограничения модели должны быть тщательно проверены.

d) Модель и входные данные должны быть проверены экспертами в области эксплуатации системы, так как ошибки, связанные с неточностями в модели или данных, могут сильно повлиять на результат анализа.

Ключевой задачей марковского анализа является корректное построение диаграммы состояний. Рекомендуемые для этого правила представлены в 8.2. Правила должны быть установлены до начала анализа, и таким образом обеспечены обозначения отдельных состояний. Это дает возможность построения четких графических моделей.

8.2 Правила разработки и представления

Приведенные ниже правила являются руководством для разработки диаграммы состояний. Построенная диаграмма состояний по данным правилам обеспечивает легкость понимания и анализа. На диаграмме допустимо использование обозначений, отличных от перечисленных ниже, а также иное расположение элементов диаграммы.

a) Каждое состояние системы должно быть изображено в виде круга или прямоугольника с идентификатором состояния (буква или число), который позволяет однозначно распознавать это состояние.

b) При необходимости знак состояния может включать описание состояния системы как непосредственное или в соответствии с принятыми обозначениями.

c) Состояния должны размещаться таким образом, чтобы крайним левым состоянием было полностью работоспособное состояние системы, а крайним правым состоянием — неработоспособное состояние. Соответственно промежуточные состояния должны быть расположены так, чтобы переход слева направо являлся результатом отказа, а переход справа налево — результатом ремонта или восстановления.

d) Состояния системы, соответствующие одинаковому количеству отказавших элементов, должны располагаться друг под другом.

e) Переходы между состояниями системы должны быть отмечены линиями со стрелками, соединяющими состояния. Линия со стрелкой справа представляет собой отказ, а линия со стрелкой слева — восстановление. Если переход между двумя состояниями может быть достигнут путем отказа или восстановления, то такой переход должен изображаться единственной линией со стрелками на обоих концах. В простой диаграмме состояний для индикации отказа или восстановления могут быть использованы отдельные линии перехода.

f) На линиях перехода должны быть указаны соответствующие интенсивности перехода. Их можно указать непосредственно на линиях или в отдельном списке.

g) При возможности, переход должен связывать только соседние состояния. Если отказ по общей причине приводит к отказу двух элементов или более, то такое состояние должно быть исключено.

h) В целях наглядности состояния отказа системы следует выделять (например, жирной линией, цветом или штриховкой).

Применение этих правил проиллюстрировано в приложении В.

9 Анализ

9.1 Общие положения

Целью анализа диаграммы состояний является определение показателей безотказности, готовности, ремонтопригодности и безопасности системы. В вычислениях используют известные математические методы (см. приложения А—С). Задача определения зависимых от времени показателей, например $R(t)$ или $A(t)$, требует больше вычислительных усилий, чем получение асимптотических по-

казателей *A* или средних значений, таких как *MTTF*, *MDT*, *MUT*. Пример выражений для вычисления зависимых от времени показателей представлен в приложении С.

Перед началом анализа следует установить, является ли основной целью анализа диаграммы состояний определение вероятностей промежуточных состояний. Несмотря на то что при исследовании готовности последующие результаты могут быть получены из предыдущих (устремляя t к бесконечности), может быть использована относительно простая математическая процедура, если известно, что требуется только стационарное решение (см. приложение А). С другой стороны, если необходимо получить промежуточное решение, нужны более специализированные процедуры, например преобразование Лапласа или матричная алгебра (см. приложение С). В общем случае выражения для показателей безотказности, готовности, ремонтопригодности и безопасности системы могут быть выведены на основе вероятностей состояний.

Анализ и интерпретация его результатов в основном сосредоточены на различиях между показателями безотказности, готовности, ремонтопригодности и безопасности. Для этого можно рассмотреть восстанавливаемый элемент, который представляют с помощью интенсивности отказов λ и интенсивности восстановлений μ. Как правило, после отказа, в котором задействован данный элемент, для его возвращения в работоспособное состояние должны произойти по крайней мере два события:

- отказ должен быть обнаружен и изолирован (т. е. следует зафиксировать состояние, в котором отказ в дальнейшем не будет иметь последствий);
- элемент должен быть восстановлен и возвращен в работу.

В данном случае время восстановления включает время логистических действий, необходимых для восстановления после обнаружения отказа, фактическое время восстановления (обнаружение отказа, восстановление, замена, проверка) и время возвращения элемента или всей системы в работоспособное состояние.

В общей базовой модели следует рассматривать четыре временных интервала и соотнести их с двумя параметрами (интенсивностью отказов λ и интенсивностью восстановлений μ).

В контексте безотказности, ремонтопригодности или готовности время до обнаружения отказа учитывают при вычислении интенсивности отказов, а время от обнаружения до восстановления отказа — при вычислении интенсивности восстановления. При повышенных требованиях к безопасности не следует полагаться на показатели самотестирования системы или другие аналогичные показатели (что используют при анализе готовности системы), но обнаружение и изоляция должны быть проведены независимо от объекта (конкретные требования и примеры представлены в МЭК 61508). Различия между показателями безотказности, готовности, ремонтопригодности и безопасности — это различия целевых показателей *MTTF*, *MDT* или $A(t)$.

В контексте безопасности фактическим временем восстановления, как правило, пренебрегают, если в течение этого периода получены другие контрольные показатели. В этом случае при вычислении интенсивностей восстановлений в ходе анализа безотказности учитывают полное время изоляции. Однако интерпретации в разных приложениях могут отличаться (пример интерпретации представлен на рисунке 3).

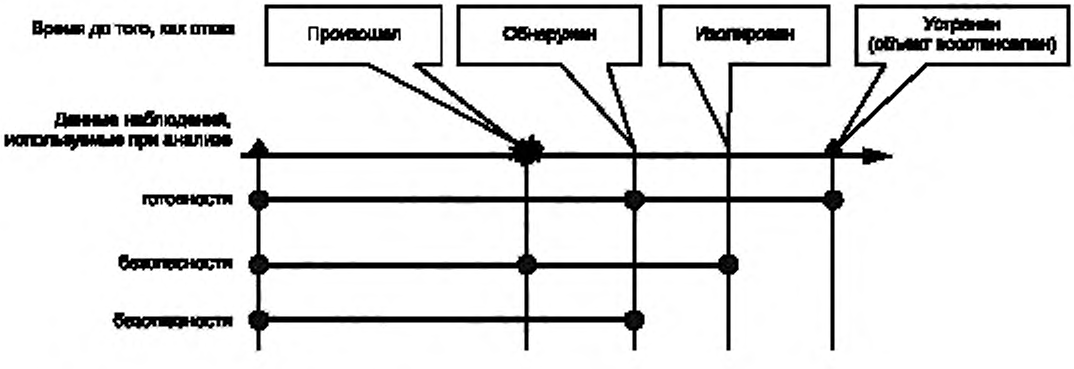


Рисунок 3 — Интерпретация наработки до отказа и времени восстановления в различных ситуациях

Однако основное наблюдение состоит в том, что, хотя модель и используемые математические методы могут быть одинаковыми, интерпретации полученных результатов могут сильно отличаться.

9.2 Анализ показателей безотказности

При анализе безотказности на диаграмме состояний все неработоспособные состояния на уровне системы являются поглощающими состояниями. Вероятность того, что в момент времени *t* система находится в заданном состоянии, вычисляют с помощью специальных математических методов (см. приложения А—С). Когда *t* стремится к бесконечности, вероятность, соответствующая каждому работоспособному состоянию, стремится к нулю, а вероятность поглощающих состояний — к единице.

Распространенным показателем безотказности является *MTTFF*. При оценке по диаграмме состояний *MTTFF* для системы в целом — это средняя продолжительность работоспособного состояния системы до перехода в поглощающее состояние, которая зависит от состояния системы в момент времени $t = 0$; для указания данной зависимости используют обозначение $MTTF_{Si}$ для обозначения *i*-го состояния системы (см. приложение А).

9.3 Анализ показателей готовности и ремонтопригодности

При анализе показателей готовности следует проверить, что каждое состояние на диаграмме состояний и переходов может быть достигнуто из любого другого состояния. Вероятность того, что в момент времени *t* система находится в заданном состоянии, вычисляют с помощью специальных математических методов (см. приложения А—С). Коэффициент готовности $A(t)$ равен сумме вероятностей работоспособных состояний системы. При *t*, стремящемся к бесконечности, вероятность, соответствующая каждому состоянию, стремится к постоянной величине. Коэффициент готовности системы также стремится к постоянному значению А.

Могут быть вычислены и другие полезные показатели (см. приложение А):

- интенсивность отказов на уровне системы;
- средняя продолжительность *i*-го состояния;
- частота перехода в *i*-е состояние;
- частота выхода из *i*-го состояния.

Также, используя вероятности состояний, можно вычислить *MUT* и *MDT* системы, где *MUT* — средняя продолжительность работоспособного состояния, *MDT* — средняя продолжительность неработоспособного состояния.

9.4 Анализ показателей безопасности

Анализ показателей безопасности в основном аналогичен анализу показателей безотказности и готовности. Однако здесь применяют другую терминологию. При анализе безопасности неработоспособные состояния подразделяют на безопасные (в которых система не опасна) и опасные (в которых система опасна).

Целевыми показателями могут быть:

- средняя наработка до возникновения первого опасного отказа *MTTFH*;
- интенсивность опасных отказов *DFR*;
- вероятность отказа по запросу *PFD*.

Показатели *MTTFH* и *DFR* вычисляют аналогично *MTTFF* и интенсивности отказов соответственно. Их рассматривают так же, как и соответствующие показатели безотказности, но только по отношению к опасным неработоспособным состояниям. Значение *PFD* в момент времени *t* представляет собой вероятность того, что система находится в опасном состоянии в момент времени *t* (оценкой *PFD* является коэффициент неготовности в момент времени *t*). В некоторых случаях необходимо получить среднее *PFD* за время *t*, оно может быть получено путем интегрирования *PFD*: $PFD_{avg} = \frac{1}{t}\int_0^t PFD(s)ds$.

10 Документирование результатов

Отчет о результатах анализа должен включать следующие сведения:

a) перечень заданных показателей (например, безотказности, готовности, ремонтопригодности, безопасности);

b) основные используемые предположения, включая их обоснование (например, постоянство интенсивностей отказов и восстановлений);

c) обоснование применимости марковских методов;

d) описание диаграммы состояний, включающее исчерпывающее рассмотрение следующих аспектов:

- идентификация работоспособных и неработоспособных состояний,
- при необходимости, указание причин группировки и исключения некоторых состояний,
- переходы между состояниями,
- выбор числовых значений для интенсивностей переходов,
- предположения, лежащие в основе построения диаграммы;

e) описание:

- методов вычислений,
- программного обеспечения (в случае его использования);

f) численные результаты:

- результаты в числовой и графической формах,
- влияние предположений, использованных при построении диаграммы состояний и при вычислениях,
- анализ чувствительности результатов по отношению к выбранным значениям интенсивностей переходов.

Дополнительная информация приведена в МЭК 60300-3-1.

Приложение А
(справочное)

Основные математические соотношения, используемые в марковских методах

А.1 Общие положения

Сведения, представленные в данном приложении, применимы к однородным по времени марковским процессам с конечным числом состояний и непрерывным временем. Так как для данных процессов характерно отсутствие памяти, распределение продолжительности состояния является экспоненциальным. Например, по отношению к модели безотказности это означает, что интенсивности отказов и восстановлений (λ и μ) — постоянные величины (т. к. не зависят от времени). Интенсивности отказов и восстановлений изменяют значение только при изменении состояния.

А.2 Матрица интенсивностей переходов

А.2.1 Диаграмма состояний

Однородный по времени марковский процесс полностью характеризуется матрицей интенсивностей переходов $Q = [q_{ij}]$ и вектором начальных вероятностей в момент времени $t = 0$. Полезным графическим отображением матрицы интенсивности переходов является диаграмма состояний и переходов. При разработке диаграммы состояний полезно использовать структурную схему надежности (при ее наличии) и FMEA системы. В любом случае для сокращения количества состояний рекомендуется объединять группу, состоящую из n ($n = 2, 3,\ldots$) последовательных элементов, в один элемент с интенсивностью отказов $\lambda_1 +\ldots+ \lambda_n$ и интенсивностью восстановлений $(\lambda_1 +\ldots+ \lambda_n)/(\lambda_1/\mu_1 +\ldots+ \lambda_n/\mu_n)$, при условии $\lambda_i << \mu_i$, где $i = 1,\ldots,n$.

После построения и проверки диаграммы состояний (с учетом тщательного анализа режимов отказов, предполагаемых приоритетов восстановления и характерных особенностей системы) пространство состояний {0, 1,..., m} делят на две совокупности: UP — множество работоспособных состояний и D — множество неработоспособных состояний, где m — общее количество состояний. Множество неработоспособных состояний зависит от исследуемых свойств системы (безотказности или безопасности).

А.2.2 Основные соотношения, используемые для вычислений в марковских методах

А.2.2.1 При анализе показателей безотказности среднюю наработку до отказа системы $MTTF_{Si}$ (если в момент времени $t = 0$ система была в состоянии i) вычисляют следующим образом:

$$MTTF_{Si} = \frac{1}{q_i} + \sum_{\substack{j=0 \\ j \in UP}}^{m} \frac{q_{ij}}{q_i} MTTF_{Sj}, \quad i \in UP, \quad q_i = \sum_{\substack{j=0 \\ j \neq i}}^{m} q_{ij}.$$

Примечание 1 — При корректном определении множества работоспособных состояний UP приведенная выше система алгебраических уравнений также может быть использована для вычисления наработки до опасного отказа (при анализе безопасности).

Примечание 2 — Если в момент времени $t = 0$ система находилась в i-ом состоянии, то точное выражение для вероятности безотказной работы системы $R_{Si}(t)$ вычисляют по формуле (например, используя преобразование Лапласа).

$$R_{Si}(t) = e^{-q_i t} + \sum_{\substack{j=0 \\ j \in UP \\ j \neq i}} \int_0^t q_{ij} e^{-q_i x} R_{Sj}(t-x)dx, \quad i \in UP.$$

А.2.2.2 Выражение для оценки асимптотического или стационарного коэффициента готовности A_s имеет вид:

$$A_s = \sum_{j \in UP} P_j,$$

где

$$P_j = \sum_{\substack{i=0 \\ i \neq j}}^{m} P_i \frac{q_{ij}}{q_i}, \quad j = 0,\ldots,m, \quad P_j > 0, \sum_{j=0}^{m} P_j = 1, \quad q_i = \sum_{\substack{j=0 \\ j \neq i}}^{m} q_{ij}.$$

Так как данные уравнения не являются независимыми, одно уравнение для P_j (произвольно выбранное) может быть заменено следующим соотношением:

$$\sum_{j=0}^{m} P_j = 1.$$

А.2.2.3 В связи с тем, что интенсивность отказов предполагается постоянной, аппроксимацией интервальной вероятности безотказной работы IR_S в стационарном состоянии является

$$IR_S(t, t+\theta) = \sum_{j \in UP} P_j R_{Qj}(\theta) \approx A_S e^{-\theta / MTTF_{eq}},$$

где 0 означает, что все элементы функционируют (или готовы функционировать).

А.2.2.4 Выражение для асимптотической или стационарной интенсивности отказов (частота отказов) на уровне системы z_S имеет следующий вид:

$$z_S = \sum_{\substack{j \in UP \\ i \in D}} P_j q_{ji} = \sum_{j \in UP} P_j \left(\sum_{i \in D} q_{ji} \right).$$

Примечание 1 — В этом выражении должны быть учтены все интенсивности переходов q_{ji} из состояния $j \in UP$ в состояние $i \in D$.

Примечание 2 — Для малых значений Δt величина $z_S \Delta t$ является вероятностью перехода из состояния, принадлежащего множеству работоспособных состояний, в состояние, относящееся к множеству неработоспособных состояний (и наоборот) за период времени $(t, t + \Delta t)$ для произвольного времени t (установившееся состояние).

А.2.2.5 Выражения для MUT_S (средняя продолжительность работоспособного состояния на уровне системы) и MDT_S (средняя продолжительность неработоспособного состояния на уровне системы) для стационарного состояния имеют следующий вид:

$$MUT_S = \frac{A_S}{z_S} \quad \text{и} \quad MDT_S = \frac{1 - A_S}{z_S}.$$

Примечание — $MUT_S + MDT_S = 1/z_S$, где z_S — асимптотическая и установившаяся интенсивность отказов (частота отказов) на уровне системы в соответствии с А.2.2.4.

А.2.2.6 Для заданного i-го состояния справедливо следующее:

$1/q_i$ — безусловная средняя продолжительность i-го состояния;

$P_j(t)q_j$ — частота выхода из i-го состояния.

$\sum_{j=0}^{m} P_j(t) q_{ji} \Delta t$ — безусловная вероятность перехода в i-е состояние в течение периода времени $(t, t + \Delta t)$ при малом Δt.

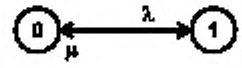
Для больших последовательно-параллельных структурных схем известны приближенные выражения, которые можно найти в литературных источниках. Для очень больших сложных систем используют метод моделирования Монте-Карло.

Приложение В
(справочное)

Пример построения диаграммы состояний

В.1 Система с одним элементом

Применение марковских методов начинают с определения состояний системы. В качестве примера рассмотрена система с одним элементом. В простейшем случае диаграмма состояний включает только два состояния: работоспособное состояние с интенсивностью отказов λ. и неработоспособное состояние с интенсивностью восстановлений μ (см. рисунок В.1).



0 — работоспособное состояние системы; 1 — неработоспособное состояние системы

Рисунок В.1 — Диаграмма состояний для восстанавливаемой системы, состоящей из одного элемента

Стрелка от состояния 0 к состоянию 1 означает появление отказа с вероятностью $\lambda\Delta(t)$ в течение периода времени $(t, t+\Delta t)$ при условии, что система находилась в состоянии 0 в момент времени t; стрелка от состояния 1 к состоянию 0 — завершение восстановления системы с вероятностью $\mu\Delta t$ в течение времени Δt.

Систему, состоящую из одного элемента, можно изобразить, используя более чем два состояния (работоспособное и неработоспособное). Ухудшенное состояние, в котором система все еще является работоспособной, также может быть включено в диаграмму. На рисунке В.2 состоянием отказа системы является состояние 2 (при этом предполагается, что в этом состоянии восстановление невозможно).

0 — состояние полного функционирования системы, 1 — ухудшенное состояние системы;
2 — неработоспособное состояние системы (состояние поглощения)

Рисунок В.2 — Диаграмма состояний для системы, состоящей из одного элемента с использованием трех состояний

Если восстановление в состоянии 2 возможно, система может быть описана диаграммой, изображенной на рисунке В.3, на которой интенсивность восстановлений μ_2 представляет собой интенсивность перехода из состояния 2 в состояние 1.

Рисунок В.3 — Диаграмма состояний, если возможно восстановление системы из состояния 2

Во многих случаях должен быть рассмотрен путь непосредственного перехода системы из состояния 0 в состояние 2. В этом случае в диаграмму состояний, изображенную на рисунке В.2, добавляют стрелку λ_3 (рисунок В.4).

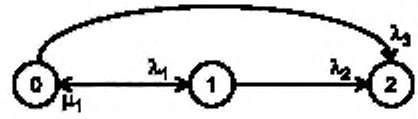


Рисунок В.4 — Диаграмма состояний системы, состоящей из одного элемента, с прямым переходом из состояния 0 в состояние 2

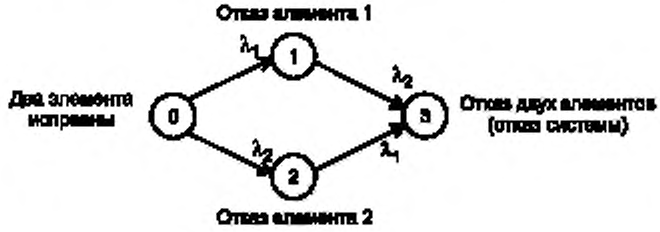
Диаграмма, представленная на рисунке В.1, может быть использована для определения оценки мгновенной готовности $A(t)$ и асимптотической готовности. Для оценки вероятности безотказности работы $R(t)$ необходима диаграмма состояний, представленная на рисунке В.5, в которой рассмотрена только интенсивность отказов λ, а состояние 1 является поглощающим состоянием.

Рисунок В.5 — Диаграмма состояний для анализа вероятности безотказной работы системы, состоящей из одного элемента

В.2 Система, состоящая из двух элементов

Так как каждый элемент может находиться в двух состояниях: 0 — работоспособном и 1 — неработоспособном, система может быть в четырех состояниях (0 0), (0 1), (1 0), (1 1). Если система, состоящая из двух элементов, является последовательной, то состояние (0 0) является ее единственным работоспособным состоянием, а (0 1), (1 0), (1 1) — неработоспособными состояниями. Если в системе с двумя элементами использован нагруженный или ненагруженный резерв, то состояния (0 0), (0 1), (1 0) являются работоспособными состояниями. В соответствии с этим может быть получено решение для системы с нагруженным резервом типа «1 из 2».

Диаграмма состояний системы (с нагруженным резервом типа «1 из 2») с невосстанавливаемыми элементами приведена на рисунке В.6.



Примечание — Обозначения состояний могут иметь следующий вид: (0 0), (0 1), (1 0), (1 1) для состояний 0, 1, 2, 3 соответственно.

Рисунок В.6 — Диаграмма состояний для системы состояний из двух невосстанавливаемых элементов типа «1 из 2»

Диаграмма состояний системы из двух восстанавливаемых элементов приведена на рисунке В.7. Дополнительные стрелки указывают на восстановление с интенсивностями μ_i (i = 1,2). Предполагается, что не существует ограничений ресурсов для восстановления системы (из состояния 3).

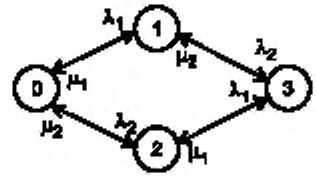


Рисунок В.7 — Диаграмма состояний системы, состоящей из двух восстанавливаемых элементов типа «1 из 2» без ограничения ресурсов для восстановления

Если отказ по общей причине одновременно вызван отказом обоих элементов восстанавливаемой системы типа «1 из 2», скорее всего время, необходимое для восстановления системы после такого отказа (возвращение системы из состояния 3 в состояние 0) отличается от времени, необходимого для восстановления системы после отказов отдельных элементов. Это следует учитывать, как показано на рисунке В.8, где λ_C и μ_C — интенсивности отказа по общей причине и его восстановления соответственно.

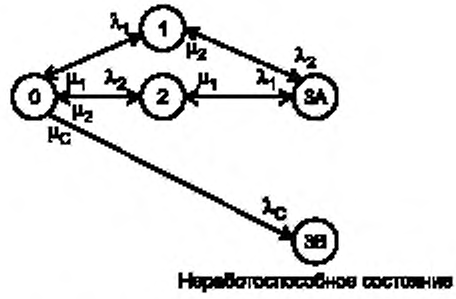


Рисунок В.8 — Диаграмма состояний системы, состоящей из двух восстанавливаемых элементов в нагруженном резерве типа «1 из 2», с общей причиной отказа элементов системы при наличии двух групп, осуществляющих восстановление элементов

В качестве примера рассмотрена система, состоящая из двух генераторов в нагруженном резерве, которые не включаются при низкой температуре. Когда система достигает состояния «оба генератора не включились», время восстановления зависит от того, находится ли каждый генератор в неработоспособном состоянии из-за механического отказа или оба генератора не включились вследствие общей причины, например воздействия низкой температуры. Поэтому необходимо рассмотреть состояние «оба генератора не включились по независимым причинам» отдельно от состояния «оба генератора не включились вследствие общей причины». Однако для пользователя системы может быть важно только то, что «оба генератора отказали» без учета причин этих отказов. Таким образом, из этих двух состояний формируют комбинированное состояние, используя которое можно анализировать безотказность, готовность, ремонтопригодность и безопасность системы.

В диаграмме состояний системы могут быть учтены стратегии технического обслуживания и ремонта, но при этом особое внимание следует уделить свойству отсутствия памяти модели. Предположим, что существует только одна группа ремонтных рабочих и стратегия технического обслуживания и ремонта является такой, что приоритет ремонта всегда принадлежит компоненту, который отказал раньше. В этом случае должен быть учтен порядок возникновения отказов. Такая диаграмма состояний приведена на рисунке В.9.

На рисунке В.9 состояния 3 и 4 имеют следующее значение:

- состояние 3 — два компонента отказали, первым отказал компонент 1;
- состояние 4 — два компонента отказали, первым отказал компонент 2.

Следует отметить, что в соответствии с диаграммой состояний, представленной на рисунке В.9, среднее время восстановления компонента, например компонента 1, в действительности превышает $MTTR = 1/\mu_1$. В силу свойства отсутствия памяти модели если в состоянии 1 возникает второй отказ, то время восстановления до второго отказа не учитывается после перехода в состояние 3, где снова начинается восстановление компонента 1. Для компенсации избыточного времени восстановления можно увеличить интенсивности оставшихся восстановлений. В случае, представленном на рисунке В.9, интенсивности восстановления в состояниях 3 и 4 с целью такой компенсации должны быть удвоены. В других случаях резервирования и при отсутствии мгновенного восстановления компенсация становится более сложной.

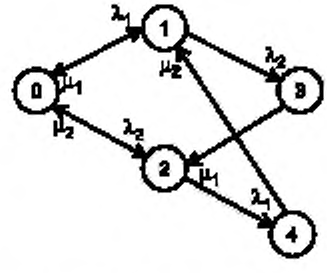


Рисунок В.9 — Диаграмма состояний при наличии только одной группы ремонта и с приоритетом восстановления по принципу «первым вошел/первым вышел»

В.3 Группировка в диаграмме состояний

Для облегчения вычислений следует строить диаграмму состояний с минимально возможным количеством состояний. Если предполагается, что элементы параллельного соединения независимы и имеют одну и ту же ин-

тенсивность отказов λ и одну и ту же интенсивность восстановлений μ, как показано на рисунке В.10 для системы «2 из 4», то диаграмма состояний может быть представлена с применением группировки элементов, как показано на рисунке В.11. Предполагается, что система, представленная на рисунке В.11, имеет неограниченные ресурсы для восстановления. Отказ системы возникает при отказе трех элементов, и дальнейшие отказы не рассматривают.

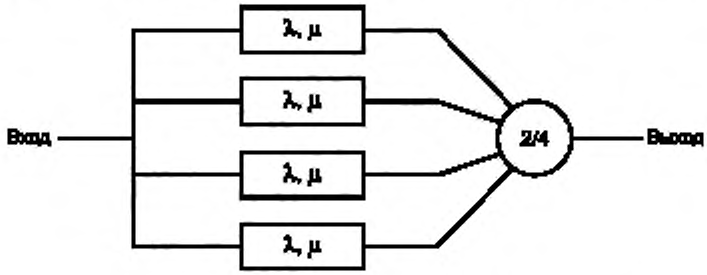


Рисунок В.10 — Блок-схема надежности восстанавливаемой системы типа «2 из 4»

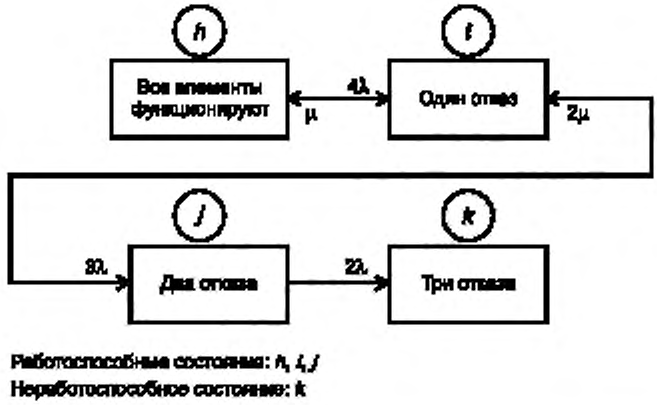


Рисунок В.11 — Диаграмма состояний с группировкой элементов для вычисления показателей безотказности системы, представленной на рисунке В.10

На основе представленной выше диаграммы могут быть составлены и решены алгебраические уравнения (см. приложение А), позволяющие получить выражение для наработки до отказа системы $MTTF_{S0}$ при условии, что $t = 0$ и все четыре элемента работоспособны

$$MTTF_{S0} = \frac{1}{4\lambda}\left(\frac{\mu}{3\lambda}\cdot\frac{2\mu}{2\lambda}+\frac{\mu}{3\lambda}+1\right)+$$
$$+\frac{1}{3\lambda}\left(\frac{2\mu}{2\lambda}+1\right)+$$
$$+\frac{1}{2\lambda}.$$

Приложение С
(справочное)

Пример анализа некоторых показателей безотказности, готовности, ремонтопригодности и безопасности для системы типа «1 из 2» с активным резервом

С.1 Объект

Ниже рассмотрены системы с активным резервом типа «1 из 2» без учета ограничений на восстановление. Анализируемыми показателями являются коэффициент готовности (мгновенный), асимптотический коэффициент готовности, вероятность безотказной работы и *MTTF*. При этом использованы стандартные для данных задач математические методы.

С.2 Моделирование

Диаграмма состояний системы типа «1 из 2» с активным резервом, приведенная на рисунке С.1, построена для определения оценки коэффициента готовности. Состояние 3 — неработоспособное состояние.

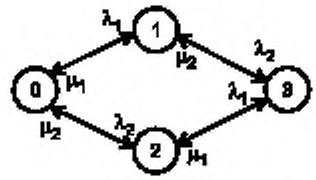


Рисунок С.1 — Диаграмма состояний системы типа «1 из 2» с активным резервом с различными элементами и двумя группами восстановления

Следует отметить, что диаграмму состояний для анализа вероятности безотказной работы $R(t)$ получают путем исключения переходов восстановления из состояния 3 в состояния 1 и 2. Таким образом, состояние 3 становится поглощающим состоянием.

Предполагая, что два элемента системы являются идентичными или имеют одинаковые интенсивности отказов и восстановлений, можно получить редуцированную диаграмму, приведенную на рисунке С.2.

Рисунок С.2 — Диаграмма состояний системы типа «1 из 2» с активным резервом с идентичными элементами, двумя группами восстановления и неограниченными ресурсами для восстановления

Следует отметить, что диаграмму состояний для анализа вероятности безотказной работы $R(t)$ можно получить путем исключения перехода восстановления из состояния 2 в состояние 1. Таким образом, состояние 2 становится поглощающим состоянием.

С.3 Метод дифференциальных уравнений

С.3.1 Выражения для показателей готовности

Пусть $P_0(t)$, $P_1(t)$, $P_2(t)$ — вероятности того, что в момент времени t система находится в состоянии 0, 1 и 2 соответственно (см. рисунок С.2). Согласно диаграмме состояний (см. рисунок С.2) могут быть записаны следующие дифференциальные уравнения:

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t) + \mu P_1(t),$$

$$\frac{dP_1(t)}{dt} = -2\lambda P_0(t) - (\lambda + \mu) P_1(t) + 2\mu P_2(t),$$

$$\frac{dP_2(t)}{dt} = \lambda P_1(t) - 2\mu P_2(t).$$

На основе диаграммы состояний также может быть построена матрица интенсивностей переходов:

$$Q(\lambda,\mu)=\begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix}.$$

Можно записать матричное дифференциальное уравнение $\frac{d}{dt}P(t)=Q(\lambda,\mu)^T\cdot P(t)$,

где $P(t)=[P_0(t)\ P_1(t)\ P_2(t)]^T$.

Затем находят собственные значения $\varepsilon(\lambda,\mu)$ и собственные векторы $E(\lambda,\mu)$ матрицы Q^T. В случае различных собственных значений (что имеет место для большинства непрерывных марковских моделей и практически всех значений параметров) вектор вероятностей состояний имеет следующий вид:

$$P(t)=E(\lambda,\mu)\cdot\begin{bmatrix} \exp(\varepsilon(\lambda,\mu)_0 t) & & \\ & \exp(\varepsilon(\lambda,\mu)_1 t) & \\ & & \exp(\varepsilon(\lambda,\mu)_2 t) \end{bmatrix}\cdot E(\lambda,\mu)^{-1}\cdot P(0).$$

Решая представленное выше матричное уравнение, вероятности $P_0(t)$, $P_1(t)$, $P_2(t)$ вычисляют, предполагая, например, что в момент времени $t = 0$ система находится в состоянии 0, т. е.

$$P(0)=\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Мгновенный коэффициент готовность $A_{S0}(t)$ вычисляют по формуле

$$A_{S0}(t)=P_0(t)+P_1(t).$$

Индекс $S0$ в $A_{S0}(t)$ указывает на то, что коэффициент готовности определяют на уровне системы в предположении, что в момент времени $t = 0$ система находилась в состоянии 0. Для простой системы явное выражение $A_{S0}(t)$ через λ и μ можно вывести с помощью преобразования Лапласа по формуле

$$A_{S0}(t)=\frac{\mu^2+2\lambda\mu}{(\lambda+\mu)^2}+\left(\frac{\lambda}{\lambda+\mu}\right)^2 e^{-(\lambda+\mu)t}\left(2-e^{-(\lambda+\mu)t}\right).$$

На рисунке С.3 представлен численный пример, показывающий изменение коэффициента неготовности во времени $U_{S0}(t) = 1 - A_{S0}(t)$.

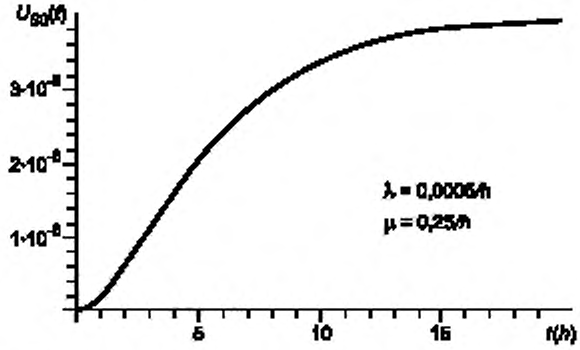


Рисунок С.3 — Численный пример изменения коэффициента неготовности во времени

В общем случае для работы с дифференциальными уравнениями следует применять соответствующее программное обеспечение, позволяющее получить численное или графическое решение.

Асимптотический коэффициент готовности $A_{S0}(\infty) = A_S$ получают непосредственно по формуле $A_{S0}(t)$. Наоборот, устанавливая $P_i(\infty) = P_i$ (i = 0, 1, 2) для асимптотических и установившихся значений вероятностей состояний, A_S получают в виде $A_S = P_0 + P_1$, где P_i являются решениями следующей системы уравнений (см. приложение А):

$$0 = -2\lambda P_0 + \mu P_1,$$
$$0 = -2\lambda P_0 - (\lambda + \mu) P_1 + 2\mu P_2,$$
$$0 = \lambda P_1 - 2\mu P_2.$$

Любое из трех приведенных алгебраических уравнений, представленных выше, может быть получено из оставшихся двух; таким образом, имеется три переменных и только два линейно независимых уравнения. Поэтому в качестве третьего уравнения используют условие на сумму вероятностей $P_0 + P_1 + P_2 = 1$. После некоторых математических преобразований получено следующее выражение:

$$A_S = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2}.$$

В соответствии с приведенным выражением выведены следующие формулы для MUT_S и MDT_S:

$$MUT_S = \frac{A_S}{z_S} = \frac{2\lambda + \mu}{2\lambda^2},$$

$$MDT_S = \frac{1 - A_S}{z_S} = \frac{1}{2\mu},$$

где $z_S = P_1\lambda = \dfrac{2\mu\lambda^2}{(\lambda + \mu)^2}$.

z_S является предельной и стационарной интенсивностью отказов (частотой отказов) на уровне системы (см. приложение А).

С.3.2 Выражения для вероятности безотказной работы

Для определения выражений для вероятности безотказной работы и наработки до отказа системы типа «1 из 2» с активным резервом (независимо от количества групп восстановления) состояние 2 (неработоспособное состояние системы) является поглощающим состоянием. Приведенные ниже дифференциальные уравнения записаны в соответствии с диаграммой состояний, приведенной на рисунке С.2, и невозможности перехода из состояния 2 в состояние 1:

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t) + \mu P_1(t),$$
$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - (\lambda + \mu) P_1(t),$$
$$\frac{dP_2(t)}{dt} = \lambda P_1(t).$$

Решая эту систему уравнений, находят вероятности $P_0(t)$, $P_1(t)$, $P_2(t)$, предполагая, что в момент времени $t = 0$ система находилась в состоянии 0:

$$P(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Вероятность безотказной работы системы $R_{S0}(t)$ вычисляют по формуле

$$R_{S0}(t) = P_0(t) + P_1(t).$$

Явное выражение $R_{S0}(t)$ через λ и μ может быть получено с помощью преобразования Лапласа и имеет следующий вид:

$$R_{S0}(t) = \frac{s_1 e^{s_2 t} - s_2 e^{s_1 t}}{s_1 - s_2},$$

где

$$s_1 s_2 = 2\lambda^2,$$

$$s_1 + s_2 = -(\mu + 3\lambda).$$

Выражение для $MTTF_{S0}$ может быть найдено или на основе $R_{S0}(t)$, в этом случае

$$MTTF_{S0} = \int_0^\infty R_{S0}(t)dt = \frac{\mu + 3\lambda}{2\lambda^2}$$

или согласно системе алгебраических уравнений, приведенной в А.2.2.1.

С.3.3 Выражения для показателей безопасности

Анализ показателей безопасности отличается только интерпретацией модели: состояние 2 должно быть определено как опасное состояние, а переход в это состояние происходит при отказе обоих элементов или если оба элемента отказывают в одно и то же время вследствие отказа по общей причине (в последнем случае диаграмма состояний должна быть расширена, как показано на рисунке В.8). При этом время восстановления следует рассматривать как время проверки.

Выражение для *PFD* такое же, как для коэффициента неготовности системы. При анализе *MTTFH* или *DFR* состояние 2 следует рассматривать как поглощающее состояние, вывод аналогичен выводам для показателей безотказности.

На рисунке С.4 показан численный пример для показателя *DFR*, полученного из соотношений для вероятности безотказной работы системы.

$$h_S(t) = \frac{-\frac{d}{dt} R_S(t)}{R_S(t)}$$

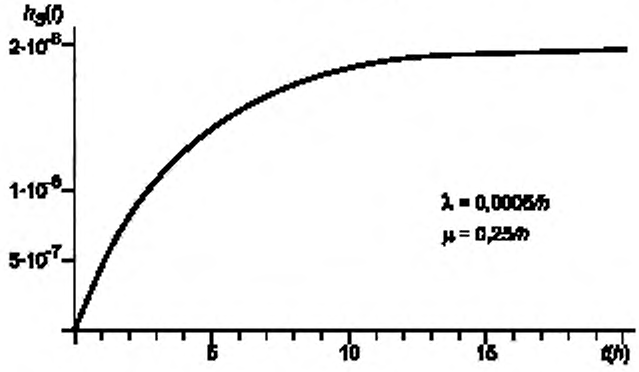


Рисунок С.4 — Численный пример для интенсивности опасных отказов

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60050(191):1990	NEQ	ГОСТ 27.002—2015 «Надежность в технике. Термины и определения»
IEC 60300-3-1	MOD	ГОСТ Р 51901.5—2005 (МЭК 60300-3-1:2003) «Менеджмент риска. Руководство по применению методов анализа надежности»
IEC 61508-4:2010	IDT	ГОСТ Р МЭК 61508-4—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»

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

- IDT — идентичный стандарт;
- MOD — модифицированный стандарт;
- NEQ — неэквивалентный стандарт.

Приложение ДБ
(справочное)

Сведения о соответствии ссылочных международных стандартов, указанных в библиографии настоящего стандарта, национальным стандартам

Таблица ДБ.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60812:2006	MOD	ГОСТ Р 51901.12—2007 (МЭК 60812:2006) «Менеджмент риска. Метод анализа видов и последствий отказов»
IEC 61025:2006	NEQ	ГОСТ Р 27.302—2009 (МЭК 61025:2006) «Надежность в технике. Анализ дерева неисправностей»
IEC 61078:2006	MOD	ГОСТ Р 51901.14—2007 (МЭК 61078:2006) «Менеджмент риска. Структурная схема надежности и булевы методы»

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

- MOD — модифицированные стандарты;
- NEQ — неэквивалентный стандарт.

Библиография

[1] IEC 60812 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[2] IEC 61025 Fault tree analysis (FTA)

[3] IEC 61078 Analysis techniques for dependability – Reliability block diagram method and Boolean methods

[4] Ajmone Marsan, M., Balbo, G.,Conte, G.: Performance models of multi-processor systems, MIT Press, Cambridge, 1986 (Application of Markov models and Petri nets to computer systems performance evaluation)

[5] Billinton R., Allan, R.N.: Reliability Evaluation of Engineering Systems. Concepts and Techniques. Second Edition, New York, Plenum Press, 1992 (Many examples of practical application of Markov models)

[6] Birolini A.: Reliability Engineering: Theory and Practice. 4th Edition, Berlin/Heidelberg/New York, Springer-Verlag, 2004. (Theoretical basis of Markov models, with many applications, approximations)

[7] Brémaud P.: Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues. Springer, New York, 1998 (Theoretical basis of Markov models, with applications)

[8] Bux, W., Herzog, U.: The Phase Concept: Approximation of Measured Data and Performance Analysis, in: Chandy, K. M., Reiser, M. (eds.): Computer Performance, North Holland, 1977, 23—38 (Explanation of the phase concept and algorithm for practical approximation)

[9] Buzacott, J.A.: Markov approach to finding failure times of repairable systems. IEEETransactions on Reliability, 1970, Vol.R-19, No.4, pp.128—134. (Matrix algebra approach for MTTTF, MUT, MDT etc.) Çinlar, E.: Introduction to Stochastic Processes. Englewood Cliffs, Prentice Hall, 1975 (Theoretical basis of Markov models, with applications)

[10] Dhillon, B.S., Singh C.: Engineering Reliability, New Techniques and Applications. New York, Wiley, 1981 (Many examples of practical application of Markov models)

[11] Endrenyi, J.: Reliability Modelling in Electric Power Systems. New York, Wiley, 1978 (Many examples of practical application of Markov models; changing weather conditions etc.)

[12] Gaede, K.W.: Zuverlässigkeit, Mathematische Modelle. München, Carl Hanser Verlag, 1977 (Theoretical basis of Markov models, with applications)

[13] Høyland, A.: Rausand M., System Reliability Theory. Models and Statistical Methods, New York, Wiley, 1994 (Many examples of practical application of Markov models)

[14] Keilson J., Markov Chain Models: Rarity and Exponentiality. Berlin, Springer Verlag, 1979 (Theoretical basis of Markov models, with applications; uniformization method)

[15] Kulkarni V., Modeling and Analysis of Stochastic Systems. London, Chapman & Hall, 1995 (Theoretical basis of Markov models, with applications, uniformization method)

[16] Kumar S., Grassmann W., Billinton R., A stable algorithm to calculate steady-state probability & frequency of a Markov system. IEEE Transactions on Reliability, 1987, Vol.R-36, No.1, pp.58—62 (Very simple and efficient algorithms for the steady-state probabilities calculation)

[17] Lisnianski A., Levitin G., Multi-state System Reliability. Assessment, Optimization and Applications. New Jersey, World Scientific, 2003 (Application of Markov models for multistate systems, with examples)

[18] Moorsel A.P.van, Sanders W.H., Transient solution of Markov models by combining adaptive and standard uniformization. IEEE Transactions on Reliability, 1997, Vol.46, No.3, pp. 430—440. (Recent paper on uniformization methods)

[19] Murphy, K., Carter, C. und Brown, S.: The Exponential Distribution: the Good, the Bad and the Ugly. A practical Guide to its Implementation, Proc. RAMS2002 (Discussion of the constant failure rate property and its pitfalls)

[20] Pagés A., Gondran A., System Reliability. Evaluation and Prediction in Engineering. 1986, Berlin, Springer Verlag (Theoretical basis of Markov models, with applications; approximations)

[21] Pukite J., Pukite P., Modeling for Reliability Analysis: Markov Modeling for Reliability, Maintainability, Safety, and Supportability Analyses of Complex Systems. Wiley-IEEE Press, 1998 (Many examples of practical application of Markov models)

[22] Reinschke K., Zuverlässigkeit von Systemen. Bd.1: Systeme mit endlich vielen Zuständen. Berlin, VEB Verlag Technik, 1973 (Theoretical basis of Markov models, with applications; matrix algebra methods)

[23] Reinschke K., Ušakov I.A., Zuverlässigkeitsstrukturen. Modellbildung, Modellauswertung. Berlin, VEB Verlag Technik, Berlin, 1987 (Theoretical basis of Markov models, with applications)

[24] Ross S.M., Stochastic processes. Second edition. New York, Wiley, 1996. (Theoretical basis of Markov models, with applications) Ross S.M., Introduction to Probability Models. Seventh Edition. Boston, Academic Press, 2000 (Theoretical basis of Markov models, with applications)

[25] Schweitzer P., A survey of aggregation-disaggregation in large Markov chains, in W.J. Stewart, editor: Numerical Solution of Markov Processes, chapter 4, pp. 63—88 New York, Marcel Dekker, 1991 (Aggregation methods, including lumping)

[26] Singh C., Billinton R., System Reliability Modelling and Evaluation. London, Hutchinson, 1977 (Many examples of practical application of Markov models, basis of Markov techniques, lumping, duration and frequency methods)

[27] Stewart W.J., Introduction to the Numerical Solution of Markov Chains. Princeton, Princeton University Press, 1994 (Numerical method for Markov techniques)

[28] Tijms H.C., Stochastic Models. An Algorithmic Approach. New York, Wiley, 1994 (Theoretical basis of Markov models, with applications; algorithms; passage times; uniformization method)

[29] Villemeur A., Reliability, Availability, Maintainability and Safety Assessment. Volume 1. Methods and Techniques, Chichester, Wiley, 1992 (Theoretical basis of Markov models, with many applications; approximation methods)

[30] Yoshimura, I., Sato, Y., Suyama, K.: Safety Integrity Level Model for Safety-related Systems in Dynamic Demand State, Proceedings of the 2004 Asian International Workshop on Advanced Reliability Modeling (AIWARM 2004), pp. 577—584, Hiroshima, Japan (Application of Markov techniques to programmable electronic safety systems)

УДК 62-192:658.562:006.354 ОКС 03.120.01; 03.120.30; 21.020

Ключевые слова: марковские методы, диаграмма состояний и переходов, интенсивность отказов, интенсивность восстановлений, состояние, переход, показатели надежности, показатели готовности, показатели ремонтопригодности, показатели безопасности

БЗ 9—2019/62

Редактор *Л.С. Зимилова*
Технические редакторы *И.Е. Черепкова, В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 09.09.2019. Подписано в печать 19.09.2019. Формат 60×84¼. Гарнитура Ариал
Усл. печ. л. 3,72. Уч.-изд. л. 3,16.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru