ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 27.011— 2019 (IEC/TR 63039:2016)

Надежность в технике

ВЕРОЯТНОСТНЫЙ АНАЛИЗ РИСКА ТЕХНИЧЕСКИХ СИСТЕМ

Оценка интенсивности конечного события для заданного исходного состояния

(IEC/TR 63039:2016, Probablistic risk analysis of technological systems — Estimation of final event rate at a given initial state, MOD)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

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 документа, 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 30 октября 2019 г. № 1226-ст

4 Настоящий стандарт является модифицированным по отношению к международному документу IEC/TR 63039:2016 «Вероятностный анализ риска технических систем. Оценка интенсивности конечного события для заданного начального состояния» (IEC/TR 63039:2016 «Probablistic risk analysis of technological systems — Estimation of final event rate at a given initial state», MOD) путем внесения технических отклонений, объяснение которых приведено во введении к настоящему стандарту.

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

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

5 ВВЕДЕН ВПЕРВЫЕ

*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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2020

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

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины, определения и сокращения 3
4 Различия терминов частоты и интенсивности конечного события 9
5 Частота конечного события и интенсивность конечного события для заданного начального состояния 10
6 Процедура вероятностного анализа риска и составление профиля риска 13
7 Методы количественного анализа появления конечного события 14
8 Интенсивность конечного события для выявленного состояния и выявленной группы состояний 26
9 Анализ нескольких уровней защиты 29
Приложение А (справочное) Риск, обусловленный отказом, выявленным только при запросе 45
Приложение В (справочное) Применение в области функциональной безопасности 50
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе 56
Библиография 58

Введение

Настоящий стандарт определяет основные свойства событий с точки зрения вероятностного анализа риска и использования связанных с надежностью методов анализа возникновения конечного события, переводящего объект в конечное состояние, в котором могут появиться конечные последствия риска (см. 3.1.1, 3.1.10 и 3.1.17).

Методы, применяемые для анализа риска, такие как контрольные перечни, анализ что/если, исследование опасности и работоспособность (HAZOP), анализ дерева событий (ETA), анализ дерева неисправностей (FTA) первоначально были разработаны для анализа безопасности систем и затем были глубоко проработаны для анализа надежности и безопасности систем [1], [2], ГОСТ Р 27.012, ГОСТ Р МЭК 61165, ГОСТ Р 27.302, ГОСТ Р МЭК 62502. Аналитические методы, описанные в ГОСТ Р 27.302, ГОСТ Р МЭК 61165, ГОСТ Р МЭК 62502 четко установлены и систематизированы применительно к анализу надежности. Однако необходимо учитывать, что существуют значительные различия между анализом надежности и вероятностным анализом риска.

Во-первых, такие состояния объекта как работоспособное и неработоспособное, рабочее и нерабочее, а также события отказа и восстановления, как правило, рассматривают с позиции анализа надежности [1], ГОСТ Р 27.010. Вероятностный анализ риска часто связан не только с аспектами состояний и событий, которые влияют на работоспособное и неработоспособное состояния, но также с состояниями наличия запроса и его отсутствия, с начальными, промежуточными и конечными состояниями, а также с такими дополнительными событиями как запрос, завершение, окончание и возобновление запроса (см. 3.1.3, 3.1.8, 3.1.10, 3.1.11, 3.1.17 и 3.1.20).

Во-вторых, при вероятностном анализе риска учитывают тип конечного события, поскольку существующие в системе зависимости часто определяют появление конечного события. А именно, в вероятностном анализе риска конечные события делят на повторяемые и неповторяемые (см. 3.1.18 и 3.1.19). Кроме того, часто необходимо учитывать последовательность появления событий, поскольку часто появление конечного события является следствием определенной последовательности событий (см. 7.2, 9.2, 9.3 и 9.4).

Количественными показателями, применяемыми при анализе надежности, обычно являются интенсивность отказов, частота отказов, интенсивность восстановлений и другие показатели безотказности, готовности и ремонтопригодности объекта. При анализе риска должны быть проанализированы не только эти показатели, но и дополнительные показатели, такие как интенсивность и частота таких событий как запрос, завершение и возобновление запроса, а также время воздействия или экспозиция риска (см. 3.1.30).

При проведении количественного анализа риска интенсивность и частоту событий обычно используют в качестве целевых показателей появления конечного события (см., например, приложение В). В настоящем стандарте в качестве целевых показателей появления конечного события рассмотрены частота конечного события (FEF), средняя FEF, интенсивность конечного события (FER) для заданного начального состояния и FEF для заданного начального состояния (см. 3.1.21, 3.1.22, 3.1.25 и 3.1.26).

Такие показатели как FEF для заданного начального состояния являются новыми для вероятностного анализа риска и значительно отличаются от показателей традиционного анализа надежности, упомянутых выше, поскольку такие переменные, как интенсивность запросов и завершения запросов и их частота, а также экспозиция риска, которую не рассматривают в традиционном анализе надежности, обычно не являются целевыми показателями надежности. Поэтому эти новые показатели должны быть определены, а соответствующие методы модифицированы применительно к вероятностному анализу риска.

Кроме того, при анализе риска сложных систем часто дополнительно применяют такие аналитические методы как HAZOP, FMEA, RBD, FTA и марковских методов. В настоящем стандарте показано, как сформировать эти модифицированные методы, чтобы извлечь максимальную пользу при их применении в вероятностном анализе риска.

Таким образом в настоящем стандарте определены целевые показатели появления конечного события в виде FER для заданного начального состояния, FER для заданного состояния и FER для заданной группы состояний при проведении вероятностного анализа риска и даны рекомендации по применению модифицированных методов в дополнение к анализу этих целевых показателей на примере анализа риска атомной электростанции, подушек безопасности автомобиля, систем автоматического торможения и рулевого управления в автомобиле, систем с распознаванием отказа только при запросе, а также рекомендации по применению настоящего стандарта в области функциональной безопасности.

Считается, что вероятностный анализ риска является более сложным, чем анализ надежности. Однако в настоящем стандарте приведен более простой и реалистичный подход проведения вероятностного анализа риска (по сравнению с традиционными подходами), что позволяет более просто проводить анализ риска сложных систем (см. таблицу 1; раздел 6; 9.1, 9.2, 9.5, А.5 и В.3).

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежность в технике

ВЕРОЯТНОСТНЫЙ АНАЛИЗ РИСКА ТЕХНИЧЕСКИХ СИСТЕМ

Оценка интенсивности конечного события для заданного исходного состояния

Dependability in technics. Probablistic risk analysis of technological systems.
Estimation of final event rate at a given initial state

Дата введения — 2020—07—01

1 Область применения

В настоящем стандарте приведены рекомендации по вероятностному анализу риска (далее — анализ риска) систем, состоящих из электротехнических объектов, применимых на производстве, где предусмотрено проведение анализа риска.

Настоящий стандарт включает следующие аспекты анализа риска:

- определение основных терминов и понятий;
- установление типов событий;
- классификация возникновения событий;
- описание использования модифицированных обозначений и методов графического представления для ETA, FTA и марковских методов при применении модифицированных методов к сложным системам;
- предполагаемые способы обработки частоты/интенсивности событий для сложных систем;
- предполагаемые способы определения оценок частоты/интенсивности событий на основе мониторинга риска;
- иллюстративные и практические примеры.

Взаимосвязь событий, рассматриваемых в настоящем стандарте с соответствующими рисками, описана в таблице 1. Риск определяют как влияние неопределенности на достижение цели (см. 3.1.1). Здесь предполагается, что неопределенность состоит из двух составляющих: эпистемической и случайной. Эпистемическая составляющая может быть известной и неизвестной, а влияние случайной составляющей может быть контролируемым и неконтролируемым соответственно. Таким образом, риск, соответствующий известному событию, влияние которого является контролируемым, представляет собой контролируемый риск, а риск, соответствующий известному событию, влияние которого является не контролируемым, представляет собой неконтролируемый риск определенной последовательности событий. Контролируемый мета-риск соответствует неизвестному событию, влияние которого может быть случайным контролируемым (если это событие возникает), а неконтролируемый мета-риск соответствует неизвестному событию, влияние которого не является контролируемым.

Например, риски, возникающие в результате случайных отказов аппаратных средств электротехнических объектов, могут быть отнесены к контролируемым или неконтролируемым рискам, в то же время риски, связанные с программными ошибками, могут быть отнесены к контролируемым или неконтролируемым мета-рискам. В настоящем стандарте рассмотрены контролируемые и неконтролируемые риски, возникающие в результате событий, появление которых предполагается случайным и не зависящими от времени (см. раздел 6; 9.1, 9.2, 9.5 и В.3).

Издание официальное

Таблица 1 — События и соответствующие им риски

Событие		
Случайное	Эпистемологическое	
	Известное	Неизвестное
Контролируемое	Контролируемый риск события	Контролируемый мета-риск
Неконтролируемое	Неконтролируемый риск события	Неконтролируемый мета-риск

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 27.002 Надежность в технике. Термины и определения

ГОСТ Р 27.010 Надежность в технике. Математические выражения для показателей безотказности, готовности, ремонтопригодности

ГОСТ Р 27.12 Анализ опасности и работоспособности (HAZOP)

ГОСТ Р 27.302 Надежность в технике. Анализ дерева неисправностей

ГОСТ Р 51897—2011 Менеджмент риска. Термины и определения

ГОСТ Р 51901.12 Менеджмент риска. Метод анализа видов и последствий отказов

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

ГОСТ Р 57149—2016 Аспекты безопасности. Руководящие указания по включению их в стандарты

ГОСТ Р ИСО 9000—2015 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

ГОСТ Р МЭК 61165—2019 Надежность в технике. Применение марковских методов

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

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

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

ГОСТ Р МЭК 61508-4—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

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

ГОСТ Р МЭК 61508-6—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3

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

ГОСТ Р МЭК 61511-1 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования

ГОСТ Р МЭК 61511-2 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1

ГОСТ Р МЭК 61511-3 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности

ГОСТ Р МЭК 62502 Менеджмент риска. Анализ дерева событий

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который

дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте приведены термины по ГОСТ 27.002, ГОСТ Р 27.010, [1], а также следующие термины с соответствующими определениями:

3.1.1 **риск** (risk): Следствие влияния неопределенности на достижение поставленных целей.

Примечание 1 — Риск часто представляют в виде сочетания последствий события (включая изменения обстоятельств) и соответствующей вероятности реализации события (см. ГОСТ Р 51897-2011, статья 1.1, примечание 4).

Примечание 2 — Риск, связанный с безопасностью, часто определяют как сочетание вероятности нанесения ущерба и тяжести этого ущерба (см. п. 3.9 в ГОСТ Р 57149—2016).

Примечание 3 — Остаточный риск представляет собой риск, оставшийся после обработки риска. Обработка риска включает в себя процесс изменения риска путем применения уровней защиты, установленных в настоящем стандарте (см. п. 3.8.1.6 в ГОСТ Р 51897—2011, пункты 7.2.1, 9.1 и B.6).

[ГОСТ Р 51897—2011, статья 1.1, изменение — примечания к исходному определению заменены новыми]

3.1.2 **состояние**

3.1.2.1 **состояние** (state): Математическое выражение, описывающее определенные условия, в которых рассматриваемый объект находится в течение установленного периода времени.

Примечание 1 — Ошибка является примером состояния, в то время как отказ является событием. Диаграмма состояний описывает состояния и переходы состояний системы (см. [1] и 3.1.4 и 3.1.5, 3.1.7).

3.1.2.2 **состояние** (state): Для идентификации, анализа и контроля риска свойства системы в течение определенного периода времени.

Примечание 1 — Состояния подразделяют на активные и неактивные в соответствии со степенью исправности объекта. Активному состоянию соответствует более высокая степень исправности объекта, а неактивному — более высокая степень неисправности. Мерой состояния системы является энтропия, которая также является мерой многообразия состояний системы (см. 3.1.2.2, примечание 4; 3.1.3, примечание 2 и B.2).

Примечание 2 — Если объекты взаимодействуют друг с другом, активное действие может быть выполнено в активном состоянии, неактивном состоянии, активное действие не может быть выполнено и вместо активного действия генерируется неактивное действие.

Примечание 3 — Активные действия подразделяют на типы, например: а) передача энергии; б) распространение информации; в) перенос агента; г) затруднение снабжения и д) остальные [2].

Примечание 4 — Функция представляет собой способность объекта производить активные и/или неактивные действия (см. 3.1.3, 3.1.13, 3.1.32, 3.1.33, 3.1.34, 7.2, 9.1, B.1, B.4, B.5 и B.6), [2].

3.1.3 **состояние запроса** (demand state): Состояние, в котором у системы запрашивают выполнение определенной функции.

Примечание 1 — В состоянии запроса объект должен функционировать для демонстрации своих установленных функций, т. е. выполнять активные и неактивные действия или те и другие при необходимости (см. 3.1.2.2, примечание 4).

Примечание 2 — Состояние отсутствия запроса — это состояние, в котором у системы не запрашивают функций, т. е. объект должен находиться в нерабочем состоянии относительно установленных функций (см. [1], статья 192-02-06).

Примечание 3 — Например, состояние, в котором водитель автомобиля активирует компьютерную систему управления тормозами для остановки автомобиля, является состоянием запроса этой функции системы, а состояние, в котором водитель не активирует эту систему управления, является состоянием отсутствия запроса этой функции системы управления. Состояние, в котором водитель не активирует систему управления тормозами, является состоянием запроса для дополнительной функции этой системы управления (предотвращение ошибочной активации функции управления тормозами для остановки автомобиля), а состояние, в котором водитель активирует систему управления, — это состояние отсутствия запроса дополнительной функции (см. 9.3.1, b) и B.2).

Примечание 4 — Запрос является началом состояния запроса, а завершением запроса является прекращение состояния запроса. Запрос и его завершение являются событиями (см. 3.1.4).

Примечание 5 — Непрерывный режим выполнения функции представляет собой режим функционирования, в котором состояние запроса функции продолжается. Режим запроса выполнения функции охватывает

состояния запроса и отсутствия запроса, т. е. при использовании системы запросы и завершения запросов появляются поочередно (см. 7.2, 9.3, А.1 и В.1, В.4, В.5, В.7).

Примечание 6 — Состояния запроса и функционирования не эквивалентны из-за возможности двух следующих режимов: объект функционирует в состоянии отсутствия запроса и объект не функционирует в состоянии запроса (см. 3.1.3, примечания 1 и 2 и 9.3).

3.1.4 **переход события** (event transition): Изменение одного состояния на другое.

Примечание 1 — Событие — это прекращение состояния или начало следующего состояния.

Примечание 2 — В контексте анализа риска риск часто представляют не только с помощью словесного описания, но также в виде состояний и их переходов с использованием дерева отказов (FT), диаграммы состояний и переходов (далее — диаграммы состояний) и т. п.

Примечание 3 — События подразделяют на промежуточные и конечные события с точки зрения диаграммы состояний для представления риска (см. 3.1.16 и 3.1.17).

[ГОСТ Р МЭК 61165—2019, статья 3.9, изменение — примечания из исходного определения были заменены новыми]

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

Примечание 1 — Структура системы может быть иерархической. Система состоит из нескольких подсистем.

Примечание 2 — Для удобства термин «состояние системы» использован для обозначения состояния, в котором находится система (см. 3.1.7).

[ГОСТ Р ИСО 9000—2015, статья 3.5.1, добавлены примечания]

3.1.6 **элемент** (element): Компонент или набор компонентов, который рассматривают как единое целое[1)].

3.1.7 **состояние системы** (system state): Конкретная комбинация состояний элементов, составляющих систему.

Примечание 1 — Состояния системы часто охватывают работоспособное и неработоспособное состояния, рабочее и нерабочее состояния, состояния запроса и отсутствия запроса и другие внешние условия, не зависящие от элементов системы (см. 3.1.5, примечание 2).

3.1.8 **начальное состояние** (initial state): Состояние системы, из которой система совершает первый переход в другое состояние на диаграмме состояний, представляющей риск.

Примечание 1 — Если риск идентифицирован, он может быть охарактеризован не только с помощью словесного описания, но и с использованием таких диаграмм, как дерево событий, FT и так далее для качественного или количественного вероятностного анализа риска (см., например, рисунки 3, 9 и 10).

Примечание 2 — Если состояние системы *X* является начальным состоянием, это состояние называется также начальным состоянием *X*.

3.1.9 **виртуальное начальное состояние** (virtual initial state): Состояние системы, в котором предполагается виртуальный переход из конечного состояния, используемое для вычисления MTFE в выявленном состоянии и FER в выявленном состоянии.

Примечание 1 — См. 3.1.11, 3.1.24, 3.1.25, 3.1.27 и 3.1.28.

Примечание 2 — См. для примера рисунок 17.

Примечание 3 — Если состояние системы *X* является виртуальным начальным состоянием, его называют виртуальным начальным состоянием *X*.

3.1.10 **конечное состояние** (final state): Состояние системы, в котором могут появиться конечные последствия риска.

Примечание 1 — Конечные последствия не всегда появляются в конечном состоянии, поскольку они могут зависеть от последовательности появления промежуточных состояний (см. 3.1.12, 7.2, 9.2 и 9.3).

Примечание 2 — Система переходит в конечное состояние при возникновении конечного события (см. 3.1.17).

3.1.11 **промежуточное состояние** (intermediate state): Состояние системы на диаграмме состояний, представляющей риск, которое не является начальным или конечным состоянием.

3.1.12 **предшествующее состояние** (antecedent state): Начальное состояние или, если оно существует, любое промежуточное состояние на диаграмме состояний, представляющей риск.

Примечание 1 — См. 3.1.8 и 3.1.11.

[1)] См. также ГОСТ 27.002.

Примечание 2 — Предшествующее состояние может быть определено при использовании набора состояний, таких как работоспособное и неработоспособное, рабочее и нерабочее, состояния запроса и отсутствия запроса, состояния отключения и других внешних условий (см. например, рисунок 3).

3.1.13 **выявленное состояние** (recognised state): Предшествующее состояние, которое обнаружено и/или выявлено в установленное время.

Примечание 1 — Предшествующие состояния часто (но не всегда) выявляют путем использования таких средств, как функции самодиагностики продукции, периодические проверки компонентов, выявление человеком некоторых обстоятельств, особенностей функционирования и так далее в установленное время.

Примечание 2 — Если предшествующее состояние системы является выявленным состоянием, то может быть обнаружено, что состоянием системы является или не является ее предшествующее состояние в установленное время и наоборот.

Примечание 3 — В настоящем стандарте предполагается, что конечное состояние является выявленным в любое время (см. 9.3 и 9.4).

Примечание 4 — Поскольку не все предшествующие состояния охвачены мониторингом и распознаванием, предшествующие состояния не всегда являются выявленными и поэтому их подразделяют на выявленные и не выявленные состояния (см. 3.1.16, примечание 1).

3.1.14 **группа состояний** (group state): Набор из двух или более предшествующих состояний, которые не могут быть распознаны как отдельные предшествующие состояния.

Примечание 1 — См. 3.1.13, примечание 4.

3.1.15 **выявленная группа состояний** (recognised group state): Группа состояний, выявленная в установленное время.

Примечание — Предположим, например, что предшествующими состояниями являются состояния системы A, B и C, а выявленным состоянием является только состояние системы C, тогда группа состояний A и B является выявленной группой состояний, поскольку можно признать, что система находится в состояниях этой группы, если в установленное время она не находится ни в состоянии C, ни в конечном состоянии и наоборот (см. 3.1.13, примечания 3 и 4).

3.1.16 **промежуточное событие** (intermediate event): Переход в состояние, которое не является конечным событием или событием восстановления.

Примечание 1 — См. 3.1.5, 3.1.18 и 3.1.21.

Примечание 2 — Переход из одного предшествующего состояния в другое промежуточное состояние является промежуточным событием, но не наоборот (см. 3.1.19).

3.1.17 **конечное событие** (final event): Начало конечного состояния, т. е. состояние перехода из любого предшествующего состояния (или критического состояния) в конечное состояние.

Примечание 1 — См. 3.1.10 и 3.1.12.

Примечание 2 — Конечное событие также называют критическим событием, но не наоборот (см. ГОСТ Р 27.010).

Примечание 3 — Данный термин может относиться к опасным событиям или событиям, приносящим вред в области функциональной безопасности (ГОСТ Р МЭК 61508, все части).

3.1.18 **повторяемое конечное событие** (repeatable final event): Конечное событие, которое может повторяться.

Примечание 1 — Например, см. рисунок 3.

Примечание 2 — Для повторяемого конечного события характерно, что это событие не влияет на способ появления и исчезновения промежуточных состояний, потому что, если конечное событие изменяет способ появления и исчезновения промежуточных состояний, исходное состояние системы и соответствующий ему риск не сохраняются после завершения конечного события.

Примечание 3 — Конечное состояние, возникающее в результате повторяемого конечного события, может привести к переходу системы в промежуточное состояние, и конечное событие может повториться (см. 3.1.17, примечание 2).

3.1.19 **неповторяемое конечное событие** (unrepeatable final event): Конечное событие, которое не является повторяемым.

Примечание 1 — Например, см. рисунок 3.

Примечание 2 — Если конечное событие постоянно изменяет способ появления и исчезновения промежуточных состояний, то конечное событие не может быть повторяемым, поскольку исходное состояние системы и риск, соответствующий исходному состоянию системы, не сохраняются (см. 3.1.19, примечание 2).

Примечание 3 — Если конечное состояние переходит в исходное состояние и система является восстановленной, конечное событие является неповторяемым конечным событием, поскольку восстановленное состояние системы отличается от исходного состояния системы (восстановленное состояние системы не совпадает с исходным состоянием системы).

3.1.20 **восстановление** (renewal event): Прекращение конечного состояния, которое происходит в результате неповторяемого конечного события, вызывающее переход в начальное состояние или виртуальное начальное состояние системы.

Примечание 1 — Конечное состояние, обусловленное повторяемым конечным событием, может вызвать переход в промежуточное состояние (см. 3.1.19, примечание 3).

3.1.21 **частота события** (event frequency): Предел, если он существует, отношения среднего числа событий в течение интервала времени [t, t Δt] к Δt, при Δt, стремящемся к нулю, при условии, что система находится в данном начальном состоянии в момент времени $t = 0$.

Примечание 1 — Для частоты событий $\omega(t)$ справедлива формула

$$\omega(t) = \lim_{\Delta t \to 0} E\left[N(t+\Delta t) - N(t)\right] / \Delta t,$$

где $N(t)$ — количество событий в интервале времени [0, t], E — знак математического ожидания.

Примечание 2 — Единицей измерения частоты событий является единица времени в степени минус 1.

3.1.22 **средняя частота событий** (average event frequency): Частота событий, усредненная по периоду времени H.

Примечание 1 — Средняя частота событий $\omega(0, H)$ имеет вид

$$\omega(0,H) = (1/H)\int_0^H \omega(t)\,\mathrm{d}t \int_0^T ,$$

где $\omega(t)$ — частота события в момент времени t;

$\int_0^H \omega(t)\mathrm{d}t$ — вероятность того, что неповторяемое событие происходит в интервале времени [0, H] или математическое ожидание количества повторяемых событий в интервале времени [0, H].

3.1.23 **интенсивность перехода состояний, условный параметр потока событий** (state transition rate, conditional event intensity): Предел, если он существует, отношения условной вероятности того, что событие, т. е. переход системы из состояния X в состояние Y, происходит в течение интервала времени [t, $t + \Delta t$] к Δt, когда Δt стремится к нулю, при условии, что в момент времени t система находится в состоянии X.

Примечание 1 — Если появление события подчиняется экспоненциальному распределению, т. е. появление события является случайным и не зависит от времени, то условный параметр потока событий является постоянным, его называют постоянной интенсивностью события или постоянной интенсивностью перехода (см. разделы 1, 5, 7, 9, А.1 и В.1).

Примечание 2 — Единицей измерения параметра потока событий и интенсивности перехода состояний является единица времени в степени минус 1.

3.1.24 **среднее время до конечного события (MTEF) для заданного начального состояния** (MTFE at a given initial state mean time to final event at a given initial state): Среднее время от начального состояния или виртуального начального состояния до первого конечного события.

Примечание 1 — Заданное начальное состояние означает любое предшествующее состояние (см. 3.1.8, 3.1.9, 3.1.12 и 3.1.20).

Примечание 2 — MTFE для заданного начального состояния аналогично среднему времени работоспособного состояния (MUT), а не средней наработке до отказа (MTTF), однако предшествующие состояния включают не только работоспособное и неработоспособное, рабочее и нерабочее состояния, а также состояния запроса, отсутствия запроса и отключение и другие внешние условия окружающей среды (см. [1]).

3.1.25 **интенсивность конечного события (FER) для заданного начального состояния** (final event rate (FER) at a given initial state): Предел, если он существует, отношения условной вероятности того, что конечное событие произойдет в течение интервала времени [t, $t + \Delta t$] к Δt , когда Δt стремится к нулю, при условии, что система, у которой интенсивность перехода является постоянной, а конечное состояние вызывает переход только в начальное состояние или виртуальное начальное состояние, находится в стационарном состоянии и не находится в конечном состоянии.

Примечание 1 — Для восстанавливаемой системы с постоянными интенсивностями перехода FER для заданного начального состояния становится постоянной и равна величине, обратной MTFE для заданного начального состояния (см. [3]—[6]).

Примечание 2 — В области функциональной безопасности FER для заданного начального состояния представляет собой интенсивность причиняющих вред или опасных событий (HER) (см. 3.1.17, примечание; 3, 7.2, 9.3.2, В.1 и В.4).

Примечание 3 — Стационарное состояние — это состояние системы через бесконечное время, при этом вероятности всех состояний системы на диаграмме состояний, представляющей риск, сходятся к постоянным значениям, если время стремится к бесконечности.

3.1.26 **частота конечного события (FEF) для заданного начального состояния** (final event frequency (FEF) at a given initial state): Частота конечного события при условии, что система, у которой интенсивность перехода является постоянной, а конечное состояние вызывает переход только в начальное состояние или виртуальное начальное состояние, находится в стационарном состоянии.

Примечание 1 — См. 3.1.17, 3.1.21 и 3.1.25, примечание 3.

Примечание 2 — Для восстанавливаемой системы с постоянными интенсивностями перехода FEF для данного начального состояния становится постоянной и равна величине, обратной среднему времени от начального состояния до появления первого восстановления (см. [3]—[6]).

Примечание 3 — Для FER для заданного начального состояния φ справедлива формула (см. [3]—[6])

$$\varphi = \omega/(1 - P\{X\}),$$

где ω — FEF для заданного начального состояния;

$P\{X\}$ — вероятность того, что система находится в конечном состоянии, и это состояние является стационарным состоянием.

3.1.27 **среднее время до конечного события (MTFE) для выявленного состояния** (mean time to final event (MTFE) at a recognised state): MTFE для заданного начального состояния, когда заданным начальным состоянием является выявленное состояние.

Примечание — См. 3.1.25.

3.1.28 **интенсивность конечного события (FER) для выявленного состояния** (final event rate FER at a recognised state): FER для заданного начального состояния, когда заданным начальным состоянием является выявленное состояние.

Примечание 1 — См. 3.1.25.

Примечание 2 — Соотношение между FER для выявленного состояния и FEF для выявленного состояния такое же, как соотношение между FER для заданного начального состояния и FEF для заданного начального состояния (см. 3.1.26, примечание 3, 8.2 и 9.3.3).

3.1.29 **интенсивность конечного события (FER) для выявленной группы состояний** (final event rate (FER) at a recognised group state): Взвешенное среднее всех FER для заданного начального состояния по группе состояний.

Примечание — См.: 8,2, 9.3.4 и 9.4.5.

3.1.30 **экспозиция риска *T*** (risk exposure time *T*): Математическое ожидание продолжительности времени, в течение которого система подвергается конкретной опасности в процессе ее срока службы.

Примечание 1 — См. 5.2, 7.2.2, 7.2.3, А.3 и А.4.

Примечание 2 — Экспозиция риска *T* часто связана с такими понятиями, как срок службы (см. [1]), ресурс и время выполнения задания. Однако эти понятия не обязательно эквивалентны применительно к экспозиции риска, поскольку риск может быть заменен на несколько трансформированных рисков в течение срока службы, эксплуатации, или времени выполнения задания системы, и только конкретный риск из этих рисков может представлять интерес по отношению к экспозиции риска. В таком случае экспозиция риска не эквивалентна времени, установленному этими терминами.

3.1.31 **приближенная вероятность опасного отказа во время состояния запроса (APF_{drg}), P_b** (approximate probability of dangerous failure during a demand state APFdrg, P_b): Приближенная вероятность того, что опасный отказ объекта произойдет в течение времени средней продолжительности состояния запроса $[0, \tau]$, где τ — математическое ожидание времени состояния запроса, при условии, что запрос произошел в нулевой момент времени.

Примечание 1 — Необходимым условием аппроксимации является то, что вероятность возникновения двух или более опасных отказов в интервале времени $[0, \tau]$ является пренебрежимо малой (см. 7.2.3, 9.3.1 б), 9.3.2 и приложение В).

Примечание 2 — Данный термин применяют только для анализа риска в области безопасности (см. приложение Б).

3.1.32 **средняя вероятность опасного отказа при запросе** PFDavg, $\mathbf{P_a}$ (average probability of dangerous failure on demand PFDavg, P_a): Средний коэффициент неготовности объекта по отношению к выполнению заданной функции безопасности при запросе.

Примечание 1 — Данный термин используют только применительно к функциональной безопасности (см. ГОСТ Р МЭК 61508-4—2012, пункт 3.6.18).

Примечание 2 — Для данного термина предполагается, что состояние объекта изменяется с состояния простоя на состояние функционирования при запросе, и объект может отказать в состоянии простоя (см. 7.2.3, 9.3.1, b), 9.3.2, приложение В).

3.1.33 **средняя частота опасного отказа в час** PFH, λ (average frequency of dangerous failure PFH per hour, λ): Среднее арифметическое частоты опасного отказа объекта при выполнении заданной функции безопасности за установленный период времени.

Примечание 1 — Независимый канал по отношению к выполняемой функции представляет собой последовательную систему, т. е. отказ одного из компонентов канала приводит к отказу канала в целом.

Примечание 2 — PFH является приближением величины, обратной средней наработке до первого отказа в случае, когда опасный отказ является неповторяемым конечным событием несмотря на то, что он является приближением величины, обратной средней наработке между отказами в случае, когда опасный отказ является повторяемым событием. Обычно предполагается, что объект может отказать в состоянии простоя (см. ГОСТ Р МЭК 61508-4—2012, пункт 3.6.19, примечание 4, а также ГОСТ Р МЭК 61508-6—2012, В.2.3.2 и В. 2.3.3 и 3.1.32, примечание 2, 7.2.3, 9.3.1 b), 9.3.2 и приложение В в настоящем стандарте).

3.1.34 **канал, Ch** (channel, Ch): Компонент или группа компонентов, независимо выполняющих функцию объекта.

Примечание 1 — Данный термин применяют только по отношению к функциональной безопасности (см. ГОСТ Р МЭК 61508-4—2012, пункт 3.6.19) (см. 3.1.5, примечание 2).

3.1.35 **базовый элемент MCS (basic element, MCS element)**: Элемент, который входит в состав MCS, полученного посредством анализа FTA или RBD, или обоих методов.

Примечание — Элемент MCS всегда является основным событием FT, но не наоборот. Таким образом, для удобства далее для элемента MCS использован термин «базовый элемент».

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

APF_{drg} — приближенная вероятность опасного отказа во время запроса;
CCF — отказы по общей причине;
Ch — канал;
D — обнаруженный;
DU — обнаруженный только при запросе;
E/E/PE — электрические/электронные/программируемые электронные;
ETA — анализ дерева событий;
FEF — частота конечного события;
FER — интенсивность конечного события;
FMEA — анализ видов и последствий отказов;
FPL — конечный уровень защиты;
FT — дерево неисправностей;
FTA — анализ дерева неисправностей;
HAZOP — исследование опасности и работоспособности;
HER — интенсивность наносящих вред (опасных) событий;
Int. — промежуточный;
MCS — набор минимальных сечений;
MTFE — среднее время до конечного события;
MTRE — среднее время восстановления события;
MTTF — средняя наработка до отказа;
MUT — средняя продолжительность работоспособного состояния;
PAND — вентиль «И»;

PFD_{avg} — средняя вероятность опасного отказа по запросу;
PFH — средняя частота опасного отказа в час;
PL — уровень защиты;
RBD — структурная схема надежности;
SIL — уровень полноты безопасности;
TTFE — время до конечного события;
TTRE — время для события восстановления;
UD — необнаруженный.

4 Различия терминов частоты и интенсивности конечного события

Термин «частота» может быть использован как по отношению к количеству возникновений событий данного вида, так и по отношению к количеству событий за заданный период времени. В настоящем стандарте использован последний вариант, что соответствует определению в 3.1.21.

Термин «интенсивность» обычно означает скорость, с которой что-то движется или происходит, а в области надежности интенсивность событий, таких как отказы, определяют как предел, если он существует, отношения условной вероятности того, что событие происходит в течение интервала времени $[t, t + \Delta t]$ к Δt, когда Δt стремится к нулю при условии, что событие не произошло до момента времени t.

Определения интенсивности события и частоты события кажутся довольно различными. Однако в области оценки риска частоту события и интенсивность события часто путают. На рисунке 1 показаны изменения состояний системы в целом, в которой появления конечного события и события восстановления подчиняются экспоненциальному распределению, т. е. интенсивность конечного события (FER) и интенсивность восстановления событий являются постоянными (см. 3.1.17, 3.1.20 и 3.1.23). На рисунке 1 приведены два состояния системы, конечное и предшествующее (см. 3.1.10 и 3.1.12).

На рисунке 2 показан процесс появления конечных событий и событий восстановления, в которых TTFE и TTRE эквивалентны по величине продолжительности предшествующего состояния и продолжительности конечного состояния соответственно. Здесь предполагается, что стохастический процесс появления конечных событий и событий восстановления может быть смоделирован с помощью диаграммы Маркова, а MTFE и MTRE равны $T_a (\neq 0)$, ч и $T_b (\neq 0)$, ч, соответственно. Тогда в стационарном состоянии процесса, FEF ω [1/ч] имеет вид

$$\omega = 1/(T_{at}T_b), \quad (1)$$

где T_a — MTFE, ч; T_b — MTRE, ч.

Интенсивность конечного события (FER) φ [1/ч] и интенсивность восстановления событий m [1/ч] имеют вид:

$$\varphi = 1/T_a \text{ (т. е. } T_a = 1/\varphi); \quad (2)$$

$$m = 1/T_b \text{ (т. е. } T_b = 1/m). \quad (3)$$

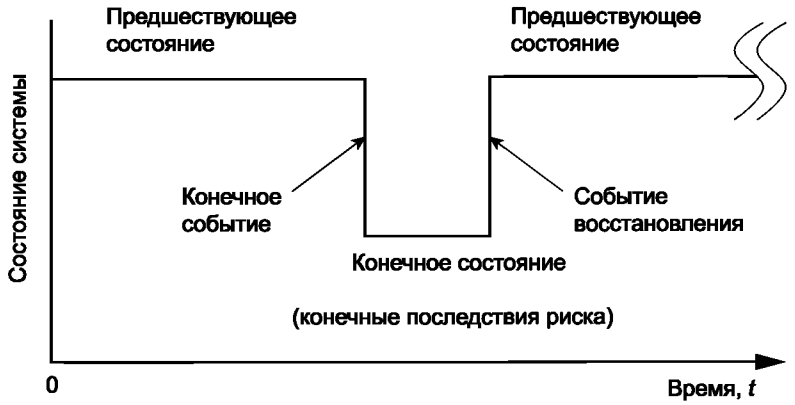


Рисунок 1 — Предшествующее состояние, конечное событие, конечное состояние и событие восстановления

Частоту конечного события (FEF) можно записать с использованием φ и m, см. (1), (2) и (3)

$$\omega = \varphi m/(\varphi + m) = \varphi/\{(T_b/T_a) + 1\}. \quad (4)$$

Если T_a много больше T_b, а именно, если φ намного меньше m, то ω почти равна φ.

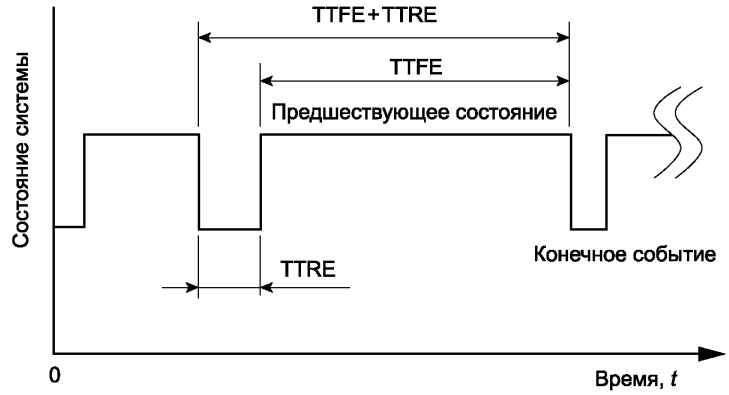


Рисунок 2 — Время до конечного состояния (TTFE), время до состояния восстановления ((TTRE)

Однако FEF не обязательно равна FER и возможны следующие ситуации:

a) например, в области оценки риска атомных электростанций допустимый риск серьезных аварий, таких как расплавление реактора, определяют путем использования частоты событий в год. Здесь конечным событием является расплавление реактора;

b) если допустимая частота конечного события равна 10^{-4} [1/год], то обычно можно предположить два случая. В первом случае $1/\varphi$ = 50 лет, $1/m$ = 9950 лет, и поэтому $1/\omega$ = 10000 лет. Во втором случае $1/\varphi$ = 9950 лет, $1/m$ = 50 лет, и $1/\omega$ = 10000 лет;

c) несмотря на то, что частоты событий в этих случаях равны, вероятности того, что событие произойдет в течение срока службы объекта или времени воздействия (эксплуатации) риска (50 лет), различны. А именно, эти вероятности могут составлять 60 % или более в первом случае и 0,5 % или ниже во втором случае. Это означает, что уровень риска в первом случае намного выше, чем во втором случае.

Таким образом, желательно использовать не частоту события, а интенсивность события в качестве целевого показателя появления редкого конечного события.

5 Частота конечного события и интенсивность конечного события для заданного начального состояния

5.1 Общие положения

В данном разделе приведены разъяснения FEF и FER для заданного начального состояния и определены способы их адаптации к целевым показателям появления конечного события.

5.2 Классификация конечных событий

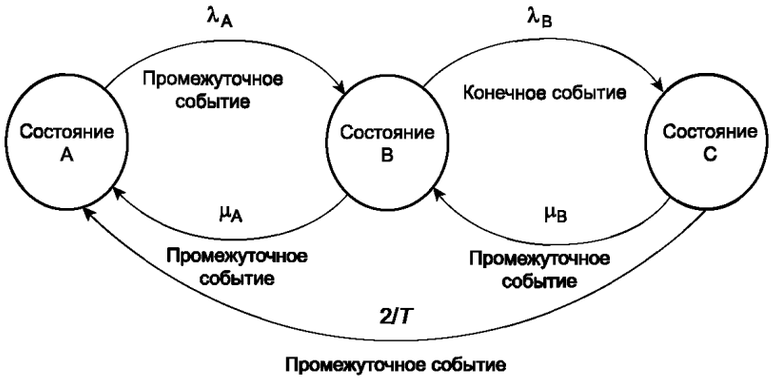
На рисунке 3, a), 3, б), 3, в) приведены диаграммы состояний, представляющие риск, когда состояния системы A, B и C являются начальным, промежуточным и конечным соответственно (см. 3.1.4, примечание 2).

Если на рисунке 3 риски связаны с некоторой деятельностью человека, то, например, состояние B может соответствовать состоянию системы, при котором человек работает, а состояние A — состоянию системы, при котором человек не работает, а отдыхает, а состояние C — состоянию системы, при котором с человеком происходят неблагоприятные события от легких происшествий до катастроф.

Если происходит конечное событие, существуют две возможные последующие ситуации:

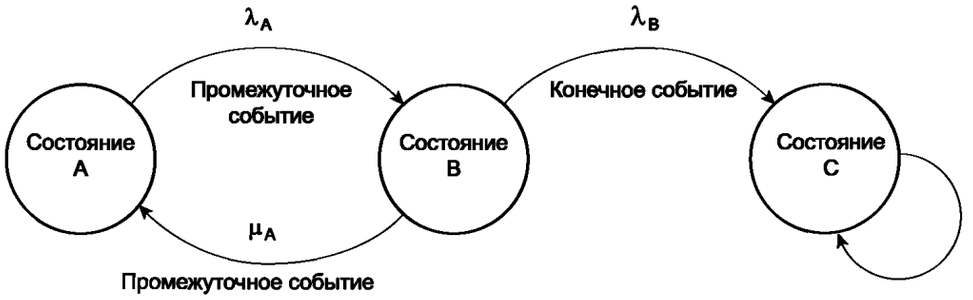
a) конечное событие не зависит от способа возникновения промежуточного события, конечное состояние может вызвать переход в промежуточное состояние и конечное событие может повториться (см. рисунок 3, a). Данное конечное событие далее рассматривают как повторяемое конечное событие (см. 3.1.19);

b) конечное событие не повторяется, потому что постоянно изменяется способ появления конечного события и исчезновения промежуточных состояний и поэтому риск идентичен риску, когда начальное состояние системы больше не поддерживается (см. рисунок 3, b) и 3, c)). Данное конечное событие далее рассматривают как неповторяемое конечное событие (см. 3.1.19).



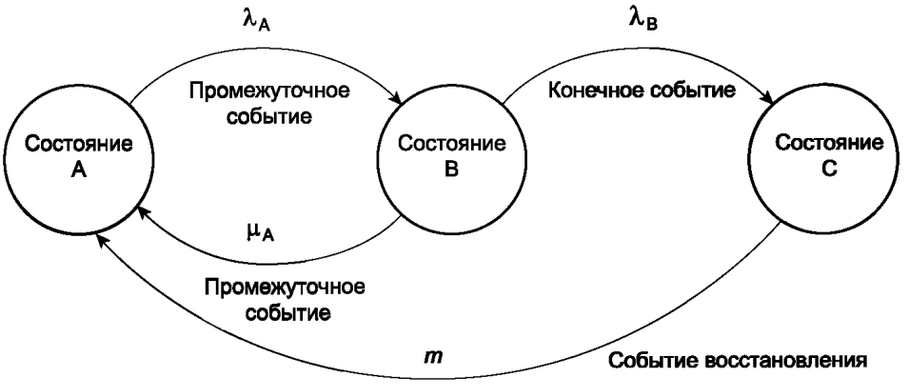
T — экспозиции риска; λ_A, μ_A, λ_B, μ_B и $2/T$ — интенсивности переходов ($1/T << \lambda_A$; $1/T << \mu_A$ и $\lambda_B << 1/T$)

a) модель повторяемого конечного события



λ_A, μ_A, λ_B — интенсивности переходов

b) модель неповторяемого конечного события



λ_A, μ_A, λ_B, m — интенсивности переходов

c) модель конечного события с восстановлением

Состояние системы A: начальное состояние (предшествующее состояние);
состояние системы B: промежуточное состояние (предшествующее состояние);
состояние системы C: конечное состояние

Рисунок 3 — Модели перехода с различными конечными состояниями

На рисунке 3, а) показана модель перехода состояний системы, в которой происходит переход из конечного состояния С в промежуточное состояние В и конечное событие может повторяться. В этой модели постоянные интенсивности событий λ_A, μ_A, λ_B, μ_B и $2/T$ являются интенсивностями событий перехода, причем $1/T << \lambda_A$, $1/T << \mu_A$ и $\lambda_B << 1/T$ (см. 3.1.24), где T — среднее время пребывания системы под воздействием риска (см. 3.1.31).

Предположим, что некоторой деятельности человека соответствует риск.

1) $1/\lambda_A$ — среднее время, когда работник не работает, а отдыхает, а $1/\mu_A$ — среднее время, когда он работает;

2) $1/\lambda_B$ — среднее время возникновения ошибки при условии, что человек находится на работе и $1/\mu_B$ — среднее время, когда человек не работает, а исправляет свои ошибки;

3) T — период занятости работника (однако переходами в течение периода занятости, т. е. периода экспозиции риска, можно пренебречь, если справедливы неравенства $1/T << \lambda_A$, $1/T << \mu_A$ и $1/T << \mu_B$).

На рисунке 3, b) конечное состояние является невосстанавливаемым, т. е. конечное событие не повторяется. На рисунке 3, b) постоянные интенсивности событий λ_A, μ_A и λ_B являются такими же, как на рисунке 3, a), за исключением интенсивности событий μ_B (= 0). В этом случае конечное состояние означает, например, что человеческий фактор исключен (не рассматривается).

На рисунке 3, c) происходит переход из конечного состояния C в начальное состояние A и постоянная интенсивность появления события m является постоянной интенсивностью восстановления события (см. 3.1.20 и 3.1.23). Здесь конечное состояние также означает, например, что человеческий фактор исключен.

5.3 Частота конечного события в стационарном состоянии

На рисунке 3, a) FEF в стационарном состоянии ω_R описывают формулой (5) при условии, что система находится в стационарном состоянии [3]

$$\omega_R = \lambda_B \, Pr\{B\}, \tag{5}$$

где $Pr\{B\}$ — вероятность того, что система находится в состоянии B, в стационарном состоянии (см. рисунок 3, a)).

На рисунке 3, c) (схематично) FEF в начальном состоянии A, ω_{UA} приведена в предположении, что восстановленная система идентична исходной системе (однако следует учитывать, что восстановленная система обычно не идентична исходной системе). Затем FEF в начальном состоянии A имеет вид (6) при условии, что система находится в стационарном состоянии [3]

$$\omega_{UA} = \lambda_B Pr\{B\}, \tag{6}$$

где $Pr\{B\}$ — вероятность того, что система находится в состоянии B, в стационарном состоянии (см. рисунок 3, c)).

5.4 Интенсивность конечного состояния для заданного начального состояния и выявленного состояния

На рисунке 3, в) FEF в начальном состоянии A, φ_A, описывает формула (7) в предположении, что система находится в стационарном состоянии, а $Pr\{C\}$ — вероятность того, что система находится в состоянии C [3], [5], [6]

$$\varphi_A = \omega_{UA} /(1\text{-}Pr\{C\}). \tag{7}$$

MTFE в начальном состоянии A, T_A, имеет вид (см. 3.1.25) [3], [5], [6]:

$$T_A = 1/\varphi_A. \tag{8}$$

На рисунке 3, c) FER в выявленном состоянии B, φ_B, описывает формула (9) в предположении перехода виртуального события (например, виртуального восстановления) из конечного состояния C в промежуточное состояние B (выявленное состояние B), подставляя FEF в выявленном состоянии B, в ω_{UB} (см. 3.1.27), получаем

$$\varphi_B = \omega_{UB}/(1 - Pr\{C\}). \tag{9}$$

Таким образом MTFE в выявленном состоянии B, T_B имеет вид (см. 3.1.28)

$$T_B = 1/\varphi_B. \tag{10}$$

5.5 Соотношение между интенсивностью и частотой конечного события для заданного начального состояния

Если время пребывания в состоянии C на рисунке 3, c) является бесконечным, т. е. $m \to 0$ (или m асимптотически приближается к 0), восстанавливаемая система становится эквивалентна невосстанавливаемой системе на рисунке 3, b). FER для заданного начального состояния и FER в выявленном состоянии не включают интенсивность восстановления m и поэтому не зависят от m. Это означает, что MTFE в данном начальном состоянии и MTFE в выявленном состоянии на рисунке 3, b) эквивалентны такому состоянию на рисунке 3, c) [3], [5], [6].

Таким образом, в отношении FER для заданного начального состояния и FER в выявленном состоянии система с невосстанавливаемым конечным состоянием эквивалентна восстанавливаемой системе при условии, что переходы системы в точности совпадают между такими же переходами системы, за исключением восстанавливаемых отказов.

Для любой восстанавливаемой системы с интенсивностью восстановления m предположим, что φ — FER для заданного исходного состояния (или выявленного состояния) и ω — FEF для заданного начального состояния (или выявленного состояния) при стационарном состоянии системы. В этом случае справедливо следующее общее соотношение [3], [5], [6]:

$$\varphi = \lim_{m\to\infty} \omega = \omega / \left(1 - P\{X\}\right), \tag{11}$$

где $P\{X\}$ — вероятность того, что система находится в конечном состоянии X в стационарном состоянии.

6 Процедура вероятностного анализа риска и составление профиля риска

Контрольные перечни анализа «что, если», исследование HAZOP (ГОСТ Р 27.12), FMEA (ГОСТ Р 51901.12) и так далее, как правило, применяют для идентификации рисков, которые используют в начале исследования системы (ГОСТ Р ИСО/МЭК 31010). Исследуемая система может включать в себя технические объекты, каждый из которых часто состоит из тысячи или более компонентов, которые пребывают в работоспособном и неработоспособном состояниях. Риск сложных систем с такими состояниями анализируют количественно и качественно с использованием таких методов как FMEA, RBD (ГОСТ Р 51901.14), FTA и ETA; основные способы исследования причин конечного состояния приведены в (9.1, 9.5 и В.2). Эти методы часто используют MCS, определенные при выполнении FTA.

Набор MCS для конечного события системы обычно состоит из нескольких MCS элементов, т. е. нескольких основных элементов (см. 3.1.35). Обычно влияние набора MCS, составленного для большего количества основных элементов, часто является незначительным по сравнению с набором MCS, составленным для меньшего числа базовых элементов, с количественной точки зрения. К примеру, отказы по общей причине часто (но не всегда) доминируют среди причин конечных событий с этой точки зрения (см. приложение А). Количественный анализ риска выполняют в строгом соответствии с набором MCS для меньшего количества базовых элементов с использованием, например, диаграмм состояний, в то время как состояние каждого базового элемента, такого как канал (Ch), может охватывать работоспособное и неработоспособное состояния сотен или более компонентов (см. 3.1.34 и 3.1.35). Таким образом, оценка FER для заданного начального состояния сложных систем может быть определена на основе скрининга таких MCS.

Процедура анализа риска сложных технических систем, включающая определение оценки FER для заданного начального состояния (см. таблицу 1; 9.1, 9.5, А.5 и В.3), включает в себя следующие этапы:

- идентификацию риска и качественный анализ риска для поиска, например, наборов MCS, состоящих из меньшего количества базовых элементов, доминирующих среди причин конечного события, путем использования таких методов, как контрольные перечни, анализ «что, если», исследование HAZOP, FMEA, RBD, ETA и FTA (детали не рассмотрены в настоящем стандарте);
- создание аналитических моделей для определения количественной оценки с должным вниманием к основным элементам в качестве доминирующих причин возникновения конечного события с количественной точки зрения путем использования таких методов, как ETA, FTA и марковских методов;
- определение FEF, FER, FEF для заданного начального состояния, FER для заданного начального состояния, FER в выявленном состоянии и FER в выявленной группе состояний для всех состояний системы, а также модели перехода, т. е. аналитической модели, состоящей из набора базовых элементов;
- валидацию моделирования и анализа с точки зрения типов, показателей, полноты и последовательности причинной связи событий, аппроксимации, источников данных о частоте/интенсивности событий и так далее (детали не рассмотрены в настоящем стандарте);
- повторение анализа, если он не является удовлетворительным;
- документирование данных и результатов анализа (детали не рассмотрены в настоящем стандарте);
- передачу результатов анализа для дальнейшей оценки риска.

Процедура анализа возникновения конечного события приведена на рисунке 4.

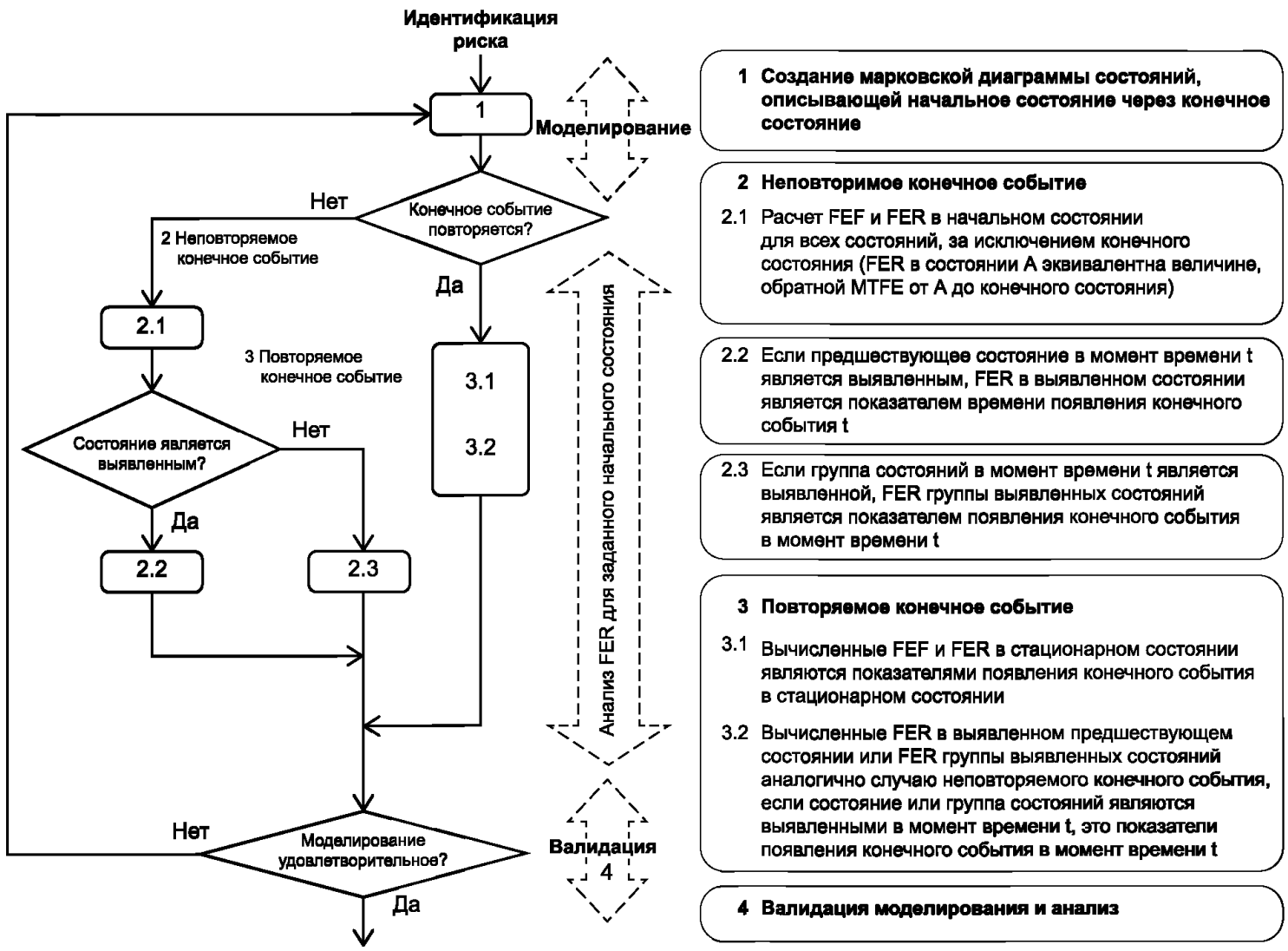


Рисунок 4 — Процедура анализа повторяемого/неповторяемого конечного события

7 Методы количественного анализа появления конечного события

7.1 Графическое обозначение трех типов конечных событий

7.1.1 Общие положения

При анализе риска сложных систем важно дополнительно использовать такие аналитические методы как HAZOP, FMEA, RBD, FTA и марковский метод. При проведении количественного анализа для выявления причин конечного события обычно используют методы ETA, FTA и марковский метод. Однако обычные методы ETA и FTA не используют символы для обозначения таких типов конечных событий, как повторяемые, восстанавливаемые, неповторяемые, которые необходимы для получения максимальной результативности этих методов. Поэтому в настоящем стандарте введены символы для использования в методах ETA, FTA и марковском методе, приведенные в таблицах 2—5, где показан способ использования этих символов и эффективность модифицированных методов анализа риска (см. 7.2).

Основные символы для ETA и FTA приведены в таблице 2 и позволяют разделить конечные события на тип 1 (повторяемые), тип 2 (неповторяемые и восстановленные) и тип 3 (неповторяемые и невосстанавливаемые).

7.1.2 Повторяемые конечные события

В таблице 3 приведены обозначения и графические представления для оценки FEF повторяемых промежуточных и конечных событий при дополнительном использовании методов ETA, FTA и марковского метода. Риск представлен начальным состоянием 1, промежуточными состояниями 2 и 3 и конечным состоянием 4, а также событиями 1 → 2, 2 → 1, 2 → 4, 4 → 2, 1 → 3, 3 → 1, 3 → 4 и 4 → 3, как по-

казано в дереве событий FT и марковской диаграмме состояний. Обозначение «$m \rightarrow n$ (m, n = 1, 2, ...)» означает переход системы из состояния m в состояние n.

Конкретные выражения для состояний и событий системы показаны в 7.2. Здесь конечными событиями являются события 2 → 4 и 3 → 4. Эти конечные события не изменяют свойства риска и поэтому не изменяют путь от начального состояния в конечное состояние.

Ветвь дерева событий, которая имеет стрелки на обоих концах, означает, что это событие может повторяться. Эта ветвь является повторяемой ветвью типа 1. Вентиль «И» с треугольником для FT означает, что выход вентиля является повторяемым событием. Вентиль «И» является вентилем типа 1.

Таблица 2 — Графические символы для анализа дерева событий и дерева неисправностей

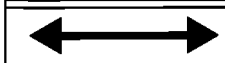
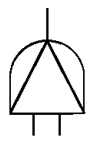
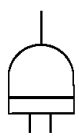
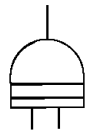
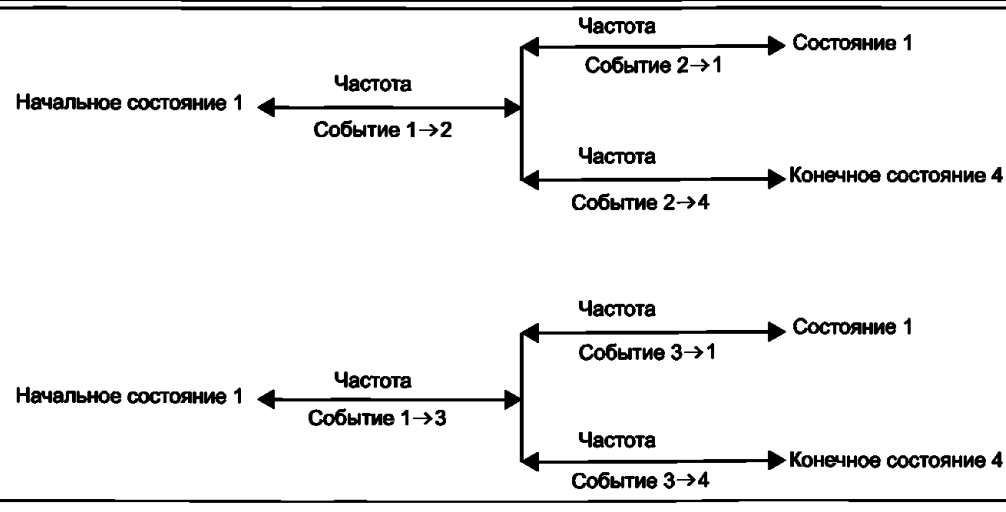
Символ	Наименование	Описание
	Повторяемая ветвь типа 1	Событие на этой ветви дерева событий (ET) является повторяемым
	Неповторяемая ветвь типа 2	Событие на этой ветви ET является неповторяемым и приводит к восстановлению конечного состояния, если это событие является конечным
	Неповторяемая ветвь типа 3	Конечное событие этой ветви ET является неповторяемым и приводит к невосстанавливаемому конечному состоянию
	Вентиль «И» типа 1	Выходное событие вентиля является повторяемым (комбинация вентиля блокировки и вентиля «И» может быть применена для невосстанавливаемого промежуточного события)
	Вентиль «И» типа 2	Выходное событие вентиля является повторяемым и приводит к восстанавливаемому конечному состоянию
	Вентиль «И» типа 3	Выходное событие является повторяемым и приводит к невосстанавливаемому конечному состоянию

Таблица 3 — Графические символы и представления для повторяемого (конечного) события

Метод	Схема
ETA	

Окончание таблицы 3

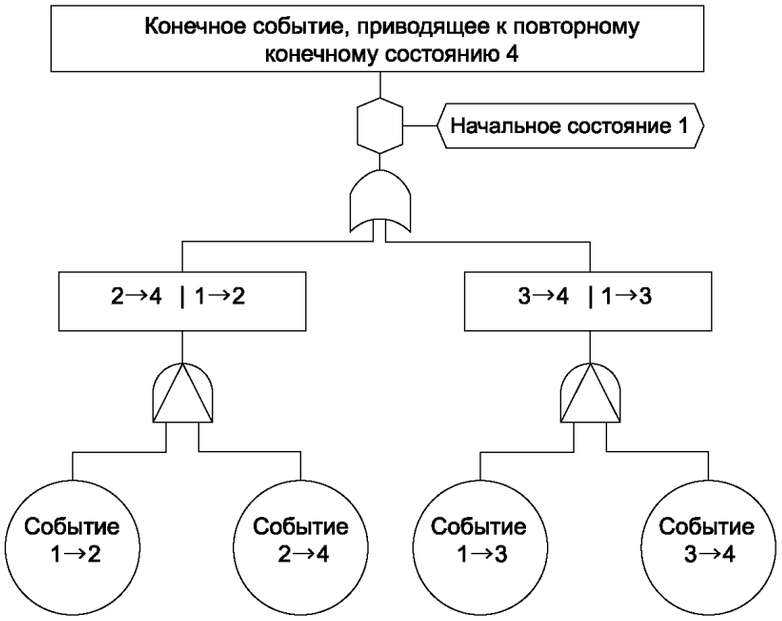
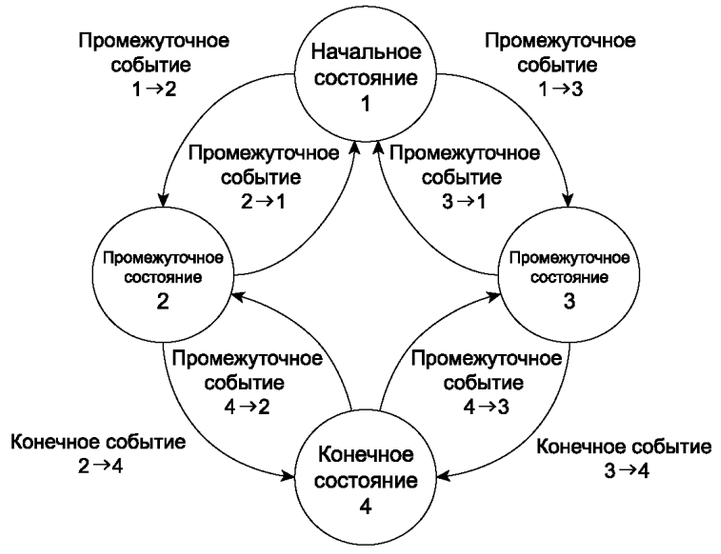
Метод	Схема
FTA	
Марковская диаграмма состояний	

Таблица 4 — Графические символы и представления для восстанавливаемого конечного состояния

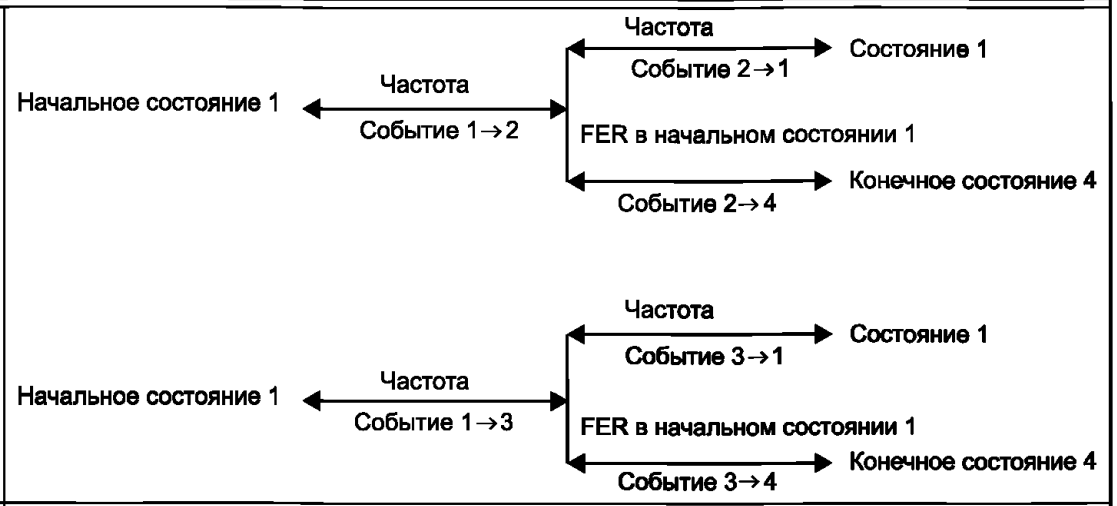
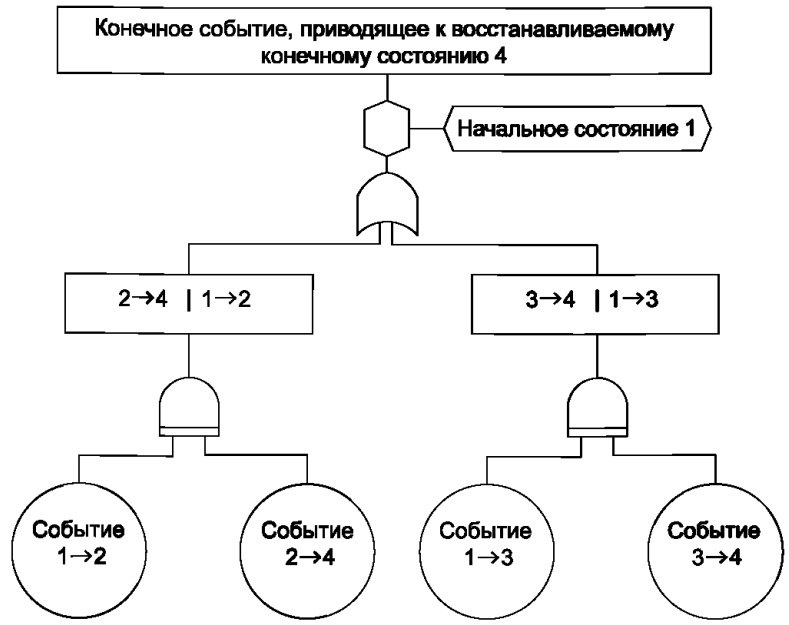
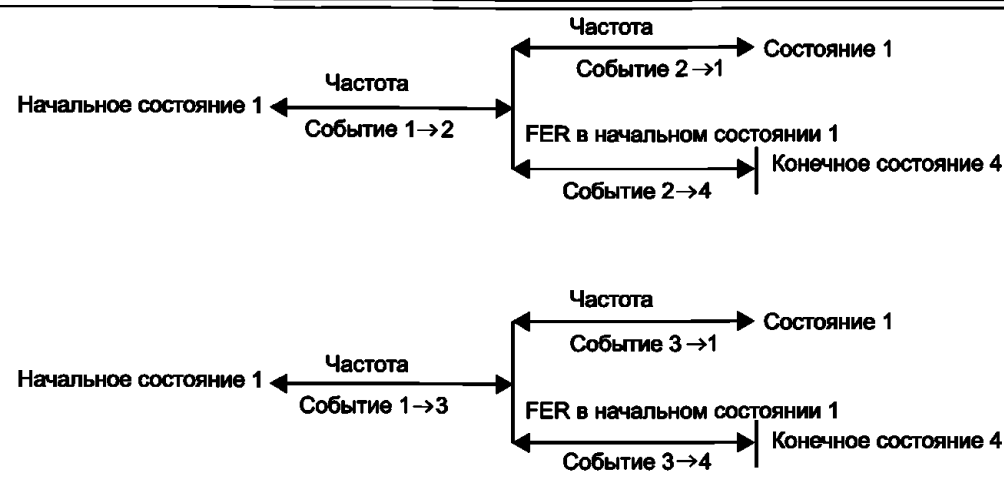
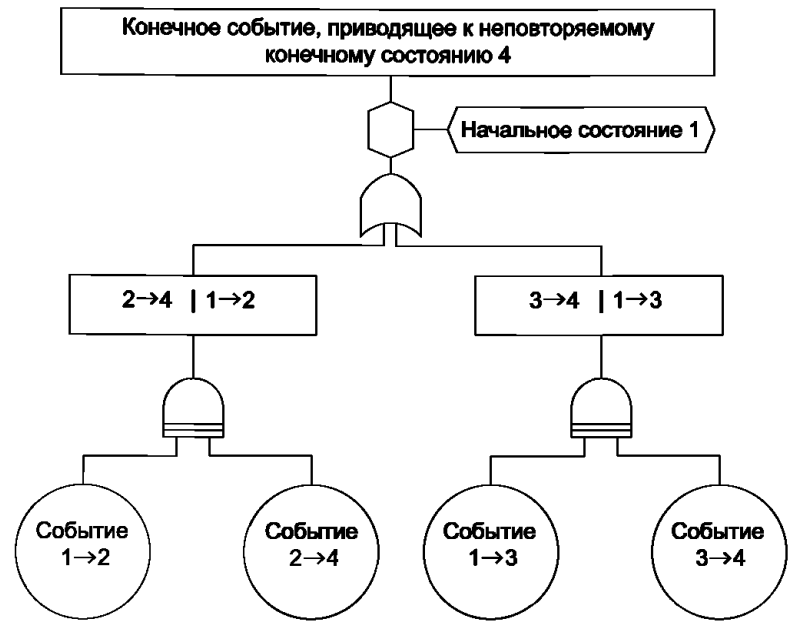
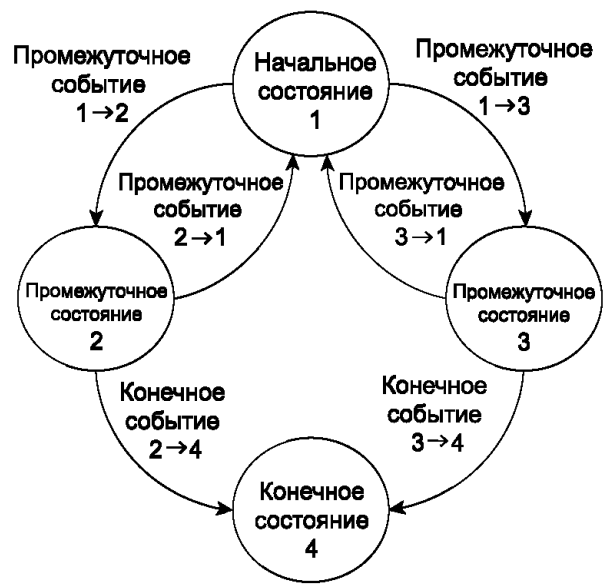
Метод	Схема
ETA	
FTA	
Марковская диаграмма состояний	

Таблица 5 — Символы и графическое представление для невосстанавливаемого конечного состояния

Метод	Схема
ETA	
FTA	
Марковская диаграмма состояний	

7.1.3 Неповторяемое конечное событие, приводящее к восстанавливаемому конечному состоянию

В таблице 4 приведены символы и графические представления для определения оценки FER в начальном состоянии 1 для неповторяемого конечного события, которое приводит к восстанавливаемому конечному состоянию путем использования методов ETA, FTA и марковского метода. Риск представлен аналогичным образом в таблице 3 с начальным состоянием 1, промежуточными состояниями 2 и 3,

и конечным состоянием 4 и событиями 1 → 2, 2 → 1, 2 → 4, 1 → 3, 3 → 1, 3 → 4 и 4 → 1, как показано в дереве событий FT и марковской диаграмме состояний в таблице 4.

Здесь события 2 → 4 и 3 → 4 являются конечными событиями, а событие 4 → 1 является восстановлением. Конечное событие изменяет риск, т. е. пути перехода из начального состояния в конечное состояние, потому что состояние системы в целом непрерывно изменяется под влиянием конечного события, и аналогичный риск тоже изменяется до тех пор, пока система в целом не будет реструктурирована.

Ветвь дерева событий в таблице 4, которая имеет стрелку на правом конце, означает, что это событие приводит к восстанавливаемому конечному состоянию. Эту ветвь классифицируют как неповторяемую типа 2. Вентиль «И» с горизонтальной линией на диаграмме FT означает, что выход из вентиля приводит к восстанавливаемому конечному состоянию, и вентиль «И» классифицируют как вентиль «И» типа 2.

Значение FER в начальном состоянии 1 рассчитывают, используя эти диаграммы.

7.1.4 Неповторяемое конечное событие, приводящее к невосстанавливаемому конечному состоянию

В таблице 5 приведены символы и графические представления для анализа неповторяемого конечного события, приводящего к невосстанавливаемому конечному состоянию с помощью использования дерева событий (FT) и марковской диаграммы состояний. Риск представлен аналогично представлению, приведенному в таблице 3 для начального состояния 1, промежуточных состояний 2 и 3 и конечного состояния 4, а также событий 1 → 2, 2 → 1, 2 → 4, 1 → 3, 3 → 1 и 3 → 4, как показано в таблице 5. Конечными событиями являются 2 → 4 и 3 → 4. Конечные события соответствуют настолько существенным изменениям системы в целом, что она не может быть восстановлена.

Ветвь дерева событий в таблице 5, которая имеет две стрелки и вертикальную линию в правом конце, означает, что событие, соответствующее этой ветви, приводит к невосстанавливаемому конечному состоянию, эту ветвь классифицируют как неповторяемую ветвь типа 3. Вентиль «И» с двумя горизонтальными линиями в FT в таблице 5 означает, что выход такого вентиля приводит к невосстанавливаемому конечному состоянию, его классифицируют как вентиль «И» типа 3.

Здесь FER в начальном состоянии 1 идентичен FER в начальном состоянии 1, полученной в соответствии с 7.1.3 для восстанавливаемой системы с восстанавливаемым конечным состоянием (см. 5.5).

7.2 Аналитический пример неповторяемого конечного события

7.2.1 Общие положения

Предположим, что риск представлен начальным состоянием A, промежуточными состояниями B и D и конечным состоянием C, а также двумя путями из начального состояния в конечное состояние, A → B → C и A → D → C. Здесь предполагается, что конечное событие является неповторяемым и единственный путь A → B → C приводит в конечное состояние, в котором появляются окончательные последствия риска (см. 3.1.10, примечание 1). На рисунке 5 описана причина неповторяемого конечного события. На рисунке состояние системы D опущено, поскольку конечное событие через путь A → D → C не приводит в какое-либо конечное состояние, в котором проявляются окончательные последствия риска. Причины конечного события также могут быть смоделированы с помощью марковской диаграммы состояний, приведенной на рисунке 6.

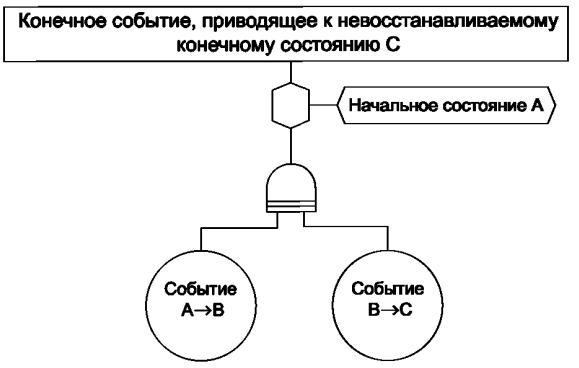
По крайней мере, два риска, связанных с отказом системы управления подушками безопасности автомобиля, выявлены в [7]: 1) система управления подушками безопасности ошибочно наполняет подушку, когда автомобиль движется в нормальном режиме; 2) система управления подушками безопасности не наполняет подушку безопасности при аварии. Система управления подушками безопасности обычно состоит из электротехнических элементов, таких как датчики, контроллеры и приводы. Риск ошибочного наполнения подушек безопасности можно считать реальным примером модели перехода состояния, приведенной на рисунке 6. В этом случае риск представляют состояния системы A—D на рисунках 5 и 6.

A — автомобиль стоит, система управления подушками безопасности находится в работоспособном состоянии;

B — автомобиль движется, система управления подушками безопасности находится в работоспособном состоянии;

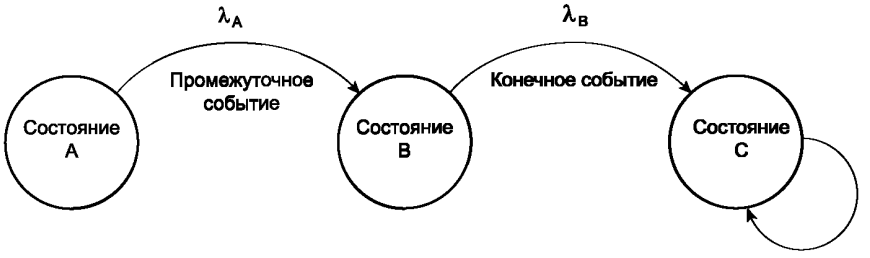
C — автомобиль движется в нормальном режиме, подушки безопасности ошибочно наполнены;

D — автомобиль стоит, подушки безопасности ошибочно наполнены.



Примечание — Состояние системы D на рисунке не приведено.

Рисунок 5 — FT для неповторяемого конечного события, которое приводит к невосстанавливаемому конечному состоянию



λ_A, λ_B – интенсивности переходов

Состояние системы А: начальное состояние (предшествующее состояние);
Состояние системы В: промежуточное состояние (предшествующее состояние);
Состояние системы С: конечное состояние

Рисунок 6 — Модель состояний с невосстанавливаемым конечным состоянием

Если система управления подушками безопасности наполняет подушки безопасности в состоянии системы В, происходит переход из состояния В в состояние С, и это может привести к дорожно-транспортному происшествию для системы в целом, включающей в себя водителя и дорожные условия. Переход из состояния А в состояние С осуществляется по пути А → В → С.

Если ошибочное наполнение подушек безопасности происходит в состоянии системы А, происходит переход из состояния А в состояние D. Однако аварии не произойдет, даже если возникнет переход из состояния D в состояние С, потому что подушки безопасности не могут быть наполнены при движении автомобиля, т. е. когда рабочий аварийной бригады транспортирует поврежденный автомобиль в автомастерскую. Последовательность таких событий представляет путь А → D → С (как упоминалось выше). Таким образом, конечным событием, которое может привести к дорожно-транспортному происшествию, является ошибочное наполнение подушек безопасности при движении автомобиля, т. е. только переход из состояния В в состояние С. Это конечное событие называют также критическим событием (ГОСТ Р 27.010).

Здесь начало состояния движения автомобиля является запросом к активации функции системы управления подушками безопасности для предотвращения их ошибочного наполнения, поскольку ошибочное наполнение подушек может привести к дорожно-транспортному происшествию. Таким образом, состояние системы В можно рассматривать как состояние запроса функции системы управления подушками безопасности для предотвращения ошибочного их наполнения.

В соответствии с рисунком 6, если предполагается, что запросы и отказы системы управления подушками безопасности происходят случайно и не зависят от времени, в качестве интенсивностей запросов и отказов функции системы управления подушками безопасности могут быть назначены постоянные величины λ_A [1/ч] и λ_B [1/ч] соответственно (см. 9.3.1 b)).

7.2.2 Средняя частота конечного события

Предположим, что общая система, в которой риск представлен на рисунках 5 и 6, находится в начальном состоянии А в момент времени 0 и $P_{A,A}(t)$ и $P_{A,B}(t)$ — вероятности того, что вся система в целом

находится в состоянии A, и в состоянии B в момент времени t, при условии, что переходы из состояния B в состояние A, и из состояния D в состояние A в интервале времени [0, t] не происходят. Эти вероятности можно записать следующим образом:

$$P_{A,A}(t) = \{\exp(-\lambda_A t)\}\exp(-\lambda_B t), \quad (12)$$

$$P_{A,B}(t) = \{1 - \exp(-\lambda_A t)\}\exp(-\lambda_B t), \quad (13)$$

где t — время;

λ_A — интенсивность спроса, т. е. постоянная интенсивность перехода из состояния A в состояние B (и из состояния D в состояние C) [1/ч];

λ_B — интенсивность отказов, т. е. постоянная интенсивность перехода из состояния B в состояние C (и из состояния A в состояние D) [1/ч].

Частота конечного события, которое приводит к конечным последствиям риска, $\omega_A(t)$ [1/ч], имеет вид (14)? при условии что система находится в начальном состоянии A в момент времени 0 и переходы B → A и D → A не происходят в интервале времени [0, t]

$$\omega_A(t) = \omega_{ABC}(t) = \lambda_B P_{A,B}(t) = \lambda_B\{1 - \exp(-\lambda_A t)\}\exp(-\lambda_B t), \quad (14)$$

где $\omega_{ABC}(t)$ — частота конечного события, возникающего в результате пути A → B → C [1/ч].

Частота конечного события, возникающего в результате переходов A → D → C, $\omega_{ADC}(t)$ не вносит вклад в $\omega_A(t)$, поскольку конечное событие не приводит к конечному состоянию, в котором появляются конечные последствия риска, а именно: $\omega_A(t) = \omega_{ABC}(t) + \omega_{ADC}(t) = \omega_{ABC}(t)$.

Средняя FEF, полученная из уравнения (14), $\omega_A(0, T)$ [1/ч] имеет вид (см. 3.1.22 и 3.1.30):

$$\omega_A(0, T) = \omega_{ABC}(0, T) = (1/T)[1 - \exp(-\lambda_B T) - \{\lambda_B/(\lambda_A + \lambda_B)\}\,[1 - \exp\{-(\lambda_A + \lambda_B)T\}]] =$$

$$= (1/T)\,[\{\lambda_A/(\lambda_A + \lambda_B)\} - \exp(-\lambda_B T) + \{\lambda_B/(\lambda_A + \lambda_B)\}\exp\{-(\lambda_A + \lambda_B)T\}], \quad (15)$$

где $\omega_{ABC}(0, T)$ — средняя частота конечного события, возникающего в результате переходов A → B → C [1/ч];

T — экспозиция риска [ч] (см. 3.1.30).

Приведенные ниже соотношения могут быть распространены на средние FEF, т. е. в соответствии с (14) и (15), если $\omega_A(t) = \omega_{ABC}(t)$, то $\omega_A(0, T) = \omega_{ABC}(0, T)$ABC (0, T):

a) если $\lambda_A t << 1$ и $\lambda_B t << 1$, то $\omega_A(t) \approx \lambda_A\lambda_B t$.

Если $1 << 1 << \lambda_A t$ и $\lambda_B t << 1$, то $\omega_A(t) \approx \lambda_B$.

Если $0 < t < (1/\lambda_A)\ln\{(\lambda_A + \lambda_B)/\lambda_B\}$, то $\omega_A(t)$ стремится к своему максимальному значению $\lambda_B[1 - \exp[-\ln\{(\lambda_A + \lambda_B)/\lambda_B\}]]\exp[-\lambda_B/\lambda_A)\ln\{(\lambda_A + \lambda_B)/\lambda_B\}]$.

Если $(1/\lambda_A)\ln\{(\lambda_A + \lambda_B)/\lambda_B\} < t$, то $\omega_A(t)$ стремится к 0;

b) если $\lambda_A T << 1$ и $\lambda_B T << 1$, то $\omega_A(0, T) \approx \lambda_A\lambda_B T/2$;

c) если $1 << \lambda_A T$ и $\lambda_B T << 1$, то $\omega_A(0, T) \approx \lambda_B$.

Стандарты серии ГОСТ Р МЭК 61508 (все части) представляют собой комплекс стандартов в области функциональной безопасности, определяемой на основе риска, и устанавливают полноту безопасности, в том числе среднюю частоту отказов (PFH) объекта, связанного с безопасностью, в качестве целевого показателя отказов объекта для контроля и/или снижения риска в режиме большого количества запросов или непрерывной работы, на основе этой приближенной формулы для средней FEF, $\omega_A(0, T) \approx \lambda_B$ (см. 3.1.33 и B.1). Здесь λ_B — интенсивность опасного отказа объекта, связанного с безопасностью, которая является целевым показателем полноты безопасности объекта (см. B.2). Интенсивность завершения запроса в стандартах серии ГОСТ Р МЭК 61508 не рассмотрена;

d) если $0 < T < T^*$, то стремится к своему максимальному значению

$(1/T^*)[\{\lambda_A/(\lambda_A + \lambda_B)\} - \exp(-\lambda_B T^*) - \{\lambda_B/(\lambda_A + \lambda_B)\}\exp\{-(\lambda_A + \lambda_B)T^*\}$, где T^* — значение, удовлетворяющее уравнению (16)

$$\exp(-\lambda_B T^*) - \{\lambda_B/(\lambda_A + \lambda_B)\}\exp\{-(\lambda_A + \lambda_B)T^* + \lambda_B T^*[\exp(-\lambda_B T^*) - \exp\{-(\lambda_A + \lambda_B)T^*\}] = \lambda_B/(\lambda_A + \lambda_B); \quad (16)$$

e) если $T^* < T$, то $\omega_A(0, T)$ стремится к 0.

7.2.3 Интенсивность конечного события для заданного начального состояния

Если система в целом находится под воздействием риска, как показано на рисунках 5 и 6 с экспозицией риска T, то необходимо определить оценку FER для начального состояния A, т. е. величину, обратную среднему времени от начального состояния A до конечного состояния C (т. е. величину, обратную среднему времени от $t = 0$ до появления неповторяемого конечного события).

Модель причин конечного события для системы с восстановлением показана на рисунках 7 и 8, на которых состояния системы A, B, C и D (опущенное) имеют те же особенности, что и на рисунке 6, соответственно. Если средняя продолжительность состояния запроса составляет τ часов, а завершение запроса в соответствии с моделью происходит с постоянной интенсивностью $1/\tau$ [1/ч], то FEF и FER для начального состояния A могут быть сформированы с использованием моделей, приведенных на рисунках 7 и 8.

Предположим, что $P_{A,A}$, $P_{A,B}$ и $P_{A,C}$ — вероятности того, что система в целом находится соответственно в состояниях A, B и C в стационарном состоянии. Тогда $P_{A,A}$, $P_{A,B}$ и $P_{A,C}$ можно записать следующим образом (если m [1/ч] — постоянная интенсивность восстановления) (см. 9.3.1, b)):

$$P_{A,A} = (\lambda_A + 1/\tau)(\lambda_B + 1/\tau)/\{(\lambda_A + 1/\tau)(\lambda_B + 1/\tau) + \lambda_A(\lambda_A + 1/\tau)(1 + \lambda_B/m) + \lambda_B(\lambda_B + 1/\tau)(1 + \lambda_A/m)\} \quad (17)$$

$$P_{A,B} = \{\lambda_A (\lambda_B + 1\tau)\}P_{A,A} \quad (18)$$

$$P_{A,C} = [\{\lambda_A/(\lambda_B + 1/\tau)\} (\lambda_B/m) + \{\lambda_B/(\lambda_A + 1/\tau)\}(\lambda_A/m)]P_{A,A}. \quad (19)$$

Если экспозиция риска равна T (см. 3.1.30 и 5.3), то FEF для начального состояния A, в котором появляются конечные последствия риска ω_A, обратной величиной к которой является среднее время от начального состояния A до первого события восстановления (см. рисунок 8), можно записать

$$\omega_A = \omega_{ABC} = \lambda_B P_{A,B} = \lambda_B\{\lambda_A/(\lambda_B + 1/\tau)\}(\lambda_A + 1/\tau)(\lambda_B + 1/\tau)/\{(\lambda_A + 1/\tau)(\lambda_B + 1/\tau) + \lambda_A(\lambda_A + 1/\tau)(1 + \lambda_B/m) + \lambda_B(\lambda_B + 1/\tau)(1 + \lambda_A/m)\}, \quad (20)$$

где ω_{ABC} — FEF для начального состояния A, когда конечное событие возникает в результате переходов $A \rightarrow B \rightarrow C$ [1/h].

Аналогично FEF для начального состояния A, когда конечное событие возникает в результате переходов $A \rightarrow D \rightarrow C$, ω_{ADC} [1/h], не вносит вклад в ω_A, а именно: $\omega_A = \omega_{ABC} + \omega_{ADC} = \omega_{ABC}$.

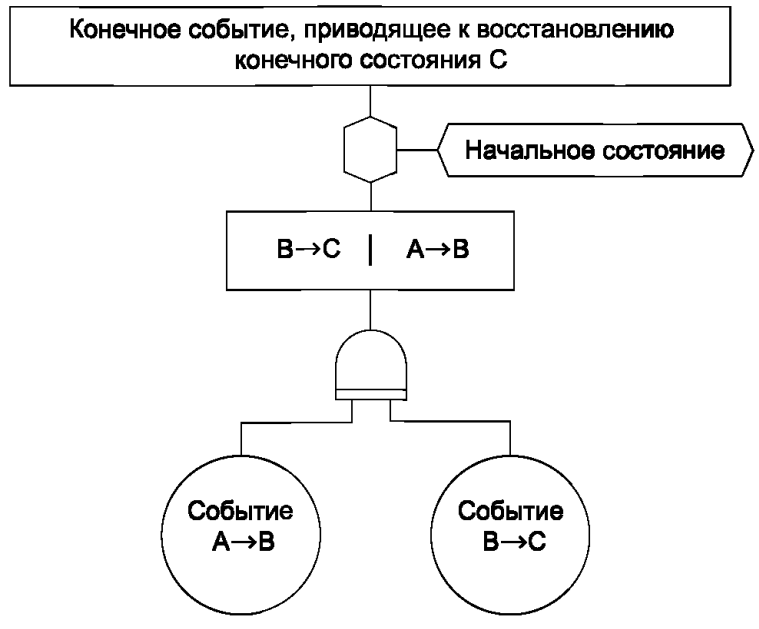


Рисунок 7 — FT для неповторяемого конечного события, приводящего к восстанавливаемому конечному состоянию

Если T — экспозиция риска, то в соответствии с (20) FER для начального состояния A, φ_A является величиной, обратной к среднему времени от начального состояния A до конечного состояния C (см. рисунок 7 и рисунок 8), а также к среднему времени от состояния A до состояния C (см. рисунок 5 и рисунок 6) и имеет вид:

$$\varphi_A = \varphi_{ABC} = \omega_{ABC}/\{1 - P_{A,C}\} = \lambda_A \lambda_B/[(\lambda_B + 1/\tau)\{1 + \lambda_A/(\lambda_B + 1/\tau) + \lambda_B/(\lambda_A + 1/\tau)\}], \quad (21)$$

где φ_{ABC} — FER для начального состояния A, если конечное событие возникает в результате переходов $A \rightarrow B \rightarrow C$ [1/h].

Аналогично FER для начального состояния A, если конечное событие возникает в результате переходов $A \rightarrow D \rightarrow C$, φ_{ADC} не вносит вклад в φ_A, т. е. $\varphi_A = \varphi_{ABC} + \varphi_{ADC} = \varphi_{ABC}$.

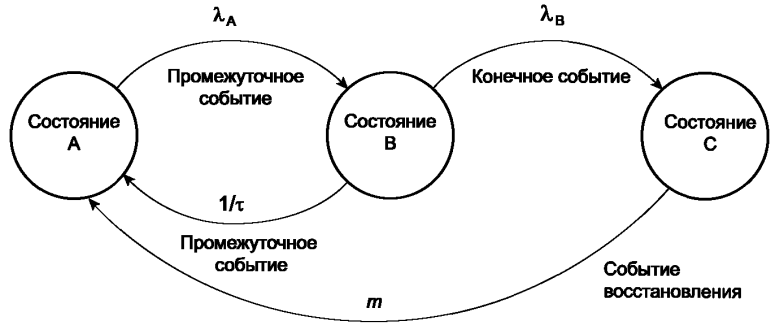


Рисунок 8 — Переходы, приводящие к восстановлению конечного состояния

На основе (21) можно заключить следующее.

a) Если $\lambda_A\tau << 1$ и $\lambda_B\tau << 1$, то $\varphi_A = \varphi_{ABC} \approx \lambda_A \lambda_B \tau$. Эта приближенная формула идентична формуле для средней FEF, при условии $\tau = T/2$ (см. 7.2.2, b), 9.3.2 и приложение B).

В случае системы управления подушками безопасности для переходов A → B → C ясно, что вероятность $\varphi_A/\lambda_B = \varphi_{ABC}/\lambda_B \approx \lambda_A\tau$ — приближенно равна средней вероятности того, что система в целом находится в состоянии запроса системы управления подушками безопасности при появлении отказа системы управления подушками безопасности. С другой стороны для перехода A → B → C также ясно, что отношение $\varphi_A/\lambda_A = \varphi_{ABC}/\lambda_A \approx \lambda_B\tau$ — приближенно равно вероятности того, что отказ системы управления подушками безопасности произойдет в течение среднего времени запроса [0, τ] при условии, что запрос возник в момент времени 0. А именно, $\varphi_{ABC}/\lambda_A \approx \lambda_B \tau$ равно APF_{drg}, т. е. $\varphi_{ABC}/\lambda_A \approx \lambda_B \tau \approx P_b$.

Однако в стандартах серии ГОСТ Р МЭК 61508 (все части) предполагается, что переходы A → D → C могут привести к конечному событию, в котором появляются конечные последствия риска в результате отказа объекта в режиме редких запросов. А именно предполагается $\varphi_{ABC} = 0$. FER (или HER в стандартах серии ГОСТ Р МЭК 61508 (все части)) φ является целевым показателем конечного события для объекта в режиме редких запросов, и определяется только приближенно $\varphi \approx \lambda_B \lambda_A \tau \approx \varphi_{ADC}$, т. е. $\varphi \approx \lambda_B \lambda_A \tau \approx \lambda_A P_a$, где λ_A и λ_B — интенсивность запроса объекта и интенсивность (опасных)отказов объекта соответственно (см. 9.3.2 и приложение B).

Если конечное событие вызвано только запросом, который возникает в результате отказа объекта, т. е. конечное событие возникает только в результате перехода A → D → C, то вероятность $\varphi_A/\lambda_A = \varphi_{ADC}/\lambda_A \approx \lambda_B\tau = \lambda_B T/2$ — приближенно равна средней вероятности того, что объект отказал в момент времени t ($0 < t \le T$), при условии, что объект находится в работоспособном состоянии в нулевой момент времени и $\lambda_B T/2 << 1$.

Эта приближенная средняя вероятность $\lambda_B\tau = \lambda_B T/2$ ($=P_a$) в стандартах серии ГОСТ Р МЭК 61508 определена как «средняя вероятность отказа по запросу (PFD_{avg}). В настоящее время только PFD_{avg} является целевым показателем отказа уровня полноты безопасности для объекта в режиме работы с редкими запросами, как упомянуто выше. Таким образом, стандарты серии ГОСТ Р МЭК 61508 (все части) не могут охватывать такие объекты, как система управления подушками безопасности, рассмотренные выше, если эти системы работают в режиме с редкими запросами (см. 9.3.2 и приложение B);

b) если $1 << \lambda_A\tau$ и $\lambda_B \tau << 1$, то $\varphi_A \approx \varphi_{ABC} \approx \lambda_B$. Это приближение аналогично приближению для средней FEF (см. 7.2.2 c), 9.3.2 и приложение B);

c) если $1 << \lambda_A\tau$ и $\lambda_B \tau << 1$, то φ_A ($= \varphi_{ABC}$) стремится к $\lambda_A/(1 + \lambda_A/\lambda_B + \lambda_B/\lambda_A)$. Эта характеристика сильно отличается от средней FEF (см. 7.2.2, d), e) и приложение B).

В случае системы управления подушками безопасности, упомянутой выше, состояние системы B на рисунках 5—8, в котором автомобиль передвигается, является состоянием запроса функции системы управления подушками безопасности, предотвращающей ошибочное наполнение подушек безопасности. Таким образом промежуточные события перехода системы A → B и B → A на рисунке 8 являются началом запроса и его завершением соответственно. Предположим, что возникновение промежуточных событий подчиняется экспоненциальному распределению, а средняя продолжительность состояния спроса составляет τ часов, тогда для завершения запроса может быть применена модель с постоянной интенсивностью 1/τ [1/ч]. В этом случае $2/T = 1/\tau$ и поэтому 2τ часов составляет экспозиция риска T системы управления подушками безопасности. Здесь снова интенсивность завершения запросов не рассмотрена в стандартах серии ГОСТ Р МЭК 61508 (все части).

Если система управления подушками безопасности проанализирована в соответствии со стандартами серии ГОСТ Р МЭК 61508 (все части), для контроля и/или снижения риска должны быть рассмотрены (как описано выше) два экстремальных целевых показателя объекта. Например, приближенными значениями HER являются: $\varphi \approx \lambda_B \lambda_A T/2 = \varphi_{ADC}$ и $\varphi \approx \omega_A (0, T) \approx \lambda_B$ для объектов со структурой «1 из 1» в режиме работы с редкими запросами и в режиме большого количества запросов или непрерывной работы соответственно. Таким образом, целевой показатель PFD_{avg} для первого равен $\varphi/\lambda_A \approx \lambda_B T/2$ (= P_a), а целевой показатель PFH для последнего равен $\omega_A(0, T) \approx \lambda_B$ (см. 3.1.32, 3.1.33 и B.1) соответственно.

Однако приближенное значение HER равно $\varphi \approx \lambda_B \lambda_A \tau \approx \varphi_{ADC}$, и следовательно PFD_{avg} (что эквивалентно $P_a = \varphi/\lambda_A \approx \lambda_B \tau$) не может быть получено для риска ошибочного наполнения подушек безопасности, поскольку на самом деле переходы A → D → C не приводят к конечному состоянию, в котором появляются конечные последствия риска.

FER для заданного начального состояния представляет решение проблемы для PFD_{avg} в области функциональной безопасности путем введения нового целевого показателя объекта для снижения и/или контроля риска в режиме работы с редкими запросами. Этот новый целевой показатель — коэффициент снижения риска φ_A/λ_A, где φ_A — FER для заданного начального состояния, а λ_A — интенсивность запросов. Формула для коэффициента снижения риска (например, $\varphi_A/\lambda_A = (\varphi_{ABC} + \varphi_{ADC})/\lambda_A$) почти равна сумме APF_{drg} и PFD_{avg} в режиме работы с редкими запросами. Таким образом, если $\varphi_{ADC} = 0$, коэффициент снижения риска $\varphi_A/\lambda_A = \varphi_{ABC}/\lambda_A$ почти равен APF_{drg}. В то время как, если выполняется $\varphi_{ABC} = 0$, то коэффициент снижения риска почти равен PFD_{avg}. Таким образом, коэффициент снижения риска φ_A/λ_A может охватывать PFD_{avg} и APF_{drg} для обоих вариантов переходов A → B → C и A → D → C (см. 9.3.2, B.4, B.5, B.6 и B.7). Численный анализ иллюстрируют следующие примеры.

1) Предположим, что водитель управляет личным автомобилем, когда интенсивность перехода состояний составляет $\lambda_A = 0{,}1$ [1/ч] (т. е. водитель управляет автомобилем в среднем каждые 10 ч), $1/\tau = 2{,}0$ [1/ч] (т. е. автомобиль находится в движении в среднем 30 мин) и $\lambda_B = 1{,}0 \cdot 10^{-5}$ [1/ч]. Тогда режим редких запросов является предпочтительным для анализа и сокращения риска, соответствующего системе управления подушками безопасности, поскольку частота запросов $1/(1/\lambda_A + \tau) \approx 0{,}1$ [1/ч] меньше обратной величины экспозиции риска $1/T = 1/(2\tau) = 1{,}0$ [1/ч]. Таким образом, приближенная формула дает оценку $\varphi_A = \varphi_{ABC} \approx \lambda_A \lambda_B \tau = 5{,}0 \cdot 10^{-7}$ [1/ч]. Точные оценки $\varphi_A = \varphi_{ABC} = 4{,}8 \cdot 10^{-7}$ [1/ч] и $\omega_A(0{,}2\tau) = \omega_{ABC}(0{,}2\tau) = 4{,}7 \cdot 10^{-7}$ [1/ч] рассчитывают по уравнениям (21) и (15) соответственно. Приближенная формула дает хорошее приближение.

2) Другим примером является такси, которое находится в движении более часто. $\lambda_A = 2{,}0$ [1/ч] (т. е. водитель управляет машиной каждые 30 мин), $1/\tau = 2{,}0$ [1/ч] (т. е. так же, как в 1)) и $\lambda_B = 1{,}0 \cdot 10^{-6}$ [1/ч]. Частота запроса $1/(1/\lambda_A + \tau) = 1{,}0$ [1/ч] находится на разделительной линии между двумя режимами работы по сравнению с $1/T = 1{,}0$ [1/ч]. Приближенные формулы: $\varphi_A = \varphi_{ABC} \approx \lambda_A \lambda_B \tau = 1{,}0 \cdot 10^{-6}$ [1/ч] (режим редких запросов) и $\omega_A (0{,}2\tau) = \omega_{ABC} (0{,}2\tau) \approx \lambda_B = 1{,}0 \cdot 10^{-6}$ [1/ч] (режим большого количества запросов), в то время как точная оценка составляет $\varphi_{ABC} = 5{,}0 \cdot 10^{-7}$ [1/ч] и $\omega_A (0{,}2\tau) = 5{,}7 \cdot 10^{-7}$ [1/ч] из уравнений (21) и (15) соответственно. В этом случае приближенные формулы $\varphi_A \approx \varphi_{ABC} \approx \lambda_A \lambda_B \tau$ и $\omega_A (0{,}2\tau) \approx \omega_{ABC} (0{,}2\tau) \approx \lambda_B$ дают в два раза более точные оценки (см. B.4).

Система управления подушками безопасности, рассмотренная выше, представляет собой последовательную систему. Однако реальные системы управления подушками безопасности могут включать резервирование и иметь более сложную структуру. Неисправные части системы могут быть обнаружены автоматически и система может перейти в состояние отключения для ремонта. Кроме того, процесс изучения причин ошибочного наполнения подушек безопасности может быть рассмотрен для анализа реального риска. Дерево FT и модели состояний, приведенные на рисунках 5 и 8, должны быть изменены на более реалистичные для такого анализа.

На рисунках 9 и 10 показан практический пример опасности, т. е. процесс ошибочного наполнения подушек безопасности в результате неисправности системы управления подушками безопасности [7]. Здесь предполагается, что система управления подушками безопасности представляет собой систему с архитектурой 1 из 2, т. е. система состоит из двух независимых каналов Ch1 и Ch2. В каждом канале происходят как обнаруженные (D), так и необнаруженные (UD) отказы, и оба канала имеют одинаковую интенсивность отказов D, λ_D и отказов UD, λ_{UD} соответственно (см. 9.3.1, b)). Безопасное состояние системы неизменно в отношении опасности ошибочного наполнения подушек (или риска), которое является противоположным по отношению к отказу системы управления подушками безопасности, приводящему к ненаполнению подушек безопасности при столкновении (см. B.2).

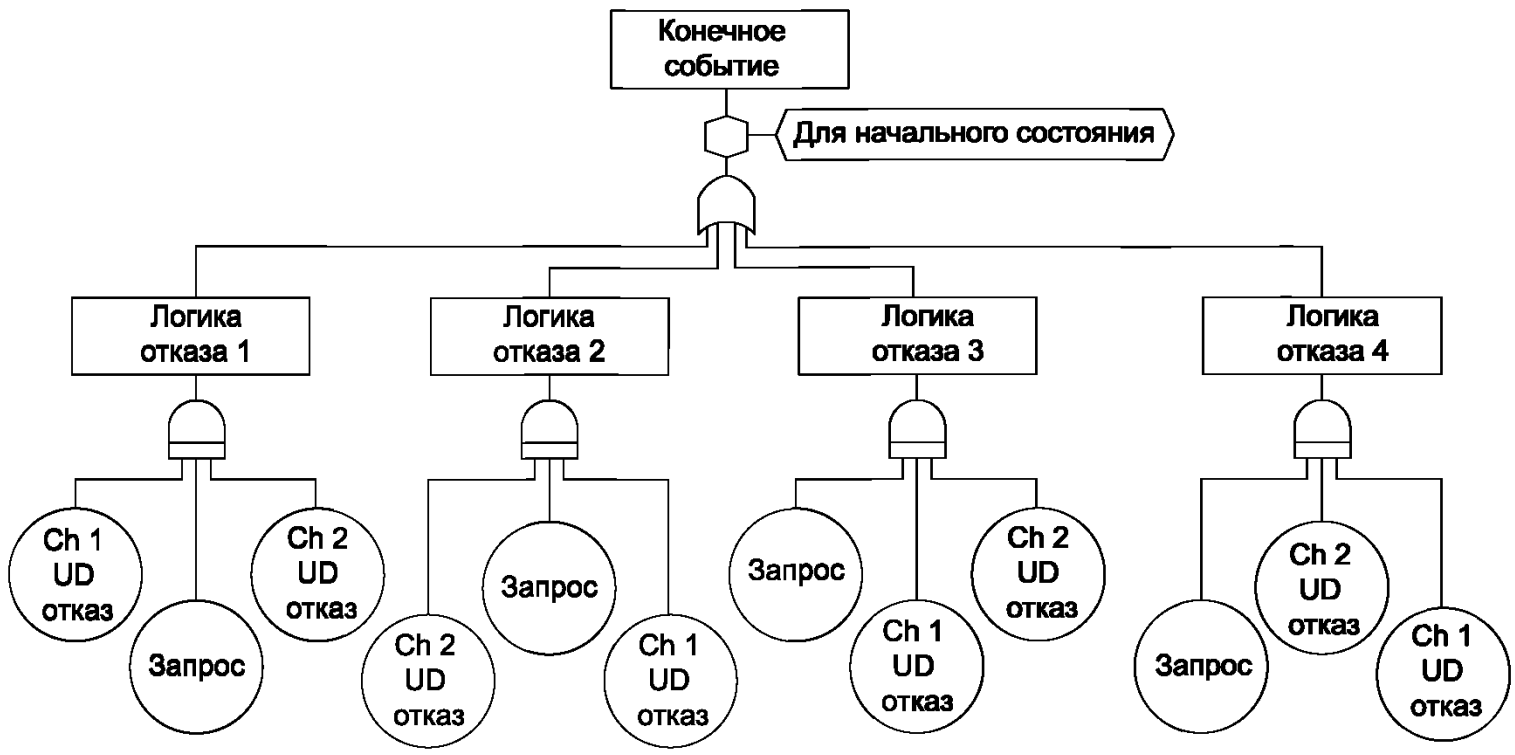
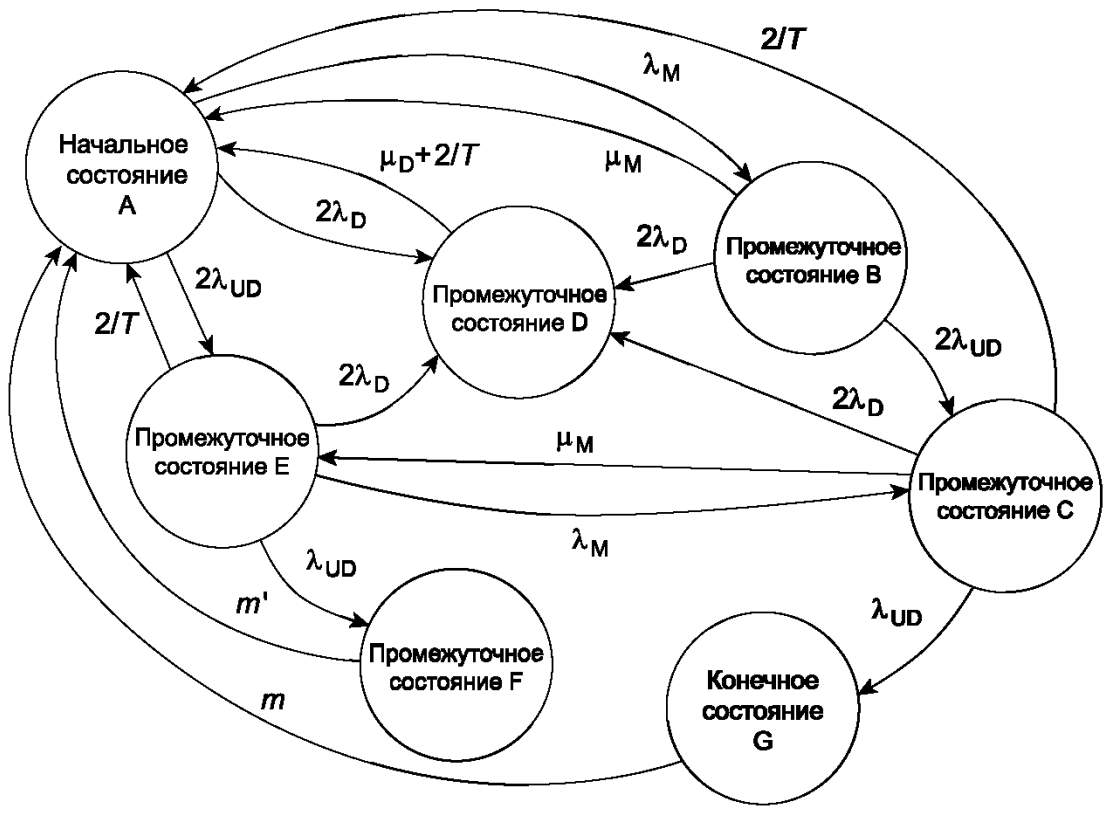


Рисунок 9 — FT для ошибочного наполнения подушек безопасности из-за отказа системы управления



Состояния системы

A: Оба канала находятся в работоспособном состоянии, когда автомобиль стоит;

B: Оба канала находятся в работоспособном состоянии, когда автомобиль движется;

C: В одном из каналов имеется невыявленный отказ (UD) при движении автомобиля;

D: система управления подушками безопасности отключена из-за обнаруженного отказа (D);

E: В одном из каналов имеется невыявленный отказ (UD), когда автомобиль стоит;

F: Ошибочное наполнение подушек безопасности при остановке автомобиля;

G: Ошибочное наполнение подушек безопасности, когда автомобиль движется.

Интенсивности переходов

λ_{UD} — интенсивность невыявленных отказов (UD) системы управления подушками безопасности;

λ_D — интенсивность выявленных отказов (D) системы управления подушками безопасности;

μ_D — интенсивность ремонта в состоянии остановки;

λ_M — интенсивность запросов;

μ_M — интенсивность завершения запросов;

m' — интенсивность ремонта при ошибочном наполнении подушек безопасности в состоянии остановки автомобиля;

m —интенсивность восстановления;

T — экспозиция риска ($1/T << \mu_M$ и $1/T << m'$)

Рисунок 10 — Модель состояний непреднамеренного наполнения подушек безопасности

Если отказ одного из каналов обнаружен функцией самодиагностики системы, датчик и блок управления системой управления подушками безопасности переводят систему в безопасное состояние и подают сигнал водителю, в этом случае ошибочное наполнение подушки не может произойти. Однако, если во время движения автомобиля в обоих каналах имеются невыявленные отказы (UD), то датчик и блок управления не могут предотвратить ошибочное наполнение подушки безопасности и может произойти дорожно-транспортное происшествие.

Отказы каналов по общей причине не представлены на рисунках 9 и10, поскольку эти отказы следует анализировать отдельно от независимых отказов (для простоты анализа). Экспозицией риска в данном случае является период контрольной проверки, если она предусмотрена, или срок службы системы управления подушками безопасности, если проверка отсутствует. Вероятности состояний системы от A до G на рисунке 10, P_A – P_G, легко рассчитать при условии, что система находится в стационарном состоянии. Оценку FER в начальном состоянии A, φ_A также легко рассчитать по формуле $\varphi_A = \lambda_{UD} P_C/(1 - P_G)$ [7].

Таким образом, аналитический метод оценки FER для данного начального состояния X, φ_X, охватывает широкий диапазон вопросов анализа риска, в том числе вопросы, которые не могут быть решены с помощью традиционных методов. Новые целевые показатели появления неповторяемого конечного события, т. е. FEF для заданного начального состояния ω_A и FER для заданного начального состояния φ_A сильно отличаются от традиционных целевых показателей надежности, таких как интенсивность отказов, частота отказа, вероятность безотказной работы, коэффициент готовности, поскольку формулы для ω_A и φ_A охватывают не только работоспособное и неработоспособное состояния объекта, а также состояния запроса, отсутствия запроса, отключения, конечные последствия риска, другие условия окружающей среды, а также экспозицию риска, которые не могут быть применены при обычном анализе надежности.

В общем случае, например, если экспозиция риска T не слишком велика и интенсивность перехода не слишком высока, т. е. если выполняются неравенства $\lambda_{AT} << 1$ и $\lambda_{BT} << 1$ или $1 << \lambda_{AT}$ и $\lambda_{BT} << 1$ (см. пример на рисунке 6), средняя FEF может почти равняться FER для заданного начального состояния. Однако эти показатели не идентичны, и если экспозиция риска T становится слишком большой, то FEF стремится к 0. По этой причине средняя FEF редко подходит в качестве целевого показателя возникновения неповторяемых конечных событий (см. раздел 4 и В.4).

Таким образом, риск ошибочного наполнения подушек безопасности, когда автомобиль движется в нормальном режиме, и риск ненаполнения подушек безопасности при столкновении (анализ которого опущен в настоящем стандарте) из-за отказа системы управления подушками безопасности можно анализировать отдельно для формирования профиля риска, данные которого необходимы на следующем этапе оценки риска [7].

8 Интенсивность конечного события для выявленного состояния и выявленной группы состояний

8.1 Общие положения

Необходимо непрерывно проводить мониторинг предыдущих состояний системы в целом в соответствии с ГОСТ Р ИСО 31000. Если предшествующее состояние или группа предшествующих состояний выявлены и обозначены для любого заданного времени, FER для выявленного состояния или FER для выявленной группы состояний следует анализировать на основе информации о мониторинге риска (см. 3.1.28 и 3.1.29). Например, при выявлении и мониторинге состояния 3 на диаграмме состояний системы в таблице 6 или группы состояний G, которая состоит из состояний системы 1 и 2 на диаграмме состояний в таблице 7, возможны следующие описания при определении оценки FER для выявленного состояния 3 и FER для группы состояний G.

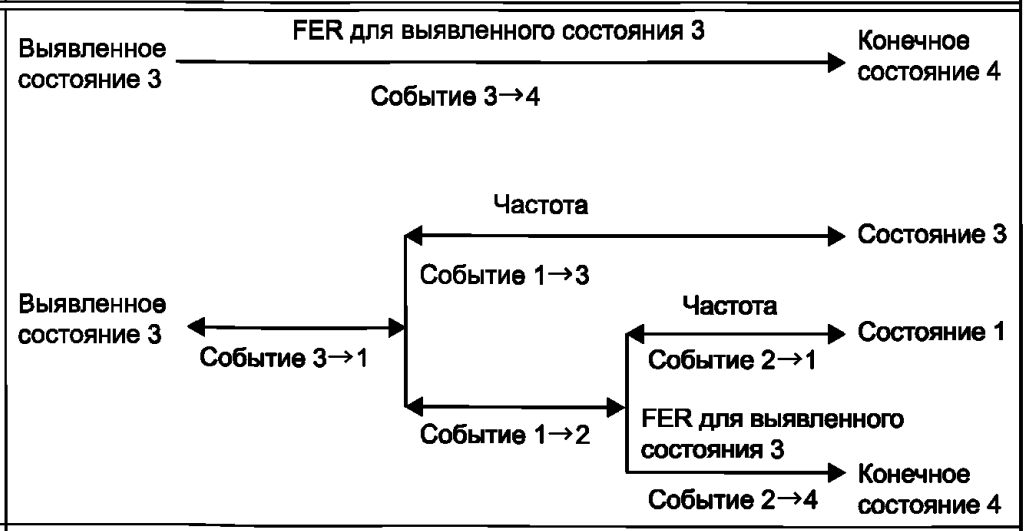
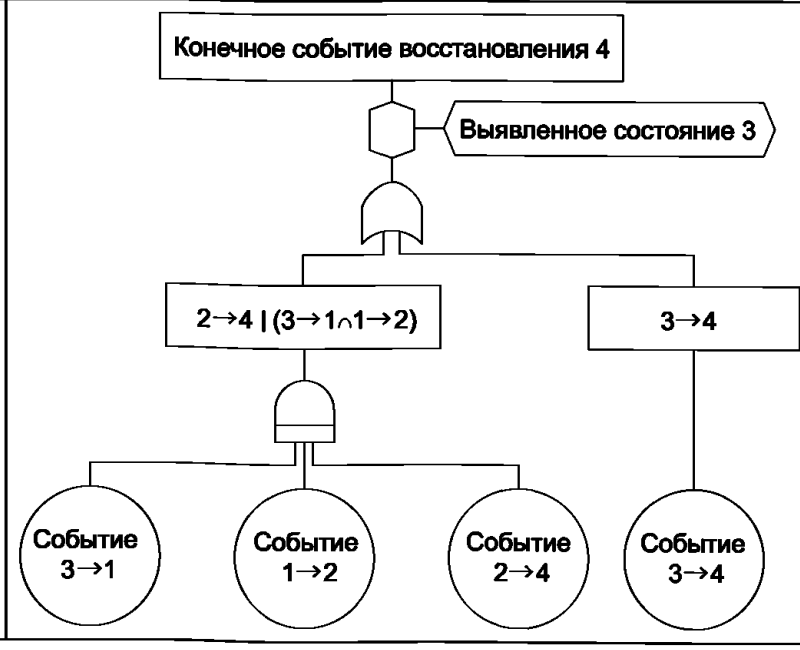
Если предшествующее состояние 3 выявлено в момент времени t, то FER выявленного состояния 3 анализируют для неповторяемого конечного события с использованием таблицы 6. FER для выявленного состояния 3 определяют как целевой показатель появления конечного события в момент времени t. В таблице 6 показаны обозначения и графическое представление, используемые при анализе FER для выявленного состояния 3 и неповторяемого конечного события с использованием методов ETA, FTA и марковского метода. Здесь предшествующее состояние 3 является виртуальным начальным состоянием, в которое конечное состояние 4 возвращается при восстановлении. Оценку FER для выявленного состояния 3 определяют с помощью этих диаграмм (см. 9.3.3). В таблице 7 приведены

обозначения и графическое представление, используемые при анализе FER для выявленной группы состояний G и неповторяемого конечного события с использованием ETA, FTA и марковского метода. Если группа состояний G распознана и проводится ее мониторинг в каждый момент времени *t*, то FER для выявленной группы состояний G определяют как целевой показатель появления конечного события в момент времени *t*. Оценку FER для выявленной группы состояний G определяют с помощью этих диаграмм (см. 9.3.4).

8.2 Пример выявленной группы состояний

На рисунке 10 начальное состояние A является выявленным состоянием в момент времени $t = 0$ сразу после контрольной проверки при условии, что контрольная проверка выполнена отлично. Если отказы по общей причине не учитывают, то состояния системы D и F являются выявленными в любое время, состояние системы G является конечным состоянием, состояния системы A и E составляют группу выявленных состояний G1, а состояния системы B и C — группу выявленных состояний G2 в любое время, кроме момента сразу после контрольной проверки (см. 9.4.6).

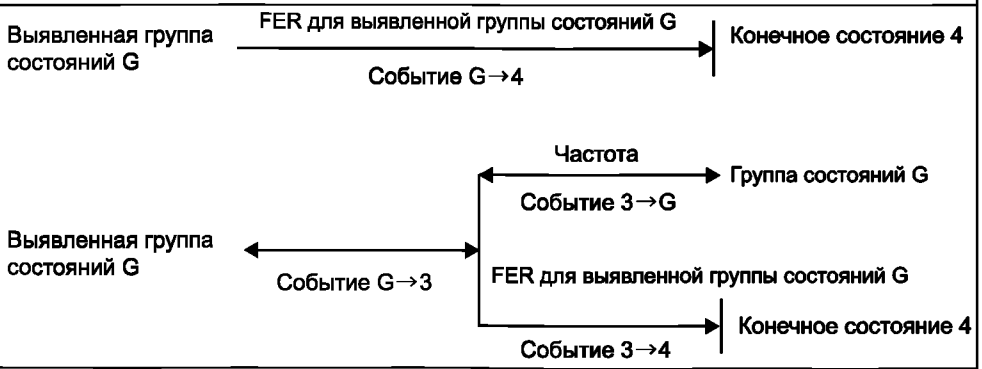
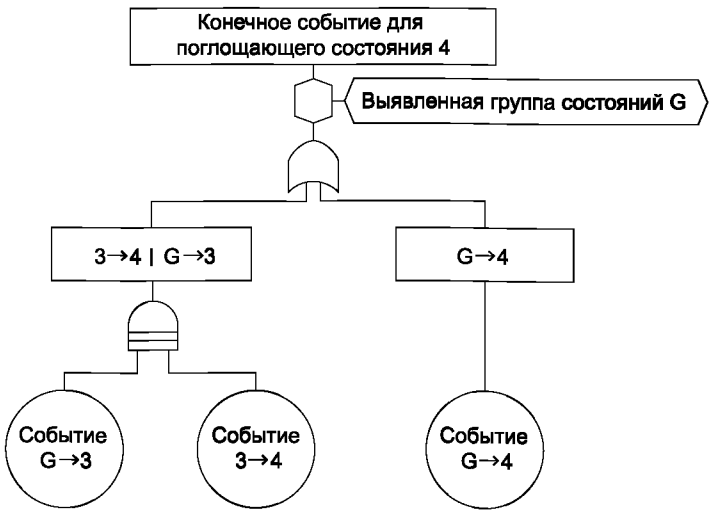
Таблица 6 — Обозначения и графическое представление FER в выявленном состоянии 3

Метод	Диаграмма
ETA	
FTA	

Окончание таблицы 6

Метод	Диаграмма
Марковский метод (диаграмма состояний)	

Таблица 7 — Обозначения и графическое представление FER для распознанной группы состояний G

Метод	Диаграмма
ETA	
FTA	

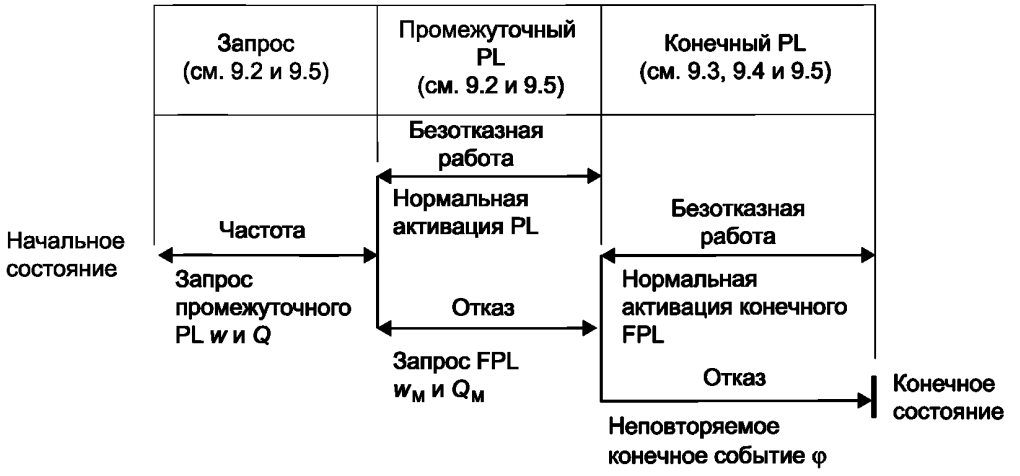
Окончание таблицы 7

Метод	Диаграмма
Марковский метод (диаграмма состояний)	

9 Анализ нескольких уровней защиты

9.1 Общие положения

Многоуровневая защита — это иерархическая система, которая активирует свои функции для предотвращения конечного события, которое может привести к возникновению конечного состояния риска. Если одному или нескольким уровням защиты PL не удается активировать свою функцию, этот отказ приводит к запросу на активацию функции следующего уровня защиты (см. рисунок 11). Уровень защиты, отказ которого может активировать следующий уровень защиты, классифицируют как промежуточный, а уровень защиты, который приводит к конечному состоянию системы в целом, классифицируют как конечный отказ (при анализе риска).



w, w_M — частоты запросов; Q, Q_M — вероятности состояний запроса; φ — FER для заданного начального состояния

Рисунок 11 — Дерево событий источника запросов, промежуточный и конечный уровни защиты при анализе риска

На рисунке 11 показано дерево событий для системы в целом с источником запросов, промежуточным и конечным уровнями защиты для контроля и/или снижения риска. Например, находящийся в эксплуатации автомобиль с водителем, его системы контроля движения и предаварийного контроля относятся к источнику запросов, предварительному и конечному уровням защиты от опасности столкновения, соответственно (см. В.2) [8], [9]. Эти системы контролируют и снижают риск аварии и делают FER для начального состояния соответствующей допустимому уровню (см. 3.1.1, примечание 3).

Если происходит отказ конечного уровня защиты в состоянии запроса (т. е. FPL отказывает в рабочем состоянии) или если запрос появляется, когда FPL отказал, обычно происходит конечное событие. Даже если конечное событие является неповторяемым, отказы промежуточных уровней защиты могут быть повторяемыми. Это означает, что запрос уровней защиты может быть повторяемым. Для таких повторяющихся событий, как отказы и запросы при составлении FTA уровней защиты (см. 9.2), полезно использовать вентиль «И» типа 1.

Если анализ риска выполняют с использованием методов RBD и FTA, для промежуточных уровней защиты могут быть выделены MCS (см. раздел 6). Здесь MCS представляет собой набор, состоящий из взаимно независимых основных элементов 1, 2,... и n (см. 3.1.35). Основными элементами являются события, такие как «отказ объекта», «отказ канала», «запрос объекта», «запрос канала» и т. д. Таким образом, основной элемент, например «отказ канала», может включать значительное количество отказов, вызванных состоянием сотен или более компонентов, составляющих канал. Восстановление нескольких каналов, которые составляют уровень защиты, часто может означать восстановление тысячи или более компонентов. Такой уровень защиты называют крупномасштабным. Анализ риска системы в целом, состоящей из крупномасштабных уровней защиты и поэтому обладающей несколькими рисками, часто называют анализом риска сложной системы (см. таблицу 1, раздел 6, 9.5, А.5, В.2 и В.3).

Риски, связанные с отказами уровней защиты, количественно рассмотрены в разделе 9. Как отказ промежуточного уровня защиты вызывает запрос следующего уровня защиты, показано для сложных систем с последовательной логикой отказов в 9.2. Затем анализ конечного уровня защиты показан в 9.3 и 9.4.

Обозначения

(0,0) конечный уровень защиты находится в работоспособном состоянии;

(0,1) конечный уровень защиты находится в состоянии UP (невыявленного отказа (UD) в состоянии запроса, т. е. конечный уровень защиты работы в обычном режиме;

(1,1) конечное состояние, т. е. состояние, в котором могут появиться конечные последствия риска;

λ_i — постоянная интенсивность событий базового элемента E_i (i = 1, 2,..., n: $E_i \in$ {1, 2,..., n}), из MCS, $\lambda_i > 0$ (интенсивность отказов, интенсивность запросов и т. д.) [1/ч];

μ_i — постоянная интенсивность ремонта базового элемента E_i (i = 1, 2,..., n) из MCS, $\mu_{ki} > 0$ (интенсивность ремонта, интенсивность завершения запросов и т. д.) [1/ч];

λ_{ki} — постоянная интенсивность событий базового элемента E_{ki} (i = 1, 2,..., n; $E_{ki} \in$ {1, 2,..., n}) из MCS K_k(k = 1, 2,..., m), $\lambda_{ki} > 0$ [1/ч];

μ_{ki} — постоянная интенсивность ремонта в состоянии E_{ki}, но $\mu_{ki} > 0$ [1/ч];

λ_{kSi} — постоянная интенсивность событий базовых элементов E_{kSi} (i = 1, 2,..., n; $E_{kSi} \in$ {1, 2,..., n}), которые включают последовательность базовых элементов S (= 1, 2,..., h) из MCS K_k (k = 1, 2,...,m), но $\lambda_{kSi} > 0$ [1/ч];

μ_{kSi} — постоянная интенсивность ремонта в состоянии E_{kSi}, но $\mu_{kSi} > 0$ [1/ч];

λ_{UD} — постоянная интенсивность невыявленных отказов UD конечного уровня защиты [1/ч];

μ_{UD} — величина, обратная к среднему времени восстановления невыявленного отказа конечного уровня защиты в процессе контрольной проверки [1/ч];

λ_D — постоянная интенсивность отказов конечного уровня защиты [1/ч];

μ_D — постоянная интенсивность ремонта конечного уровня защиты [1/ч];

λ_M — постоянная интенсивность запроса конечного уровня защиты [1/ч];

μ_M — постоянная интенсивность завершения запроса конечного уровня защиты (т. е. величина, обратная среднему времени до завершения запроса) [1/ч];

m — постоянная интенсивность восстановления [1/ч];

T — экспозиция риска для конечного уровня защиты [ч];

$P_{X,Y}(X, Y)$ — вероятность того, что система находится в состоянии системы (X, Y) в стационарном состоянии при условии, что она находится в состоянии системы (x, y) в момент времени 0, и ее конечное состояние вызывает переход только в состояние (x,y);

$P_{G_i(X, Y)}(t)$ — вероятность того, что система находится в состоянии (X, Y) в момент времени t при условии, что система входит в группу выявленных состояний G_i (i = 1, 2,..., n) в момент времени 0 и не покидает эту группу в течение времени t;

$\omega_{x,y}$ — FEF в начальном (или выявленном) состоянии (x, y) [1/ч];
φ_{xy} — FER в начальном (или выявленном) состоянии (x, y) [1/ч];
$T_{x,y}$ — MTFE в начальном (или выявленном) состоянии (x, y) [h];
$\varphi_{G_i}(t)$ — FER группы состояний G_i (динамическая оценка) [1/ч];
$T_{G_i}(t)$ — MTFE группы состояний G_i (динамическая оценка) [ч];
$\varphi_{G_i}(x, y)$ — центрированная по (x, y) FER группы состояний G_i [1/h];
$T_{G_i}(x, y)$ — центрированная по (x, y) MTFE группы состояний G_i [h];
$\{\varphi_{x,y}, T_{x,y}\}_{G_i}$ — набор FER в группе выявленных состояний G_i (i = 1, 2,..., n) ($\varphi_{x,y}$ и $T_{x,y}$ для всех (x, y), входящих в группу выявленных состояний G_i).

9.2 Частота и интенсивность повторяемых событий

9.2.1 Общие положения

Промежуточные уровни защиты организованы в виде систем произвольной структуры. Предполагается, что MCS K_1, K_2,...,K_m извлекаются в соответствии с произвольным значением m с помощью FTA для промежуточного уровня защиты и K_k (k = 1, 2, ...,m) состоит из произвольного числа основных элементов 1, 2,... и n. В общем случае базовые элементы часто, но не всегда, повторяются, однако в 9.2 предполагается, что все K_k основных элементов минимальных сечений повторяются, т. е. неравенство $\mu_{ki} > 0$ (i = 1, 2,..., n) выполняется для всех k (см. 9.1). Таким образом, количественный анализ вентиля «И» типа 1 показан как для непоследовательной, так и для последовательной логики отказов в 9.2.2 и 9.2.3, соответственно [10]—[12].

Для всех базовых элементов, которые не повторяются, т. е. i = 0 (i = 1, 2,..., n), Фассель и другие количественно определили логику последовательного отказа вентиля «И» для таких базовых элементов [13]. Тем не менее, если повторяющиеся и неповторяющиеся базовые элементы входят в минимальное сечение, то FEF для заданного начального состояния можно применять для количественного анализа вентиля «И», как показано в 9.3 и 9.4 [3], [5], [6].

9.2.2 Независимость от последовательности событий

Если повторные отказы промежуточного уровня защиты происходят независимо от последовательности базовых элементов, 1, 2,..., n, составляющих минимальное сечение K_k, то логика отказа, ведущая к вершине событий, может быть описана, например, как на рисунке 12 с вентилем «И» типа 1. Входными событиями в вентиль «И» типа 1 для минимальных сечений K_k являются базовые элементы 1, 2,... и n. Выходным событием вентиля «И» является высшее событие «отказ промежуточного уровня защиты» (из MCS K_k)».

Высшее событие становится истинным, если все входные события $E_{ki \neq j}$(i = 1, 2,..., n; $i \neq j$) становятся истинными раньше, чем входное событие E_{ki} становится истинным, при условии, что все входные события не являются истинными в нулевой момент времени. Эта логика отказа приводит к высшему событию, описанному на рисунке 12, где:

$E_{ki \neq j}$ — все базовые элементы i (i = 1, 2,... n; $i \neq j$) минимальных сечений K_k(k = 1, 2,..., m) становятся истинными;

E_{kj} — базовый элемент j (j = 1, 2,... n; но $j \neq i$) минимальных сечений K_k (k = 1, 2,..., m) становится истинным.

Высшее событие, описанное на рисунке 12, приводит к запросу следующего уровня защиты или конечного уровня защиты (см. рисунок 11). Таким образом, вероятность того, что следующий уровень защиты или конечный уровень защиты находятся в состоянии запроса Q_k* и частота запроса следующего уровня защиты или конечного уровня защиты w_k* в соответствии с минимальным сечением K_k в стационарном состоянии определены следующим образом:

Q_k* — вероятность того, что следующий уровень защиты или конечный уровень защиты находятся в состоянии запроса, которое является результатом запроса, возникшего в соответствии с логикой отказов промежуточного уровня защиты, как показано на рисунке 12, в стационарном состоянии;

w_k* — частота запроса, который возникает в соответствии с логикой отказов промежуточного уровня защиты, как показано на рисунке 12, в стационарном состоянии.

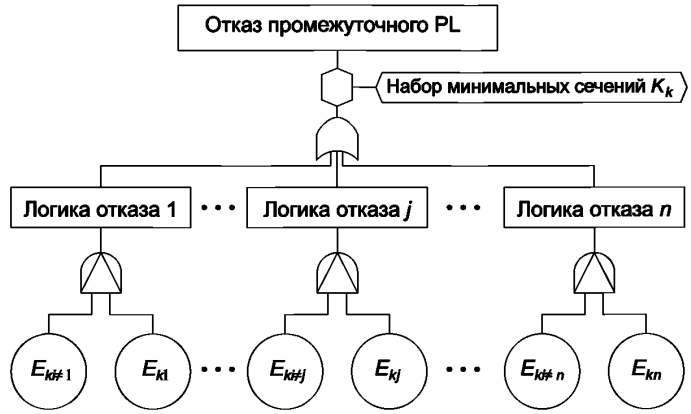


Рисунок 12 — Отказ промежуточного уровня защиты, не зависящий от последовательности событий

Для Q_k^* и w_k^* справедливы следующие формулы [10], [11]:

$$Q_k^* = \prod_{i=1}^{n} \left\{ \lambda_{ki} / \left(\lambda_{ki} + \mu_{ki} \right) \right\}, \tag{22}$$

$$w_k^* = \sum_{j=1}^{n} \left[\prod_{i=1, i\neq j}^{n} \left\{ \lambda_{ki} / \left(\lambda_{ki} + \mu_{ki} \right) \right\} \right] \lambda_{kjk} \mu_{kj} / \left(\lambda_{kj} + \mu_{kj} \right). \tag{23}$$

Следовательно, верхний предел вероятности состояния запроса Q_{UL}^* и верхний предел частоты запроса w_{UL}^* определяют при условии, что $Q_k^* << 1$ (k = 1, 2,..., m) [10], [11]:

Q_{UL}^* — верхний предел приближенной вероятности того, что следующий уровень защиты или конечный уровень защиты находятся в состоянии запроса в соответствии со всей логикой отказов минимальных сечений K_k (k = 1, 2,...,m) промежуточного уровня защиты, показанного на рисунке 12 в стационарном состоянии;

w_{UL}^* — верхний предел приближенной частоты запроса на следующем уровне защиты или конечном уровне защиты в соответствии со всеми логиками отказов минимальных сечений K_k (k = 1, 2,...,m) промежуточного уровня защиты (см. рисунок 12) в стационарном состоянии.

Для Q_{UL}^* и w_{UL}^* справедливы следующие формулы:

$$Q_{UL}^* = \sum_{k=1}^{m} \prod_{i=1}^{n} \left\{ \lambda_{ki} \left(\lambda_{ki} + \mu_{ki} \right) \right\}, \tag{24}$$

$$w_{UL}^* = \sum_{k=1}^{m} \left[\prod_{j=1}^{n} \left\{ \prod_{i=1, i\neq j}^{n} \lambda_{kil} \left(\lambda_{ki} + \mu_{ki} \right) \right\} \right] \lambda_{kj} \mu_{kj} / \left(\lambda_{kj} + \mu_{kj} \right). \tag{25}$$

Если неравенство $Q_k^* << 1$ для всех k (k = 1, 2,..., m) не выполняется, возможны два варианта: a) и b).

a) Вероятность и частота запроса должны быть определены в соответствии с точной процедурой количественной оценки минимальных сечений, однако это выходит за рамки настоящего стандарта (см., например, [11]).

b) Предположение о том, что главное событие «отказ промежуточного уровня защиты» может быть повторяемым неуместно. Например, если запрос промежуточного уровня защиты является непрерывным, то $Q_k^* << 1$ может не выполняться. В таком случае вариант a) может привести к неблагоприятному результату, и поэтому FEF и FER для заданного начального состояния должны быть применены для определения оценки вероятности и частоты запроса следующего уровня защиты.

Поскольку отказ промежуточного уровня защиты активирует проактивную функцию следующего уровня защиты или конечного уровня защиты (см. рисунок 11), справедливы следующие соотношения для w_{UL}^*, Q_{UL}^* частотой запросов следующего уровня защиты или конечного уровня защиты w_M и вероятности запроса следующего уровня защиты или конечного уровня защиты Q_M в стационарном состоянии:

$$w_M = \lambda_M/\mu_M/(\lambda_M + \mu_M) \approx w^*_{UL},$$

$$Q_M = \lambda_M/(\lambda_M + \mu_M) \approx Q^*_{UL}.$$

Таким образом

$$\lambda_M \approx w^*_{UL}/(1 - Q^*_{UL});$$

$$\lambda_M \approx w^*_{UL}/Q^*_{UL}.$$

9.2.3 Зависимость от последовательности событий

9.2.3.1 Общие положения

Если отказ промежуточного уровня защиты повторяется и зависит от последовательности событий с базовыми элементами, т. е. последовательности базовых элементов S (S = 1, 2,..., h), то логика отказов в последовательности базовых элементов S (S = 1, 2,..., h), приводящая к вершине событий, может быть описана с помощью вентиля «И» типа 1. Эта логика отказа показана на рисунке 13, где выходное событие вентиля «И» типа 1 «отказ промежуточного уровня защиты (в соответствии с логикой отказов в последовательности базовых элементов S (S = 1, 2,..., h) минимальных сечений K_k)» становится истинным, если все входные события E_{kSi} (i = 1, 2,..., n; $E_{kSi} \in$ {1, 2,..., n}) минимальных сечений K_k (k = 1, 2,..., m) в последовательности S становятся истинными, т. е. в порядке слева направо на рисунке, и если истинные состояния не восстанавливаются до того, как входное событие E_{kSn} окончательно становится истинным, при условии, что все базовые элементы не являются истинными в нулевой момент времени. Входное событие E_{kSi} на рисунке 13 определяют следующим образом:

E_{kSi} — базовый элемент i-го порядка (i = 1, 2,..., n) в последовательности S (S = 1, 2,..., h) минимальных сечений K_k (k = 1, 2,..., m) становится истинным.

9.2.3.2 Формулы для стационарного состояния

Вероятность состояния запроса Q_{kS} и частоту запросов w_{kS} в стационарном состоянии определяют следующим образом:

Q_{kS} — вероятность того, что следующий уровень защиты или конечный уровень защиты находятся в состоянии запроса, которое является результатом запроса в соответствии с логикой отказа промежуточного уровня защиты в соответствии с последовательностью S (S = 1, 2,..., h), как показано на рисунке 13, в стационарном состоянии;

w_{kS} — частота запроса, возникающего в соответствии с логикой отказа промежуточного уровня защиты в соответствии с последовательностью S (S = 1, 2,..., h), как показано на рисунке 13, в стационарном состоянии.

Для Q_{kS} и w_{kS} справедливы следующие формулы [12]:

$$Q_{kS} = \prod_{i=1}^{n}\left\{\lambda_{kSi}\mu_{kSi}/\left(\lambda_{kSi} + \mu_{kSi}\right)\right\}/\left\{\prod_{i=1}^{n}\left(\sum_{j=1}^{i}\mu_{kSj}\right)\right\}, \quad (26)$$

$$w_{kS} = \prod_{i=1}^{n}\left\{\lambda_{kSi}\mu_{kSi}/\left(\lambda_{kSi} + \mu_{kSi}\right)\right\}/\left\{\prod_{i=1}^{n-1}\left(\sum_{j=1}^{i}\mu_{kSj}\right)\right\}. \quad (27)$$

Для вероятности состояния запроса Q_k и частоты запроса w_k в любых последовательностях базовых элементов S (S = 1, 2,... и h) минимальных сечений K_k в стационарном состоянии справедливы следующие выражения [12]:

$$Q_k = \sum_{S=1}^{h}\left[\prod_{i=1}^{n}\left\{\lambda_{kSi}\mu_{kSi}/\left(\lambda_{kSi} + \mu_{kSi}\right)\right\}/\left\{\prod_{i=1}^{n}\left(\sum_{j=1}^{i}\mu_{kSj}\right)\right\}\right], \quad (28)$$

$$w_k = \sum_{S=1}^{h}\left[\prod_{i=1}^{n}\left\{\lambda_{kSi}\mu_{kSi}/\left(\lambda_{kSi} + \mu_{kSi}\right)\right\}/\left\{\prod_{i=1}^{n}\left(\sum_{j=1}^{i}\mu_{kSj}\right)\right\}\right]. \quad (29)$$

Аналогично для верхних пределов вероятности состояния запроса Q_{UL} и частоты запроса w_{UL}, по всем минимальным сечениям K_k (k = 1, 2,..., m) при условии, что $Q_k << 1$ (k = 1, 2,..., m) справедливы следующие выражения [12]:

$$Q_{UL} = \sum_{k=1}^{m}\left[\sum_{S=1}^{h}\left[\prod_{i=1}^{n}\left\{\lambda_{kSi}\mu_{kSi} / \left(\lambda_{kSi} + \mu_{kSi}\right)\right\} / \left\{\prod_{i=1}^{n}\left(\sum_{j=1}^{i}\mu_{kSj}\right)\right\}\right]\right] \quad (30)$$

$$w_{UL} = \sum_{k=1}^{m}\left[\sum_{S=1}^{h}\left[\prod_{i=1}^{n}\left\{\lambda_{kSi}\mu_{kSi} / \left(\lambda_{kSi} + \mu_{kSi}\right)\right\} / \left\{\prod_{i=1}^{n-1}\left(\sum_{j=1}^{i}\mu_{kSj}\right)\right\}\right]\right] \quad (31)$$

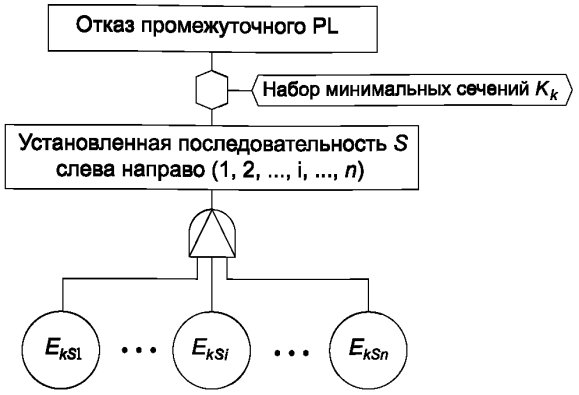


Рисунок 13 — FT для отказа промежуточного уровня защиты в соответствии с логикой последовательных отказов

Аналогичным образом, если отказ промежуточного уровня защиты активирует проактивную функцию следующего уровня защиты или конечного уровня защиты, могут быть полезны следующие соотношения для w_M, Q_M, w_{UL} и Q_{UL}:

$$\lambda_M \approx w_{UL}/(1 - Q_{UL});$$

$$\mu_M \approx w_{UL}/Q_{UL}).$$

9.2.3.3 Приближенные формулы в динамическом состоянии при условии $\lambda_{kSi}/\mu_{kSi} << 1$

Если $\lambda_{kSi}/\mu_{kSi} << 1$ для любых k, S и i, приближенную вероятность состояния запроса $Q_{akS}(t)$ и приближенную частоту запроса $w_{akS}(t)$ в момент времени t определяют при условии, что все базовые элементы не были истинны в момент времени 0:

$Q_{akS}(t)$ — приближенная вероятность того, что следующий уровень защиты или конечный уровень защиты находятся в состоянии запроса в момент времени t, что следует из запроса, возникающего в соответствии с логикой отказов промежуточного уровня защиты в соответствии с последовательностью S (S = 1, 2,…,h), как показано на рисунке 13;

$w_{akS}(t)$ — приближенная частота запросов в момент времени t, возникающих в соответствии с логикой отказов промежуточного уровня защиты в соответствии с последовательностью S (S = 1, 2,…, h), как показано на рисунке 13.

Для $Q_{akS}(t)$ справедлива формула [12]:

$$Q_{akS}(t) = \left(\prod_{i=1}^{n}\lambda_{kSi}\right)\sum_{r=0}^{n}\left[\exp(-a_r t) / \left\{\prod_{j=0, j\neq r}^{n}\left(a_j - a_r\right)\right\}\right], \quad (32)$$

где $a_u \equiv \sum_{i=1}^{u}\mu_{kSi}$ (u = 1, 2, ..., n), a_0 = 0.

Аналогично $w_{akS}(t)$ имеет вид [12]:

$$w_{akS}(t) = \left(\prod_{i=1}^{n}\lambda_{kSi}\right)\sum_{r=0}^{n}\left[\exp(-a_r t) / \left\{\prod_{j=0, j\neq r}^{n-1}\left(a_j - a_r\right)\right\}\right]. \quad (33)$$

Аналогично приближенная вероятность запроса $Q_{ak}(t)$ и приближенная частота запроса $w_{ak}(t)$ для всех базовых элементов последовательности S (S = 1, 2,... и h) минимальных сечений K_k (k = 1, 2, ..., m) имеет вид:

$$Q_{ak}(t) = \sum_{S=1}^{h}\left[\left(\prod_{i=1}^{n}\lambda_{kSi}\right)\sum_{r=0}^{n}\left[\exp(-a_r t)/\left\{\prod_{j=0,j\neq r}^{n}(a_j - a_r)\right\}\right]\right], \quad (34)$$

$$w_{ak}(t) = \sum_{S=1}^{h}\left[\left(\prod_{i=1}^{n}\lambda_{kSi}\right)\sum_{r=0}^{n-1}\left[\exp(-a_r t)/\left\{\prod_{j=0,j\neq r}^{n-1}(a_j - a_r)\right\}\right]\right]. \quad (35)$$

Верхние границы приближенной вероятности состояния запроса, $Q_{aUL}(t)$ и приближенной частоты запроса $w_{aUL}(t)$ по минимальным сечениям K_k (k = 1, 2, ..., m) при условии, что $Q_{ak}(t) << 1$, справедливы для всех минимальных сечений [12]:

$$Q_{aUL}(t) = \sum_{k=1}^{m}\left[\sum_{S=1}^{h}\left[\left(\prod_{i=1}^{n}\lambda_{kSi}\right)\sum_{r=0}^{n}\left[\exp(-a_r t)/\left\{\prod_{j=0,j\neq r}^{n}(a_j - a_r)\right\}\right]\right]\right], \quad (36)$$

$$w_{aUL}(t) = \sum_{k=1}^{m}\left[\sum_{S=1}^{h}\left[\left(\prod_{i=1}^{n}\lambda_{kSi}\right)\sum_{r=0}^{n-1}\left[\exp(-a_r t)/\left\{\prod_{j=0,j\neq r}^{n-1}(a_j - a_r)\right\}\right]\right]\right]. \quad (37)$$

9.2.3.4 Формула в динамическом состоянии для n = 3

Предположим, например, что n = 3 на рисунке 13 и входы в вентиль «И» типа 1: E_{kS1} = 1, E_{kS2} = 2 и E_{kS3} = 3 для последовательности базовых элементов S базовых элементов 1, 2 и 3 минимальных сечений K_k. Тогда частоту запросов $w_{3kS}(t)$ из этого уровня защиты следующего уровня защиты (или конечного уровня защиты) в этой последовательности событий базовых элементов 1, 2 и 3 в момент времени t при условии, что все основные элементы этих минимальных сечений не истинны в момент времени 0, и $\lambda_1 \neq \mu_2$ и $\mu_1 \neq \lambda_2$, можно записать следующим образом [12]:

$$\begin{aligned} w_{3kS}(t) = \left[\prod_{i=1}^{3}\{\lambda_i/(\lambda_i + \mu_i)\}\right][\{\mu_2\mu_3/(\mu_1 + \mu_2)\} - \{\mu_2\mu_3/(\mu_2 - \lambda_1)\}\exp\{-(\lambda_1 + \mu_1)t\} - \\ - \{\lambda_2\mu_3/(\lambda_2 - \mu_1)t\}\exp\{-(\lambda_2 + \mu_2)t\} + \mu_3\{(\lambda_1/(\lambda_1 + \lambda_2)) + (\mu_1/(\mu_1 + \mu_2)) + (\mu_1/(\lambda_2 - \mu_1)) + \\ + (\lambda_1/(\mu_2 - \lambda_1))\}\exp\{-(\mu_1 + \mu_2)t\} + \{\lambda_2\mu_3/(\lambda_1 + \lambda_2)\}\exp\{-(\lambda_1 + \mu_1 + \lambda_2 + \mu_2)t\} + \\ + \{\mu_2\lambda_3(\mu_1 + \mu_2)\}\exp\{-(\lambda_3 + \mu_3)t\} - \{\mu_2\lambda_3/(\mu_2 - \lambda_1)\}\exp\{-(\lambda_1 + \mu_1 + \lambda_3 + \mu_3)t\} - \\ - \{\lambda_2\lambda_3(\lambda_2 - \mu_1)\}\exp\{-\lambda_2 + \mu_2 + \lambda_3 + \mu_3)t\} + \{\lambda_2\lambda_3/(\lambda_1 + \lambda_2)\}\exp\{-(\lambda_1 + \mu_1 + \lambda_2 + \mu_2 + \lambda_3 + \mu_3)t\} + \\ + \lambda_3\{(\lambda_1/(\lambda_1 + \lambda_2)) + (\mu_1/(\mu_1 + \mu_2)) + (\mu_1(\lambda_2 - \mu_1)) + (\lambda_1/(\mu_2 - \lambda_1))\}\exp\{-(\mu_1 + \mu_2 + \lambda_3 + \mu_3)t\}]. \end{aligned} \quad (38)$$

9.3 Конечный уровень защиты в системе с последовательной структурой «1 из 1»

9.3.1 Общие положения

Возможность отказов по общей причине часто оценивают с помощью β. Если β составляет несколько процентов или более, отказы по общей причине часто (но не всегда) доминируют над другими отказами системы с точки зрения анализа риска (см. рисунки А.3; А.4 и В.4). Это приводит к необходимости рассматривать объект как систему с последовательной структурой, поскольку отказы нескольких каналов по общей причине часто могут быть смоделированы как отказы одного канала системы [5]. На рисунках 14—19 представлены FT и модели перехода состояний системы в целом применительно к запросам конечного уровня защиты в системе с последовательной структурой, имеющей только невыявленные отказы. Вначале необходимо сделать следующие пояснения:

а) параметр T на рисунке 15 является экспозицией риска, а π — отношение интенсивности отказов неработающего объекта в состоянии отсутствия запроса, к интенсивности отказов работающего объекта в состоянии запроса. В общем случае $0 < \pi \leq 1$. Если π = 1, интенсивность отказов объекта в рабочем состоянии эквивалентна интенсивности отказов в нерабочем состоянии. Если значение π асимптотически приближается к 0, объект не может отказать в нерабочем состоянии. Однако для простоты

рассуждений в настоящем стандарте далее рассмотрено значение коэффициента, равное 1 (см. [14], [15] для анализа риска);

b) если система в целом находится в состоянии запроса по отношению к функции объекта, необходимо, чтобы объект был в рабочем состоянии по отношению к запрашиваемым функциям, в то время как объект может быть в нерабочем состоянии при отсутствии запроса. Следовательно, необходимо рассмотреть два режима отказов, т. е. объект находится в нерабочем состоянии при наличии запроса, и объект находится в рабочем состоянии при отсутствии запроса (см. 3.1.3, примечание 6);

c) невыявленный отказ обнаруживают только при выполнении контрольной проверки. Контрольная проверка является видом периодического контроля, выполняемого специалистами по техническому обслуживанию и ремонту для обнаружения и восстановления отказавших частей промежуточного уровня защиты и конечного уровня защиты. Контрольную проверку обычно проводят каждый год или один раз в два года, при этом для технического обслуживания и ремонта требуется от нескольких часов до нескольких дней. Время, необходимое для проведения технического обслуживания и ремонта, является незначительным по сравнению с интервалом времени между контрольными проверками, и, следовательно, можно предположить, что неисправные части, выявленные при контрольной проверке, восстанавливают мгновенно и полностью (см. А.1 для примера неполной контрольной проверки);

d) невыявленный отказ не может быть обнаружен в течение интервала времени между проведением контрольных проверок, тогда как состояние запроса может быть выявлено, когда промежуточный уровень защиты или конечный уровень защиты работают нормально в состоянии запроса, конечное состояние также является выявленным, поскольку состояние системы в целом значительно ухудшилось в конечном состоянии (см. 3.1.13, примечание 3). Конечное событие является неповторяемым и восстанавливаемым; интенсивности переходов предполагаются постоянными в 9.3.2—9.4.

9.3.2 Интенсивность конечного события для начального состояния (0, 0) и неповторяемого конечного события

На рисунках 14 и 15 представлена причинно-следственная связь конечного события, обусловленного невыявленным отказом конечного уровня защиты и запросом конечного уровня защиты при условии, что $1/T << \mu_M$ и $\lambda_{UD} << 1/T$. В соответствии с рисунком 15 значения $P_{0,0}$ (1,0), $P_{0,0}$ (0,1) и $P_{0,0}$ (1,1) легко рассчитать (см. примечания в 9.1). Таким образом, FEF в начальном состоянии $\omega_{0,0}$, FER в начальном состоянии $\varphi_{0,0}$ и MTFE в начальном состоянии (0,0), $T_{0,0}$, при условии, что начальное состояние (0,0) выявлено в момент времени $t = 0$, имеют вид [3], [4], [16]

$$\omega_{0,0} = P_{0,0}(1,0)\lambda_M + P_{0,0}(1,0)\lambda_{UD},$$

$$\varphi_{0,0} = \omega_{0,0} / \{1 - P_{0,0}(1,1)\},$$

$$T_{0,0} = 1/\varphi_{0,0},$$

где $P_{0,0}(0,0) = 1/[1 + \{\lambda_M/(\mu_M + \lambda_{UD})\}\{1 + \lambda_{UD}/m)\} + \{\lambda_{UD}/(\lambda_M + \mu_{UD})\}\{1 + (\lambda_M/m)\}]$,

$P_{0,0}(0,1) = \{\lambda_U/(\lambda_M + \mu_{UD})\} P_{0,0}(0,0)$,

$P_{0,0}(0,1) = \{\lambda_M/(\mu_M + \lambda_{UD})\} P_{0,0}(0,0)$,

$P_{0,0}(1,1) = [(\lambda_{UD}/m)\{\lambda_M/(\mu_M + \lambda_{UD})\} + (\lambda_M/m)\{\lambda_{UD}/(\lambda_M + \mu_{UD})\}] P_{0,0}(0,0)$

при условии, что $2/T << \mu_{UD}$ и $\pi = 1$ (см. 9.3).

Если конечное состояние, в котором появляются окончательные последствия риска, возникает в обеих последовательностях событий (0,0) → (1,0) → (1,1) и (0,0) → (0,1) → (1,1), т. е. в соответствии с логикой конечных событий «сначала отказ, потом запрос» (логика № 1) и «сначала запрос, потом отказ» (логика № 2), FER для начального состояния (0,0) $\varphi_{0,0}$ можно записать в следующем виде при условии, что $\lambda_{UD} << (\lambda_M + \mu_{UD})$ и $\lambda_{UD} << \mu_M$ [3], [4], [16]:

$$\varphi_{0,0} \approx [\{(1 - Q_M)\} \lambda_{UD} w_M /\{(1 - Q_M) \mu_{UD} + w_M\}] + Q_M \lambda_{UD}, \quad (39)$$

где Q_M — вероятность состояния запроса, а w_M — частота запроса и выполняются следующие соотношения:

$Q_M = \lambda_M /(\lambda_M + \mu_M)$,

$w_M = \lambda_M \mu_M /(\lambda_M + \mu_M)$.

Если окончательные последствия риска появляются только в соответствии с логикой № 1, то (39) можно переписать в виде

$$\varphi_{0,0} \approx (1 - Q_M)\lambda_{UD} w_M/\{(1 - Q_M)\mu_{UD} + w_M\}.$$

Если окончательные последствия риска появляются только в соответствии с логикой № 2, то (39) можно переписать в виде

$$\varphi_{0,0} \approx Q_M \lambda_{UD}.$$

Если $Q_M << 1$ и $w_M << \mu_{UD}$, то система находится в режиме редких запросов, из (39) может быть получено следующее соотношение:

$$\varphi_{0,0} \approx \lambda_{UD} w_M/\mu_{UD} + Q_M \lambda_{UD} = (\lambda_{UD}/\mu_{UD})w_M + (\lambda_{UD}/\mu_M) w_M \approx (P_a + P_b)w_M. \quad (40)$$

Однако в стандартах серии ГОСТ Р МЭК 61508 (все части) предполагается, что $\varphi_{0,0} \approx P_a w_M$ всегда выполняется, т. е. $P_b w_M \equiv 0$ в режиме редких запросов. Это означает, что окончательные последствия риска появляются только в соответствии с логикой № 1 (см. 7.2.3 и приложение В).

Если $Q_M << 1$ и $\mu_{UD} << w_M$, то система работает в режиме большого количества запросов, следующее соотношение может быть получено из уравнения (39) (см. 7.2.3 и приложение В)

$$\varphi_{0,0} \approx \lambda_{UD} w_M/(\mu_{UD} + w_M) + Q_M \lambda_{UD}. \quad (41)$$

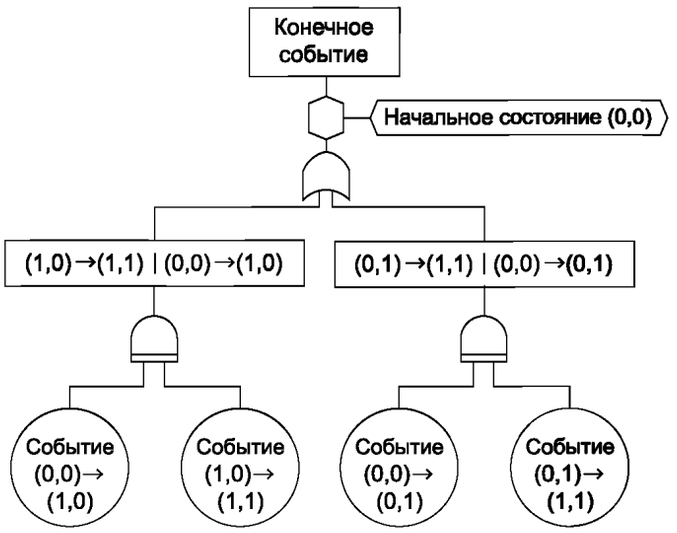


Рисунок 14 — FT неповторяемого конечного события для начального состояния (0,0)

Если окончательные последствия риска появляются только в соответствии с логикой № 1, второй член правой части (41) $Q_M \lambda_{UD}$ удаляют и, следовательно,

$$\varphi_{0,0} \approx \lambda_{UD} w_M/(\mu_{UD} + w_M) \approx \lambda_{UD}.$$

Аналогично, если окончательные последствия риска проявляются только в соответствии с логикой № 2, первый член правой части (41) $\lambda_{UD} w_M/(\mu_{UD} + w_M)$ удаляют и, следовательно,

$$\varphi_{0,0} \approx Q_M \lambda_{UD}.$$

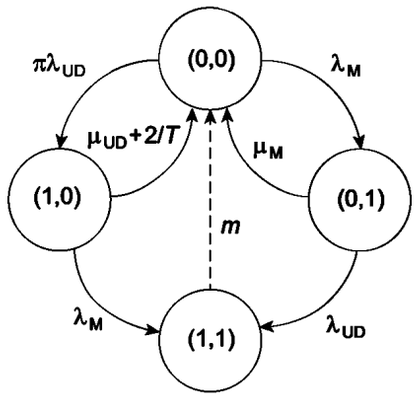


Рисунок 15 — Модель состояний неповторяемого конечного события для начального состояния (0,0)

Если $Q_M \approx 1$ и $\mu_{UD} << w_M$, то система работает непрерывно и из (39) следует

$$\varphi_{0,0} \approx (1 - Q_M)\lambda_{UD} + Q_M \lambda_{UD} = \lambda_{UD}. \quad (42)$$

9.3.3 Интенсивность конечного события для выявленного состояния (x, y)

Если выявлено, что в момент времени t конечный уровень защиты работает нормально, то система находится в предшествующем состоянии (0,1), показанном на рисунках 16 и 17. Из рисунков 16 и 17 видно, как смоделировать и проанализировать причины конечного события при определении оценки FEF ($\omega_{0,1}$), FER ($\varphi_{0,1}$) и MTFE ($T_{0,1}$) для выявленного состояния (0,1) при условии, что предшествующее состояние (0,1) выявлено в момент времени t, $1/T << \mu_M$ и $\lambda_{UD} << 1/T$.

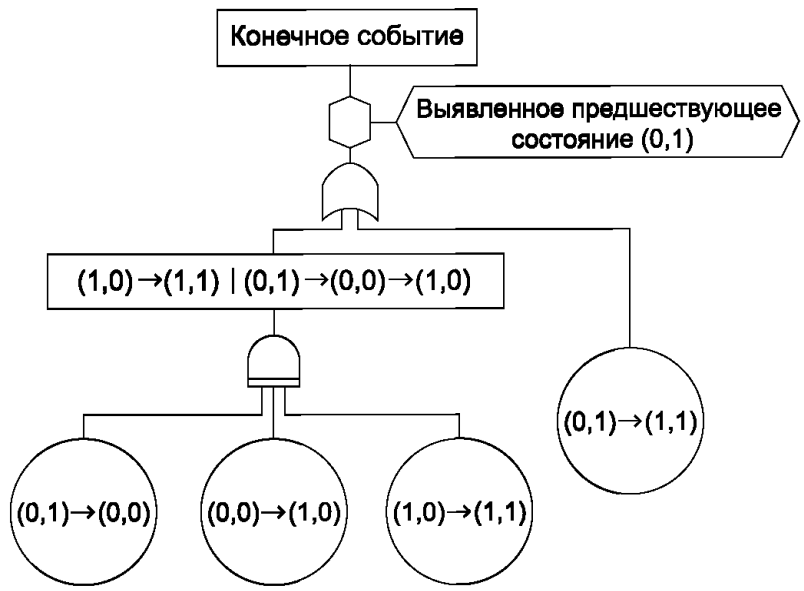


Рисунок 16 — FT для неповторяемого конечного события и выявленного состояния (0,1)

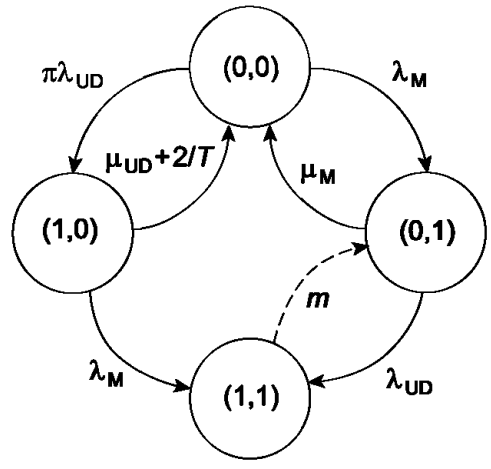


Рисунок 17 — Модель состояний для выявленного состояния (0,1)

На рисунке 17 переход из конечного состояния (1,1) в выявленное состояние (0,1) представляет собой нереальный переход, т. е. виртуальное событие восстановления для вычисления $\omega_{0,1}$ и $\varphi_{0,1}$. Таким образом, $\omega_{0,1}$, $\varphi_{0,1}$ и $T_{0,1}$ можно получить одним и тем же способом в соответствии с 9.3.2 (см. 5.4 и 7.2.3).

9.3.4 Интенсивность конечного события для выявленной группы состояний

9.3.4.1 Общие положения

Если выявлено, что система в целом в момент времени t находится или в предшествующем состоянии (0,1), или в конечном состоянии (1,1), то система в целом находится в состоянии из группы состояний G1, как показано на рисунках 18 и 19. На рисунках показано, как моделировать и анализировать причины конечного события при определении оценок FER и MTFE выявленной группы состояний G1 при условии, что система в целом находится в одном из состояний этой группы с момента времени 0 до момента времени t и $1/T << \mu_M$ и $\lambda_{UD} << 1/T$.

Поскольку нельзя указать, в каком состоянии (0,0) или (1,0) система в целом пребывает в момент времени t, оценку FER для выявленной группы состояний G1 необходимо определять с использованием взвешенного среднего арифметического.

9.3.4.2 Динамическая оценка интенсивности конечных событий для выявленной группы состояний G_i

В общем случае, если вероятность того, что система в целом находится в состоянии (*X, Y*) из выявленной группы состояний G_i , может быть представлена в виде функции времени *t*, эту вероятность состояния (*X, Y*) в момент времени *t* при условии, что система в целом пребывает в состоянии этой группы в момент времени 0 до момента времени *t*, $P_{G_i(X,Y)}(t)$ используют в качестве весового коэффициента в средневзвешенной оценке FER для выявленной группы состояний G_i (см. 9.1).

Для состояний системы (0,0) и (1,0), которые составляют выявленную группу состояний G1(см. рисунок 19), вероятности состояний системы (0,0) и (1,0) в момент времени *t* при условии, что система в целом пребывает в этих состояниях (группы G1) с момента времени 0 до момента времени *t*, $P_{G1(0,0)}(t)$ и $P_{G1(1,0)}(t)$, могут быть представлены как функции времени. Тогда FER для выявленной группы состояний G1 в момент времени *t*, $\varphi_{G1}(t)$, имеет вид

$$\varphi_{G1}(t) = (1/T_{0,0})P_{G1(0,0)}(t)/\{P_{G1(0,0)}(t) + P_{G1(1,0)}(t)\} + (1/T_{1,0})P_{G1(1,0)}(t)/\{P_{G1(0,0)}(t) + P_{G1(1,0)}(t)\},$$

где $1/T_{0,0} = \varphi_{0,0}$, $1/T_{1,0} = \varphi_{1,0}$ и $P_{G1(0,0)}(t) + P_{G1(1,0)}(t) = 1$ и, следовательно, $\varphi_{G1}(t)$ и $T_{G1}(t)$ имеют следующий вид:

$$\varphi_{G1}(t) = \varphi_{0,0}P_{G1(0,0)}(t) + \varphi_{1,0}P_{G1(1,0)}(t),$$

$$T_{G1}(t) = 1/\varphi_{G1}(t).$$

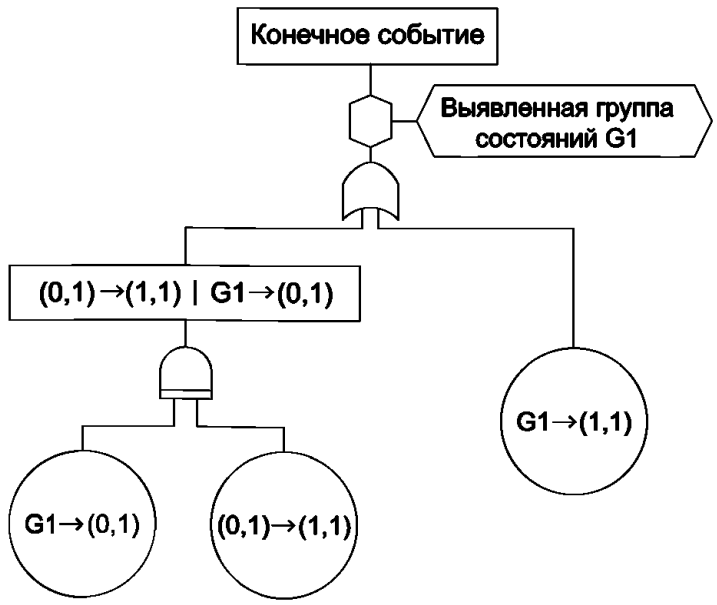


Рисунок 18 — FT неповторяемого конечного события для выявленной группы состояний G1

9.3.4.3 Центрированная по (*x, y*) частота конечного события в группе состояний G_i

Если вероятность состояния системы из группы G_i не может быть описана функцией времени, вероятность состояния системы (*X, Y*) в стационарном состоянии при условии, что система в целом находилась в состоянии (*x, y*) в момент времени 0, а конечное состояние вызывает переход только в состояние (*x, y*), $P_{x,y}$ (*X, Y*) полезна в качестве весового коэффициента (см. 9.1). Здесь состояние (*x, y*) является истинным или виртуальным начальным состоянием из выявленной группы состояний G_i:

a) FER, центрированная по (0,0), для группы состояний G1

Показанные на рисунках 18 и 19 $P_{0,0}(0,0)$ и $P_{0,0}(1,0)$ полезны в качестве весовых коэффициентов при оценке FER для выявленной группы состояний G1. Таким образом FER, центрированная относительно (0,0), для группы состояний G1, $\varphi_{G1}(0,0)$, и MTFE, центрированная относительно (0,0), для группы состояний G1, $T_{G1}(0,0)$ имеют вид:

$$\varphi_{G1(0,0)} = \varphi_{0,0}P_{0,0}(0,0)/\{P_{0,0}(0,0) + P_{0,0}(1,0)\} + \varphi_{1,0}P_{0,0}(1,0)/P_{0,0}(0,0) + P_{0,0}(1,0)\},$$

$$T_{G1(0,0)} = 1/\varphi_{G1(0,0)};$$

b) интенсивность конечного события группы состояний G1, центрированная по (1,0).

Показанные на рисунках 18 и 19 $P_{1,0}$ (0,0) и $P_{1,0}$ (1,0) полезны в качестве весовых коэффициентов при определении оценки FER для группы состояний G. Таким образом, центрированная относительно (1,0) FER для группы состояний G1, $\varphi_{G1(1,0)}$, и центрированная относительно (1,0) MTFE для группы состояний G1, $T_{G1(1,0)}$, имеют вид:

$$\varphi_{G1(1,0)} = \varphi_{0,0}\, P_{1,0}(0,0)/\{P_{1,0}(0,0) + P_{1,0}(1,0)\} + \varphi_{1,0}\, P_{1,0}(1,0)/P_{1,0}(0,0) + P_{1,0}(1,0),$$

$$T_{G1(1,0)} = 1/\varphi_{G1(1,0)}.$$

9.3.4.4 Верхний и нижний пределы интенсивности конечного события для выявленной группы состояний G_i

При определении оценки всех $\varphi_{x,y}$, у которых состояние (x, y) принадлежит выявленной группе состояний G_i, можно определить минимальное и максимальное значения $\varphi_{x,y}$. Минимальное значение $\varphi_{x,y}$ является нижним пределом, а максимальное значение $\varphi_{x,y}$ является верхним пределом FER для выявленной группы состояний G_i. Т. е. величина, обратная к нижнему пределу, и величина, обратная к верхнему пределу, дальше всего и ближе всего расположены к конечному событию (состоянию системы) в выявленной группе состояний соответственно.

Набор FER для выявленной группы состояний G1 представляет собой $\{\varphi_{0,0}, T_{0,0}, \varphi_{1,0}, T_{1,0}\}_{G1}$, легко определить самую дальнюю и самую ближнюю позиции (или состояния системы) от конечного события, а также MTFE для этих значений в выявленной группе состояний.

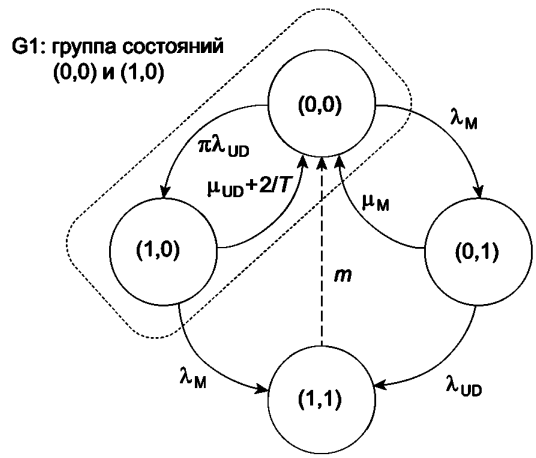


Рисунок 19 — Модель состояний для выявленной группы состояний G1

9.4 Конечный уровень защиты в системе со структурой «1 из 2»

9.4.1 Общие положения

Предположим, что конечный уровень защиты состоит из двух каналов: Ch 1 и Ch 2, в которых происходят независимые (D) и невыявленные (UD) отказы, а также выявленные и невыявленные отказы по общей причине, этот уровень защиты необходим для работы в условиях реальной изменчивости состояний системы безопасности, например автоматическое рулевое управление автомобиля (см. В.2).

Здесь выявленный отказ определяется автоматически с помощью системы самодиагностики, а невыявленный отказ обнаруживают в процессе периодических контрольных проверок при проведении технического обслуживания и ремонта (см. 9.3).

Конечный уровень защиты может быть описан, например, с использованием RBD в виде системы со структурой «1 из 2» и отказами по общей причине, как показано на рисунке 20. На рисунке 20 независимые отказы обоих каналов расположены параллельно, а отказы по общей причине соединены с параллельным блоком последовательно (см. ГОСТ Р 51901.14, [17]).

9.4.2 Независимые отказы элементов системы со структурой «1 из 2»

Структурная схема надежности, состоящая из независимых составных частей, т. е. параллельных блоков (каналов), приведенная на рисунке 20, показана на рисунке 21. Блоки независимых отказов (выявленных и невыявленных) каждого канала соединены параллельно.

Приведенная на рисунке 21 RBD эквивалентна показанной на рисунке 22. Блоки «Выявленные отказы Ch 1 и Ch 2», «Выявленные отказы Ch 1 и невыявленные отказы Ch 2», «Невыявленные отказы Ch 1 и «Выявленные отказы Ch 2» и «Невыявленные отказы Ch 1 и Ch 2» соединены параллельно, а эти параллельные структуры соединены последовательно (см. ГОСТ Р 51901.14, [17]).

Если отказал один из четырех параллельных блоков на рисунке 22, например параллельный блок, состоящий из невыявленных отказов Ch 1 и выявленных отказов Ch 2, и появился запрос к конечному уровню защиты или если конечный уровень защиты находится в состоянии запроса и произошел

отказ одного из четырех параллельных блоков, может произойти отказ конечного уровня защиты (в зависимости от логики отказов). Здесь сделаны предположения, что вероятность того, что два или более параллельных блока отказали одновременно, ничтожно мала по сравнению с вероятностью того, что отказал один из четырех параллельных блоков, и вероятность того, что отказ параллельного блока и отказ по общей причине произойдут одновременно, тоже незначительна.



Рисунок 20 — RBD конечного уровня защиты в виде системы со структурой «1 из 2»

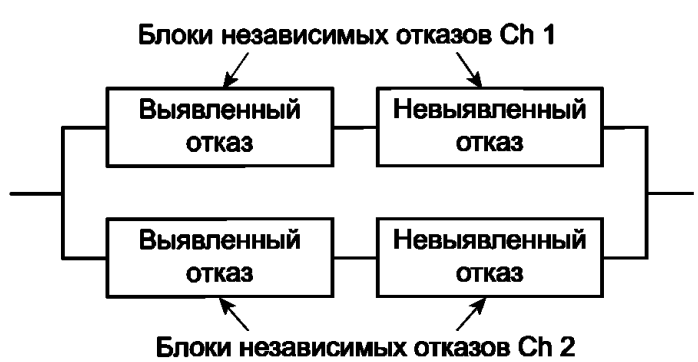


Рисунок 21 — RBD независимых блоков Ch 1 и Ch 2

9.4.3 Дерево неисправностей для независимых выявленных и невыявленных отказов

Причина главного события, например «конечного события, вызванного отказом параллельного блока невыявленных отказов Ch 1 и выявленных отказов Ch 2», разработана как FT, приведенное на рисунке 23, при условии, что все логики последовательных отказов состоят из событий «Невыявленный отказ канала Ch 1», «Выявленный отказ канала Ch 2» и «запрос, вызывающий главное событие».

Главное событие FT является истинным, когда одна из шести перестановок появления трех базовых элементов (невыявленный отказ канала Ch 1, выявленный отказ канала Ch 2 и запрос) является истинной. Три базовых элемента, участвующих в шести перестановках, являются входами в вентиль «И» типа 2 на рисунке 23.

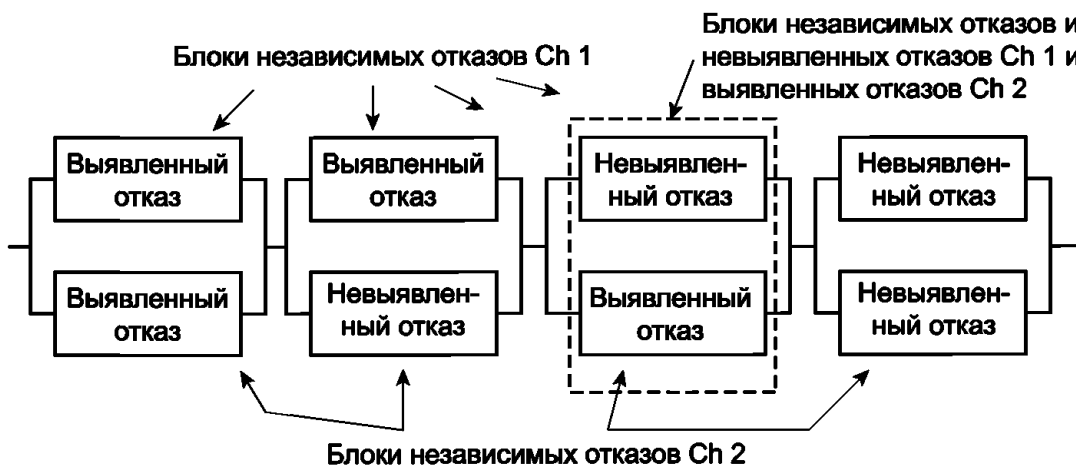


Рисунок 22 — RBD, эквивалентная приведенной на рисунке 21

9.4.4 Интенсивность конечного события для данного начального состояния при независимых отказах

Приближенная оценка FER для заданного начального состояния при независимых отказах каналов Ch 1 и Ch 2 представляет собой общую сумму FER для заданного начального состояния для отказа

каждого из четырех параллельных блоков, показанных на рисунке 22, при условии, что вероятность того, что два или более параллельных блока откажут одновременно, ничтожно мала по сравнению с вероятностью того, что откажет один из параллельных блоков.

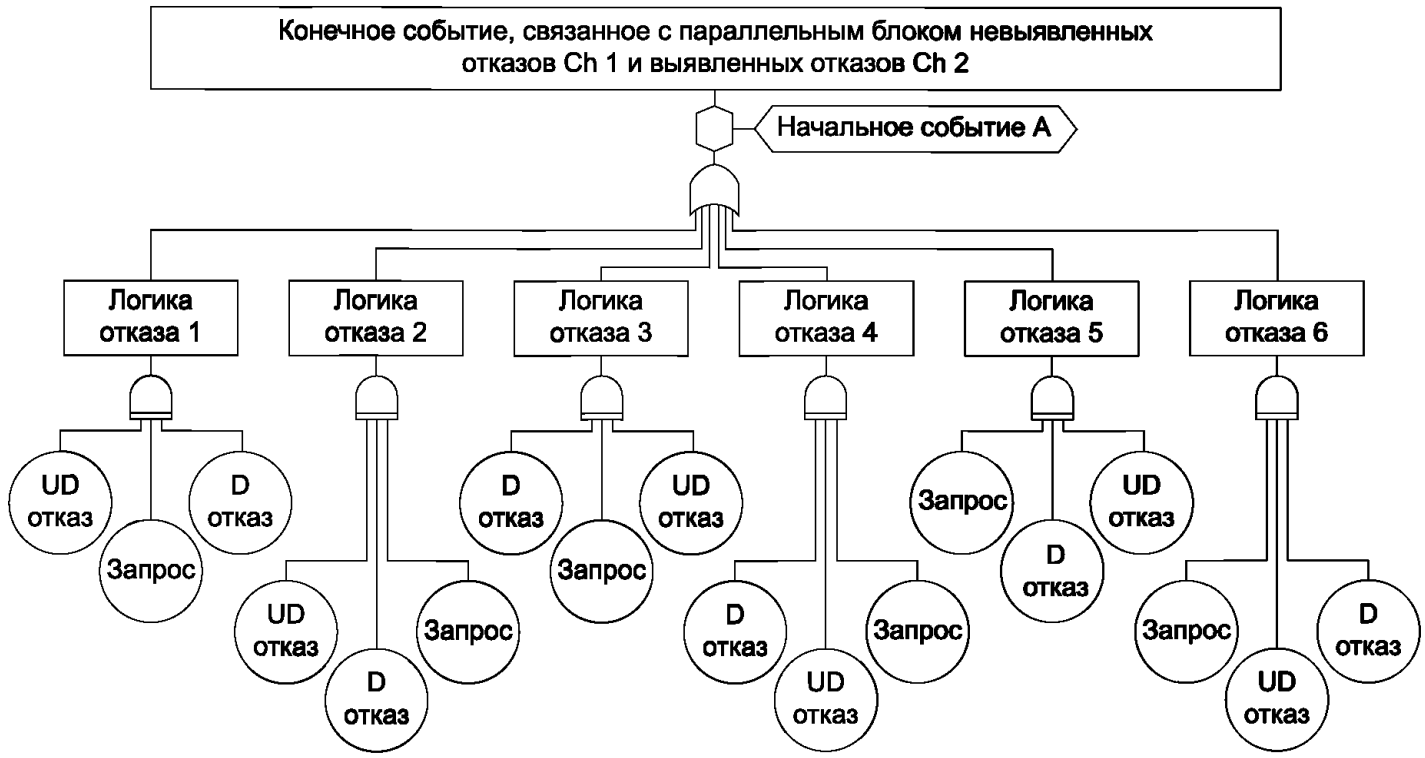
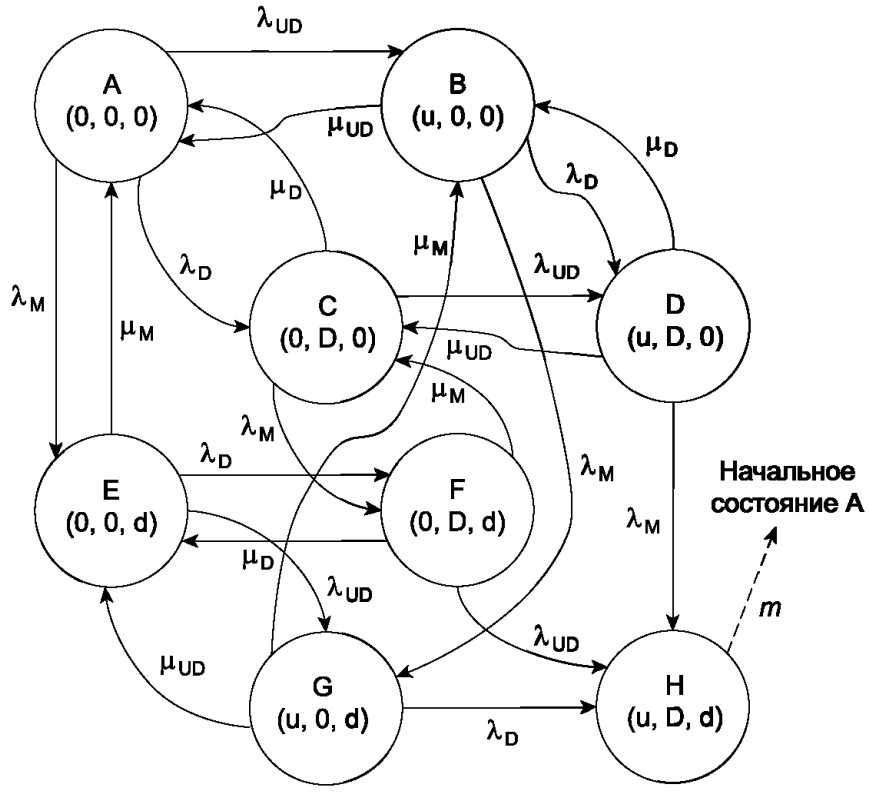


Рисунок 23 — FT для невыявленных отказов канала Ch1, выявленных отказов канала Ch2 и запроса

Оценку FER для начального состояния A, т. е. состояния системы (0,0,0), например из-за отказа параллельного блока невыявленных отказов Ch 1 и выявленных отказов Ch 2, рассчитывают с использованием модели состояний, приведенной на рисунке 24, где интенсивности переходов следующие:

1) Интенсивности невыявленных отказов и ремонтов: λ_{UD} [1/ч] и μ_{UD} [1/ч] соответственно;
2) Интенсивности выявленных отказов и ремонтов: λ_D [1/ч] и μ_{UD} [1/ч] соответственно;
3) Интенсивности запросов и завершения запросов: λ_M [1/ч] и μ_M [1/ч] соответственно;
4) Интенсивность восстановления: m [1/ч].



	Состояние (*x*, *y*, *z*):
x	0: работоспособное состояние Ch 1 u: невыявленный отказ Ch 1
y	0: работоспособное состояние Ch 2 D: выявленный отказ Ch 2
z	0: отсутствие запроса d: запрос

Рисунок 24 — Диаграмма состояний (*x*, *y*, *z*) для невыявленных отказов (UD) канала Ch 1, выявленных отказов (D) канала Ch 2 и запроса

Предположим, что $P_{0,0,0}$ (x, y, z) — вероятность того, что система находится в состоянии (x, y, z), описанном на рисунке 24, в стационарном состоянии при условии, что начальное состояние является состоянием системы (0,0,0). Вероятности того, что система в целом находится в состояниях (u, 0, d), (0, D, d), (u, D, 0) и (u, D, d) $P_{0,0,0}$ (u, 0, d), $P_{0,0,0}$ (0, D, d), $P_{0,0,0}$ (u, D, 0) и $P_{0,0,0}$ (u, D, d), легко рассчитать на основе подхода, описанного в 5.4 и 5.5. Таким образом, FEF для начального состояния (0,0,0), $\omega_{0,0,0}$, FER для начального состояния (0,0,0), $\varphi_{0,0,0}$ и MTFE для начального состояния (0,0,0), $T_{0,0,0}$ при условии, что начальное состояние (0,0,0) выявлено в момент времени $t = 0$, имеют вид [17]:

$$\omega_{0,0,0} = P_{0,0,0}(\text{u, 0, d})\,\lambda_D + P_{0,0,0}(\text{0, D, d})\lambda_{UD} + P_{0,0,0}(\text{u, D, 0})\lambda_M,$$

$$\varphi_{0,0,0} = \omega_{0,0,0}/\{1 - P_{0,0,0}(\text{u, D, d})\},$$

$$T_{0,0,0} = 1/\varphi_{0,0,0}.$$

Выявленное состояние и выявленная группа состояний указаны в 9.4.5 и 9.4.6.

9.4.5 Выявленное состояние каждого блока

9.4.5.1 Общие положения

Предполагается, что вероятность одновременного возникновения двух или более отказов в одном канале и одновременного возникновения независимых отказов и отказов по общей причине в системе со структурой «1 из 2» незначительны (см. 9.4.2).

9.4.5.2 Выявленные отказы каналов Ch 1 и Ch 2

Ниже предполагается, что вся система находится в начальном состоянии (0,0,0) в момент времени $t = 0$ и после этого может перейти в выявленное состояние, одно из состояний выявленной группы состояний или конечное состояние в данный момент времени (см. рисунок 24 для (x, y, z)).

Затем выявленное состояние (D, D, 0), (D, 0, d) и (0, D, d) и конечное состояние (D, D, d) находят на основе сделанного предположения. Любое предшествующее состояние (0,0,0), (D, 0,0), (0, D, 0) или (0,0, d) не выявлено, как единичное состояние системы.

9.4.5.3 Выявленный отказ канала Ch 1 и невыявленный отказ канала Ch 2

Аналогично находят выявленное состояние (D, 0, d) и конечное состояние (D, u, d). Любое предыдущее состояние (0,0,0), (0, u, 0), (D, 0, 0), (D, u, 0), (0,0, d) или (0, u, d) не выявлено, как единичное состояние системы.

9.4.5.4 Невыявленный отказ канала Ch 1 и выявленный отказ канала Ch 2 D

Аналогично находят выявленное состояние (0, D, d) и конечное состояние (u, D, d). Любое предшествующее состояние (0,0,0), (u, 0,0), (0, D, 0), (u, D, 0), (0,0, d) или (u, 0, d) не выявлено, как единичное состояние системы.

9.4.5.5 Невыявленные отказы каналов Ch 1 и Ch 2

Аналогично находят конечное состояние (u, u, d), а любое предшествующее состояние (0,0,0), (u, 0,0), (0, u, 0), (u, u, 0), (0,0, d), (u, 0, d) или (0, u, d) не выявлено, как единичное состояние системы.

9.4.5.6 Отказы по общей причине, выявленные и невыявленные

Выявленные состояния (0, d) и (D, 0), а также конечные состояния (u, d) и (D, d) находят по аналогии с изложенным для независимых отказов. Предыдущие состояния (0,0) или (u, 0) не выявлены, как единичное состояние системы в соответствии с 9.4.5.1). Здесь

(0, d) — конечный уровень защиты не является отказом по общей причине в состоянии запроса;

(D, 0) — конечный уровень защиты является отказом по общей причине в состоянии отсутствия запроса;

(0,0) — конечный уровень защиты не является отказом по общей причине в состоянии отсутствия запроса;

(u, d) — конечный уровень защиты является невыявленным отказом по общей причине в состоянии запроса;

(D, d) — конечный уровень защиты является выявленным отказом по общей причине в состоянии запроса.

9.4.6 Выявленные группы состояний и конечные состояния системы в целом

Для системы в целом, рассмотренной в 9.4.5.2—9.4.5.6, полностью идентифицируют состояния (0, x, y, z), (D, x, y, z) и (u, x, y, z), это означает, что конечный уровень защиты не является отказом по общей причине (выявленным или невыявленным) при условии, что состояния независимых каналов Ch 1, Ch 2 и запроса указаны в состоянии системы (x, y, z) соответственно (см. рисунок 24). А именно x и y принимают значение «0», «D» или «u» для обозначения «работоспособного состояния», «выявленного отказа» или «невыявленного отказа» соответственно, а z равно «0» или «d» для обозначения состояния отсутствия запроса или наличия запроса соответственно.

Затем для системы в целом суммируют выявленные состояния, выявленные группы состояний G1, G2, G3 и G4, конечные состояния и рабочие состояния системы (см. 9.4.5):

1) выявленными состояниями являются (D, 0,0,0), (0, D, D, 0), (0, D, 0, d) и (0,0, D, d);

2) группа G1 включает в себя состояния системы (0,0,0,0), (u, 0,0,0), (0, u, 0,0), (0,0, u, 0) и (0, и, и, 0);

3) группа G2 включает в себя состояния системы (0,0,0, d), (0, u, 0, d) и (0,0, u, d);

4) группа G3 включает в себя состояния системы (0, D, 0,0) и (0, D, u, 0);

5) группа G4 включает в себя состояния системы (0,0, D, 0) и (0, u, D, 0);

6) конечными состояниями системы являются (u, 0,0, d), (D, 0,0, d), (0, u, u, d), (0, u, D, d), (0, D, u, d) и (0, D, D, d);

7) рабочими состояниями системы являются: (0,0,0, d), (0, D, 0, d), (0,0, D, d), (0, u, 0, d) и (0,0 , и, г).

FER для выявленного состояния и FER для выявленной группы состояний могут быть проанализированы и получены оценки для этих выявленных состояний (D, 0,0,0), (0, D, D, 0), (0, D, 0, d) и (0, 0, D, d) и выявленных групп состояний G1, G2, G3 и G4 в соответствии с процедурой, приведенной в 9.3.2—9.4.4.

9.5 Отказы по общей причине уровней защиты и сложность системы

Возможность возникновения отказа по общей причине является фактором сложности для системы в целом. Необходимо рассмотреть отказы по общей причине не только нескольких каналов проактивных функций защиты одного уровня защиты, но также и нескольких уровней защиты, которые могут включать первоначальные источники запросов. Система в целом с отказами по общей причине нескольких уровней защиты является более сложной, чем система без таких отказов.

При наличии нескольких уровней защиты возможны два типа отказов по общей причине, т. е. прогнозируемый и непрогнозируемый. Риск, связанный с прогнозируемым или известным отказом по общей причине, подразделяют на риск контролируемого или неконтролируемого события, и, следовательно, такой риск должен быть включен в область применения настоящего стандарта (см. таблицу 1).

Риск, соответствующий непрогнозируемому или неизвестному отказу по общей причине, классифицируют как мета-риск, и поэтому он не рассмотрен в настоящем стандарте (см. таблицу 1). Система в целом, в которой может произойти неизвестный отказ по общей причине нескольких уровней защиты, является более сложной, чем система без таких отказов.

Прогнозируемый отказ по общей причине нескольких уровней защиты можно обрабатывать по аналогии с 9,3 и 9,4.

9.6 Выводы и замечания

Полный комплексный подход, включающий оценку FER для данного начального состояния, FER для заданного выявленного состояния и FER для выявленной группы состояний, приведенный в настоящем стандарте, является достаточно мощным методом количественного и вероятностного анализа риска сложных систем (в том числе электротехнических объектов), как показано в разделе 9.

Предполагается, что уровни защиты включены в системы произвольной структуры (см. 9.2), однако конечные уровни защиты включены в системы со структурой «1 из 1» или «1 из 2» (см. пример в 9.3 и 9.4). Конечный уровень защиты может иметь более сложную структуру с использованием резервирования. Тогда деревья отказов и модели состояний, описанные в примерах отказов уровней защиты, могут быть изменены для более реалистичного моделирования такой ситуации.

Разработка реалистичных моделей для анализа риска все еще относится больше к искусству, чем к строгим научным методикам. Насколько разработанная модель подходит для анализа риска, зависит от опыта аналитика. Статьи, приведенные в библиографии, могут помочь в повышении квалификации при анализе риска.

Приложение А
(справочное)

Риск, обусловленный отказом, выявленным только при запросе

А.1 Запрос, обнаружение и логика отказов

Если отказ объекта не обнаружен при диагностике или контрольной проверке, он может быть выявлен другими методами, в том числе на этапе такого промежуточного события, как запрос, который активирует функции, приводящие объект в рабочее состояние (см. 9.3). Однако, если отказ не выявлен такими методами, включая капитальный ремонт, он останется в объекте на весь срок службы объекта. В этом приложении приведен пример анализа риска конечного уровня защиты с отказами, выявленными только по запросу (далее — DU-отказами).

Рассмотрим DU-отказы в конечном уровне защиты, которые могут быть обнаружены только по запросу конечного уровня защиты. Предположим, что время до запроса и его завершения подчиняется экспоненциальному распределению с интенсивностью запросов λ_M [1/ч] и интенсивностью завершения запроса μ_M [1/ч], соответственно. Предположим, что конечный уровень защиты входит в структуру системы «1 из 2» с независимыми отказами блоков Ch 1 и Ch 2, а также блока отказов по общей причине, как показано на рисунке А.1 (см. 9.4). Предположим также, что, если запрос произошел в состоянии DU-отказа или если конечный уровень защиты отказывает в состоянии запроса, возникает неповторяемое конечное событие. Это конечное событие анализируют с использованием дерева неисправностей, как показано на рисунке А.2 [18].

Высшее событие дерева неисправностей возникает, если происходят невыявленные отказы (DU-отказы) по общей причине и запрос (т. е. логика отказа 1) или если возникают независимые DU-отказы по запросу (логика отказа 2). Отказы в соответствии с логикой 1 и логикой 2 получили дальнейшее развитие в виде логики последовательности отказов 1-1 и логики последовательности отказов 1-2, а также логики последовательности отказов с 2-1 до 2-6 соответственно. Их можно уточнить с помощью FTA, где такие логики отказов могут привести или не привести к конечному состоянию, в котором появляются конечные последствия риска.

a) Логика 1-1: DU-отказы по общей причине происходят в состоянии запроса.

Логика 1-2: Запрос возникает в случае DU-отказов по общей причине.Высшее событие происходит, если логика последовательности отказов 1-1 либо логика последовательности отказов 1-2.

b) Логика 2-1: сначала появляется запрос, затем происходит независимый DU-отказ канала Ch 1, независимый DU-отказ канала Ch 2 происходит по запросу в состоянии независимого DU-отказа канала Ch 1.

Логика 2-2: сначала появляется запрос, затем происходит независимый DU-отказ канала Ch 2, а независимый DU-отказ канала Ch 1 происходит по запросу в состоянии независимого DU-отказа канала Ch 2.

Другие логики последовательности отказов с 2-3 до 2-6 анализируют таким же способом, высшее событие происходит, если одна из шести логик последовательности отказов 2-1 через 2-6 становится истинной.

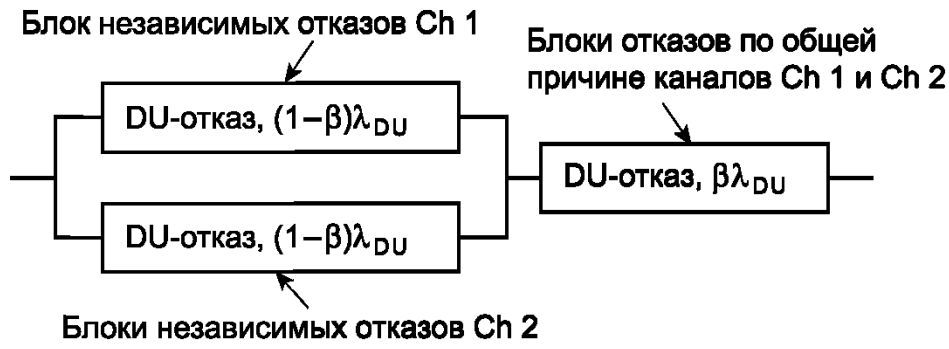


Рисунок А.1 — Блок-схема надежности с независимыми отказами и отказами по общей причине

Каналам соответствуют идентичные интенсивности DU-отказов, которые выявляют только при запросе, и идентичные интенсивности восстановлений. Времена до DU-отказа и восстановления подчиняются экспоненциальному распределению с постоянной интенсивностью DU-отказов λ_{DU} [1/ч] и интенсивностью восстановлений μ_R [1/ч]. Интенсивность отказов независимых DU-отказов каналов составляет $(1 - \beta)\ \lambda_{DU}$, а интенсивность DU-отказов по общей причине составляет $\beta\ \lambda_{DU}$ [1/ч]. Здесь β — бета-фактор каналов при условии $0 \le \beta < 1$, $0 < \lambda_M$, $0 < \mu_M$, $0 < \lambda_{DU}$ и $0 < \mu_R$.

Модель состояний, приведенная на рисунке А.3, разработана на основе анализа RBD (см. ГОСТ Р 51901.14) и FTA (см. таблицу 4) при условии, что вероятность одновременного появления независимого отказа и отказа по общей причине в течение рассматриваемого периода времени незначительна по сравнению с вероятностью возникновения только отказа по общей причине в течение того периода времени. Модель включает восемь логик последовательности отказов и двенадцать состояний системы от A до H, обозначенных в виде (*X, Y, Z*) на рисунке А.3.

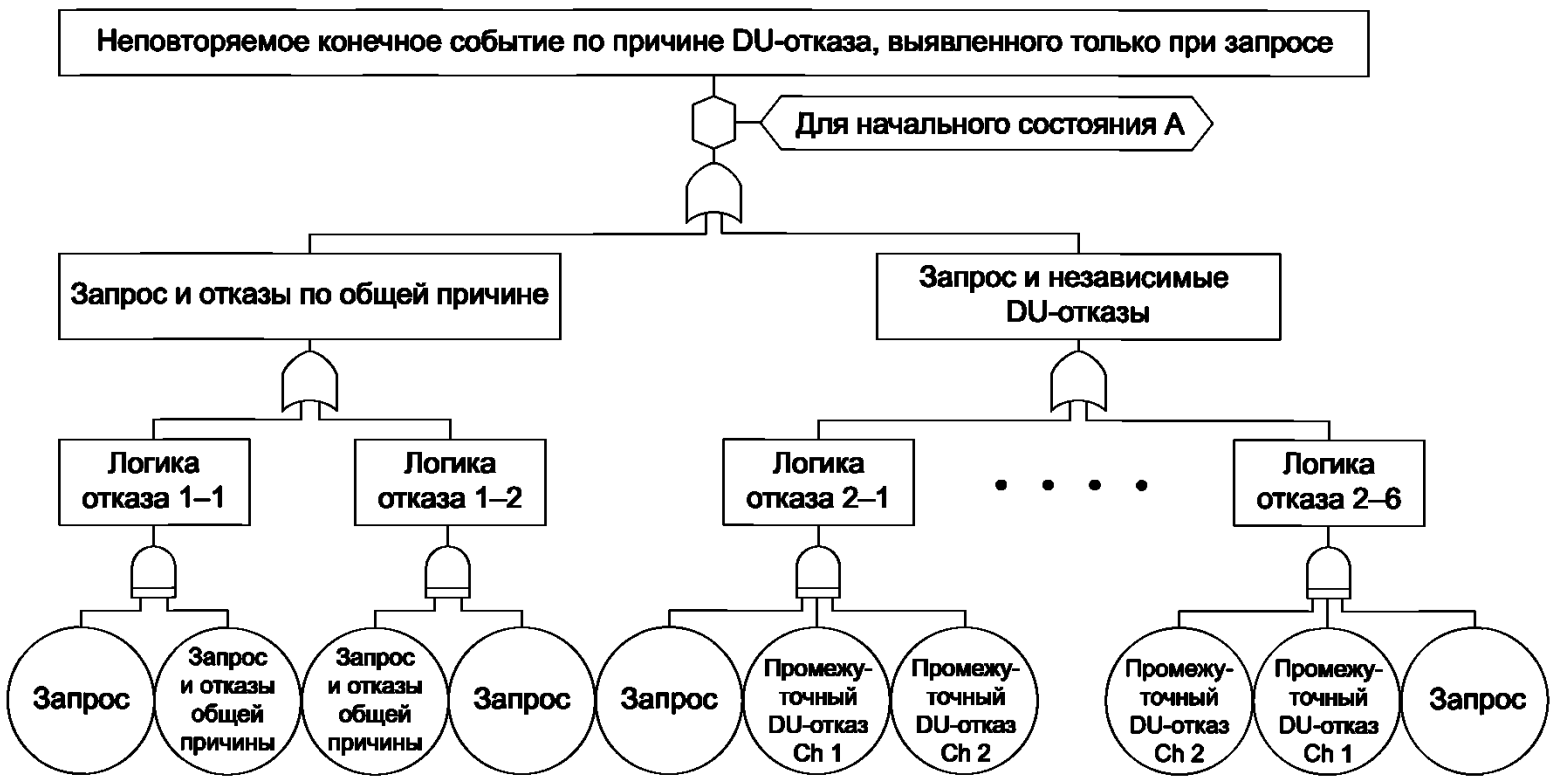
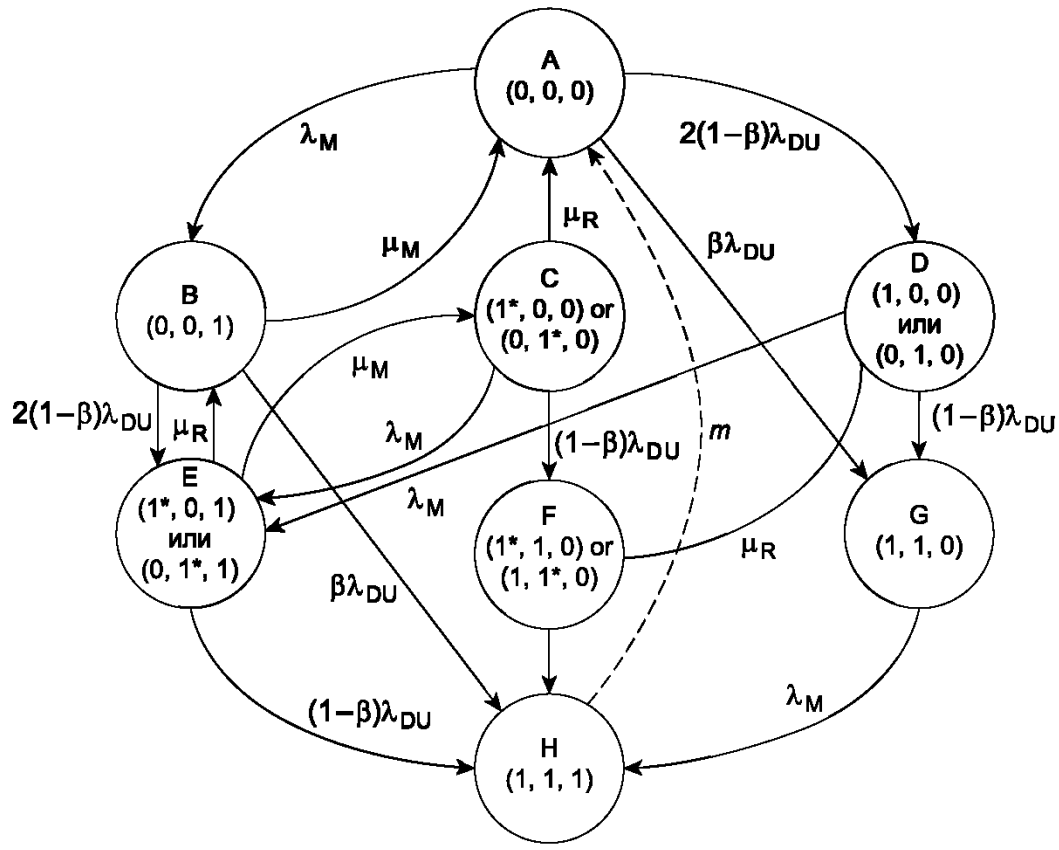


Рисунок А.2 — Дерево отказов неповторяемого конечного события по причине DU-отказов



Состояние (X, Y, Z):	
X	0: канал Ch 1 – находится в работоспособном состоянии
	1: в канале Ch 1 произошел DU-отказ, который не восстанавливается
	1 *: в канале Ch 1 произошел DU-отказ, который восстанавливается
Y	0: канал Ch 2 находится в работоспособном состоянии
	1: в канале Ch 2 произошел DU-отказ, который не восстанавливается
	1 *: в канале Ch 2 произошел DU-отказ, который восстанавливается
Z	0: система в целом находится в состоянии отсутствия запроса
	1: система в целом находится в состоянии запроса

Рисунок А.3 — Модель состояний (X, Y, Z) для неповторяемого конечного события, вызванного DU-отказами

А.2 Интенсивность конечного события для заданного начального состояния

На рисунке А.3 состояние системы (0,0,0) является начальным состоянием А, а состояние системы (1,1,1) является неповторяемым конечным состоянием Н. Здесь P_K — вероятность того, что система в целом находится в состоянии K (B, E, F, G или H) в стационарном состоянии.

В соответствии с рисунком А.3 FEF для начального состояния А, ω_C [1/h] с вероятностями состояний системы и интенсивностями событий можно представить следующим образом [18]:

$$\omega_C = \beta\lambda_{DU}P_B + (1-\beta)\lambda_{DU}P_E + \lambda_M P_F + \lambda_M P_G (= mP_н). \quad (А.1)$$

В соответствии с (А.1) ω_C можно записать

$$\omega_C = X_0/(1 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_0/m), \quad (А.2)$$

где $X_0 = \beta\lambda_{DU}X_3 + (1-\beta)\lambda_{DU}X_1 + \lambda_M(X_2 + X_6)$,

$X_1 = \{\mu_R + \lambda_M + (1-\beta)\lambda_{DU}\}/\mu_M$,

$X_2 = (1-\beta)\lambda_{DU}/(\lambda_M + \mu_R)$,

$X_3 = \{2(1-\beta)\lambda_{DU}\mu_R X_1 - \lambda_M\mu_R X_2\}/2(1-\beta)\lambda_{DU}[\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \{(1-\beta)\lambda_{DU} + \lambda_M\}] + [X_1\{\mu_R + \mu_M + (1-\beta)\lambda_{DU}\} - \lambda_M]\{\lambda_M + (1-\beta)\lambda_{DU}\}/2(1-\beta)\lambda_{DU}[\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \{((1-\beta)\lambda_{DU} + \lambda_M\}]$,

$X_4 = [X_1\{\mu_R + \mu_M + (1-\beta)\lambda_{DU}\} - \lambda_M]\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\}]/[\lambda_M\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \lambda_M\{(1-\beta)\lambda_{DU} + \lambda_M\}] + \{-2(1-\beta)\lambda_{DU}\mu_R X_1 + \lambda_M\mu_R X_2\}/\{\lambda_M 2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \lambda_M\{(1-\beta)\lambda_{DU} + \lambda_M\}]$,

$X_5 = \{\mu_M X_3 + \mu_R + \beta\lambda_{DU}X_3 + (1-\beta)\lambda_{DU}X_1 + \lambda_M X_2 + (1-\beta)\lambda_{DU}X_4\}/2(1-\beta)\lambda_{DU} + \lambda_M\}$,

$X_6 = (1-\beta)\lambda_{DU}X_4 + \beta\lambda_{DU}X_5\}/\lambda_M$.

Таким образом, для FER для начального состояния А, r [1/h], справедлива формула

$$r = \omega_C/(1-P_H) = \lim_{m\to\infty} X_0/(1 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_0/m) =$$

$$= \{(1-\beta)\lambda_{DU}X_1 + \beta\lambda_{DU}X_3 + \lambda_M(X_2 + X_6)\}/(1 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6). \quad (А.3)$$

А.3 Сопоставление нового и традиционного анализа

На рисунке А.4 показана взаимосвязь между переменной интенсивности запроса λ_M и FER для начального состояния А, r, в виде функции от λ_M, т. е. $r(\lambda_M)$, когда $\lambda_{DU} = 10^{-6}$ [1/ч], $\mu_R = 10^{-1}$ [1/ч] и $\mu_M = 10$ [1/ч], а β принимает значение 10 %, 1 % и 0 % соответственно.

На рисунке А.4 функции, изображенные пунктирными линиями, рассчитаны по формулам, приведенным в А.2, а функции, изображенные прямыми линиями, рассчитаны на основе традиционного анализа, как показано ниже.

В ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-5 и ГОСТ Р МЭК 61508-6 HER, $\overline{\omega}$ [1/h], является целевым показателем конечного события (см. 3.1.25, примечание 2 и В.1). Таким образом, FER для заданного начального состояния относится к HER в указанных стандартах серии ГОСТ Р МЭК 61508. HER, $\overline{\omega}$, может быть записана с использованием PFD_{avg}, P_a и интенсивности запросов λ_M [1/ч] для режима работы с редкими запросами (см. ГОСТ Р МЭК 61508-5). В соответствии с ГОСТ Р МЭК 61508-6—2012, пункт В.3.2.5, HER объекта, связанного с безопасностью, со структурой «1 из 2» и DU-отказами, приведенной на рисунке А.1, можно записать в виде (см. ГОСТ Р МЭК 61508-6):

$$\overline{\omega} = \lambda_M P_a, \quad (А.4)$$

где $P_a = 2(1 — \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta\lambda_{DU}(T_2/2 + 1/\mu_R)$.

$t_{CE} = (T_2/2 + 1/\mu_R)$;

$t_{GE} = (T_2/3 + 1/\mu_R)$;

$T_2 = 1/\lambda_M$[ч] (среднее время до запроса);

$1/\mu_R$ MRT [ч] (среднее время восстановления).

О подходе ГОСТ Р МЭК 61508-6 можно заметить следующее:

а) во-первых, ГОСТ Р МЭК 61508-6 применим для режима работы с редкими запросами и $\exp\{-\lambda_{DU}T_2\} \approx 1 - \lambda_{DU}T_2$ является ее первым приближением HER. Поэтому интенсивность запросов должна соответствовать обоим условиям: режим работы является режимом работы с редкими запросами, т. е. $\lambda_M \le 10^{-4}$ [1/ч] и приближение первого порядка имеет вид $\lambda_{DU}T_2 << 1$ (т. е. $\lambda_{DU} << \lambda_M$);

b) во-вторых, если значение λ_{DU} составляет, например, 10^{-6} [1/ч], значение λ_M должно удовлетворять неравенству $10^{-6} << \lambda_M \le 10^{-4}$ [1/ч], т. е. иметь значение 10^{-5} и 10^{-4} [1/ч]. Таким образом, оказывается, что формула ГОСТ Р МЭК 61508-6 может быть применена для очень ограниченного диапазона значений интенсивности запросов (см. рисунок А.4).

С другой стороны анализ, приведенный в настоящем стандарте, может быть применен ко всему диапазону значений интенсивности запросов, как показано на рисунке А.4.

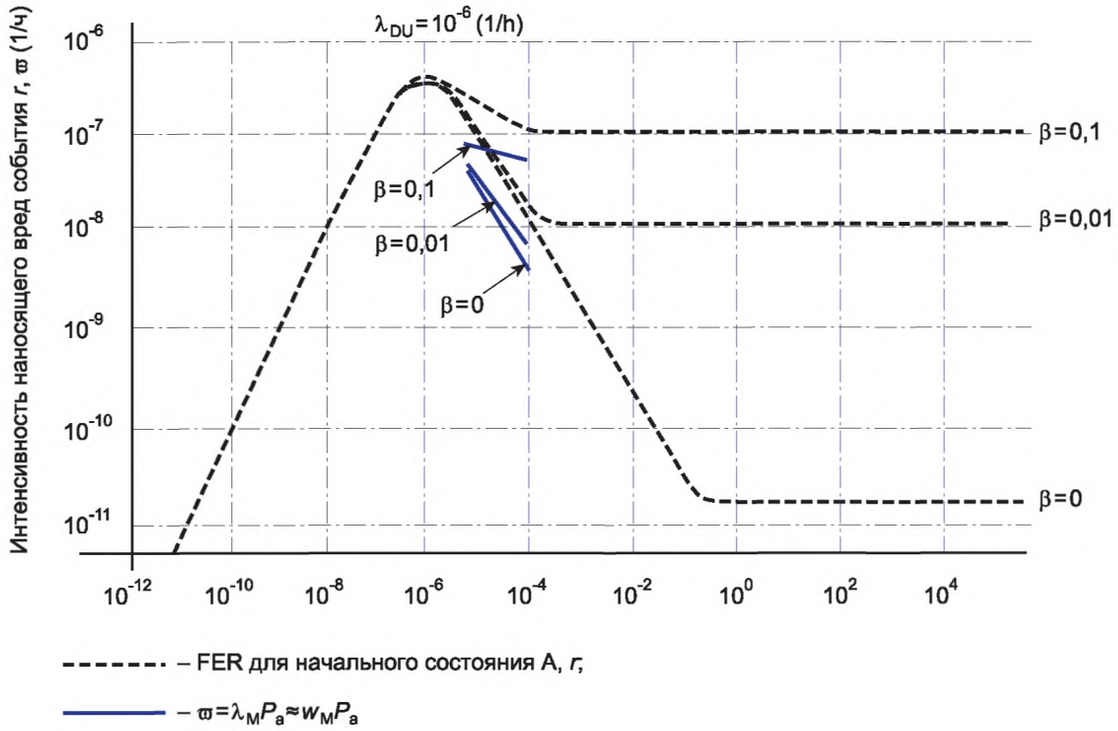


Рисунок А.4 — Сопоставление $r(\lambda_M)$ и $\overline{\omega}$

Анализ изложенного позволяет сделать следующие выводы [18]:

a) если интенсивность запросов становится достаточно низкой, то HER приближается к интенсивности запросов, т. е. $r(\lambda_M) \approx \lambda_M$;

b) если интенсивность запросов достаточно высока, то справедлива формула $r(\lambda_M) \approx 2\{(1-\beta)\lambda_{DU}\}\,2/\{(1-\beta)\lambda_{DU} + \mu_R\} + \beta\lambda_{DU}$, и это означает, что $r(\lambda_M) \approx 2\{(1-\beta)\lambda_{DU}\}2/\mu_R + \beta\lambda_{DU}$, если $\lambda_{DU} << \mu_R$ или $r(\lambda_M) \approx (2\text{-}\beta)\lambda_{DU}$ и $\mu_R << \lambda_{DU}$;

c) обычно считается, если при определении фактора β, как показателя наличия отказов по общей причине для системы с несколькими каналами, оценка составляет несколько процентов или более, то отказы по общей причине доминируют над отказами системы (т. е. HER) (см. 9.3 и В.4). Однако это не всегда так. Хотя отказы по общей причине всегда доминируют над HER в области высоких значений интенсивности запросов (т. е. когда интенсивность запросов более 10^{-2} [1/ч]), HER почти не подвержена влиянию β в области низких значений интенсивности запросов (т. е. когда интенсивность запросов менее 10^{-6} [1/ч]), как показано на рисунке А.4;

d) если допустимая HER для риска установлена равной $2 \cdot 10^{-7}$ [1/ч], то допустимая HER не может быть удовлетворена при интенсивности запросов от $2 \cdot 10^{-7}$ [1/ч] до $2 \cdot 10^{-5}$ [1/ч], а также от $2 \cdot 10^{-7}$ [1/ч] до $7 \cdot 10^{-6}$ [1/ч] для объекта, у которого β принимает значения от 0,1 до 0,01 соответственно;

e) оказывается, что $\overline{\omega}(\lambda_M) \approx (1/2)\,(1/3)\,r(\lambda_M)$ выполняется для значений λ_M от 10^{-5} до 10^{-4} [1/ч]. Рекомендуется удалять коэффициенты (1/2) и (1/3) перед T_2 в формулах, приведенных в ГОСТ Р МЭК 61508-6: 2012, пункт В.3.2.5.

А.4 Дальнейшие исследования

Экспозиция риска T предполагается бесконечной в приведенном выше анализе, соответствующем предположениям, используемым при определении оценки PFD_G и $\overline{\omega}$ в ГОСТ Р МЭК 61508-6.

Однако, если экспозиция риска существенно влияет на HER, диаграмма состояний на рисунке А.3 может быть изменена для более реалистичного представления ситуации. Если, например, $0 \le \beta < 1$, $\lambda_{DU} << 1/T$, $1/T << \mu_R$ и $1/T << \mu_M$, необходимо вставить в диаграмму переходы D → A и G → A с интенсивностью перехода, например, $2/T$.

Таким образом, FER для начального состояния A может быть определена более реалистично на основе модифицированной диаграммы.

А.5 Выводы и замечания

Если отказ объекта обнаружен в результате диагностики или контрольной проверки и быстро восстановлен, влияние на HER запросов (по которым отказ выявлен и восстановлен) может быть незначительным по сравнению с влиянием диагностики на восстановление, выполняемое по результатам диагностики или контрольной проверки, особенно при низкой интенсивности запросов. В этом случае HER как функция интенсивности запросов λ_M, $r(\lambda_M)$, является непрерывной и монотонно возрастающей по переменной λ_M (см. рисунок В.1).

Тип системы выбора определяет выходы независимых каналов для генерирования нормального выхода системы в целом. Если выходы независимых каналов генерируют запросы, могут быть ситуации, когда влиянием запроса на HER вряд ли можно пренебречь в системе в целом [7]—[9].

a) Естественно предположить, что различные виды отказов, таких как D, UD и DU, обычно характерны для сложных объектов. Таким образом, функция HER, $r(\lambda_M)$, может иметь точку (точки) перегиба, т. е. $r(\lambda_M)$ уже не будет монотонно возрастающей по переменной λ_M для системы в целом (см. В.4 и В.5). Это означает, что HER в области промежуточной интенсивности запросов может быть выше, чем в области с более высокой и/или более низкой интенсивностями запросов (см. рисунок А.4).

b) Анализ сложности системы в целом должен включать в себя анализ сложности функции HER, $r(\lambda_M)$. А именно с точки зрения анализа риска система в целом, у которой $r(\lambda_M)$ не является монотонно возрастающей функцией, является более сложной по сравнению с системой, у которой $r(\lambda_M)$ монотонно возрастает по переменной λ_M (см. раздел 6, 9.1, 9.2, 9.5 и В.3).

Таким образом, в приложении А показано, что подход, представленный в настоящем стандарте, может быть применен к сложным системам, у которых функция HER не обязательно монотонно возрастает и не является монотонно возрастающей по переменной λ_M.

Приложение В
(справочное)

Применение в области функциональной безопасности

В.1 Целевые показатели в области функциональной безопасности, основанные на риске

Большая часть методов количественного анализа риска возникла в области анализа безопасности системы и разработана путем объединения методов в области безопасности и безотказности (или надежности) систем [11], [19].

Стандарты безопасности на основе риска серии ГОСТ Р МЭК 61508 широко применяют в различных сферах, таких как железнодорожный транспорт, машиностроение, медицинское электротехническое оборудование, автомобильная и робототехническая промышленность. В серии стандартов ГОСТ Р МЭК 61508 на основе риска установлена количественная мера эффективности объектов, связанных с безопасностью, называемая полной безопасностью. Целевыми показателями полной безопасности являются:

- средняя вероятность отказов по запросу (PFDavg), P_a, для объекта, связанного с безопасностью, в режиме работы с редкими запросами;
- средняя частота опасных отказов в час (PFH) λ [1/ч], для объектов, связанных с безопасностью, в режиме большого количества запросов или непрерывной работы.

Эти целевые показатели устанавливают эффективность объектов, связанных с безопасностью, которые называются связанными с безопасностью системами электрическими, электронными, программируемыми электронными (далее — системами E/E/PE) относительно контроля и/или снижения риска, связанного с безопасностью до допустимого или приемлемого уровня (см. 3.1.1, примечание 3, 3.1.32 и 3.1.33).

Одну из сторон риска, связанного с безопасностью, а именно вероятность нанесения вреда, характеризует HER, φ [1/ч], и это количественный целевой показатель риска, связанного с безопасностью, для контроля и/или сокращения риска путем применения системы E/E/PE, связанной с безопасностью в соответствии с ГОСТ Р МЭК 61508 (все части) (см. 3.1.1, примечание 2 и 3.1.25, примечание 2). Соотношения между PFDavg (т. е. P_a), PFH (т. е. λ) и φ описаны в ГОСТ Р МЭК 61508-6:

- $\varphi \approx P_a\lambda_M \approx P_a w_M$ для объекта, работающего в режиме с редкими запросами;
- $\varphi \approx \lambda$ для объекта, работающего в режиме с большим количеством запросов или непрерывной работы.

Здесь λ_M и w_M — интенсивность запросов и частота запросов, соответственно (см. обозначения в 9.1).

На самой ранней стадии разработки приведенных методов HER был рассчитан с использованием формулы $\varphi \approx P_a\lambda_M \approx P_a w_M$. А целевым показателем отказов системы E/E/PE, связанной с безопасностью, была только PFD_{avg} (см. 9.3.2). Исследование в области машин, у которых интенсивность запросов достаточно высока, например $\lambda_M \approx w_M \approx 1000$ [1/ч] и $\varphi \approx P_a\lambda_M \approx P_a w_M \approx 1{,}0$ [1/ч], показали, что значения HER, рассчитанные по формуле, намного выше, чем рассчитанные по статистическим данным, полученным из эксплуатации.

Затем было установлено следующее:

a) если система E/E/PE, связанная с безопасностью, постоянно работает или ее интенсивность запросов достаточно высока, HER φ, соответствующая опасным отказам системы E/E/PE, связанной с безопасностью, следует аппроксимировать ее интенсивностью опасных отказов λ [1/ч], поскольку опасный отказ немедленно приводит к событию, наносящему вред;

b) исходя из этого в начале разработки приведенных методов было принято три вида режимов работы, т. е. режима работы с редкими запросами (обычный режим), режима работы с большим количеством запросов и режима непрерывной работы;

c) формула $\varphi \approx P_a\lambda_M \approx P_a w_M$ принята для режима работы с редкими запросами, а формула $\varphi \approx \lambda$ — для двух введенных режимов работы, т. е. режимов с большим количеством запросов и непрерывной работы.

Таким образом, на ранней стадии разработки приведенных методов режим работы с редкими запросами был определен как «режим работы, при котором интенсивность запросов достаточно низка», а режим работы с большим количеством запросов как «режим работы, при котором интенсивность запросов достаточно высока», соответственно. В настоящем стандарте в случае применения к безопасности (см. В.2) отказ означает опасный отказ.

В средней области, когда интенсивность запросов не является ни слишком низкой, ни достаточно высокой, для решения проблемы необходимо:

- провести линии ограничения режима работы с редкими запросами и режима работы с большим количеством запросов;
- распространить зоны, соответствующие этим режимам работы, на новые области, соответствующие промежуточным режимам работы по обе стороны от линии соответственно.

Режим работы с редкими запросами определен в ГОСТ Р МЭК 61508-4 как режим работы, при котором частота запросов работы системы, связанной с безопасностью, не превышает одного раза в год, а частота проведения контрольных проверок не превышает двух в год. Частота запросов один раз в год приближенно равна $w_M \approx \lambda_M \approx 10^{-4}$ [1/ч]. Здесь w_M и λ_M — постоянные частота и интенсивность запросов соответственно.

В настоящее время работа в режиме редких запросов определена как режим работы, «при котором функция безопасности выполняется только по запросу для перевода EUC в установленное безопасное состояние, а частота запросов составляет не более одного раза в год» (см. ГОСТ Р МЭК 61508-4).

Тогда понятны причины, по которым формулу $\varphi \approx P_a\lambda_M \approx P_a w_M$ вряд ли можно применить к системам E/E/PE, работающим в режимах с большим количеством запросов или непрерывной работы:

a) формула $\varphi \approx P_a\lambda_M \approx P_a w_M$ является приближенной для повторяемого и неповторяемого конечного события при условии, что интенсивность запросов достаточно низка, а интенсивность завершения достаточно высока. Однако формула вряд ли применима к неповторяемому конечному событию, если интенсивность запроса недостаточно низка или интенсивность завершения недостаточно высока [19], [3], [4];

b) формула вряд ли применима к такому конкретному случаю, как система контроля подушек безопасности автомобиля или система в целом, описанная в приложении А (см. 7.2.3, 9.3.2) [18], [7];

c) какой режим работы должен быть адаптирован к системе, зависит от соотношения между интенсивностью запросов и HER, и, следовательно, выбор режима работы должен основываться не только на интенсивности запросов, но также на интенсивностях завершения запроса, отказов, ремонтов объекта и экспозиции риска (см. 7.2.3 и B.4, B.8) [3], [4], [16], [17] [18];

d) события, связанные с нанесением вреда в машиностроительном секторе, где интенсивность запросов достаточно высока, можно считать неповторяемыми конечными событиями.

B.2 Безопасные/опасные состояния системы и отказы

Система E/E/PE, связанная с безопасностью, выполняет функции безопасности для поддержания безопасного состояния системы в целом и сохранения остаточного риска, связанного с безопасностью, на допустимом уровне (см. 3.1.1, примечание 3). Обычно, если объект, входящий в состав системы E/E/PE, отказал, отказ может выявить несколько режимов отказа. Эти режимы подразделяют на безопасные и опасные в соответствии с безопасным или опасным состоянием системы. Таким образом, отказ, приводящий к безопасному или опасному режиму, называют безопасным или опасным отказом, соответственно (см. ГОСТ Р МЭК 61508-4);

a) безопасный отказ определяют как отказ, который приводит к необоснованному выполнению функций безопасности или увеличению вероятности необоснованного выполнения функций безопасности, или поддержанию безопасного состояния системы в целом, следовательно, безопасное состояние системы сохраняется (см. ГОСТ Р МЭК 61508-4);

b) опасный отказ определяют как отказ, препятствующий выполнению функций безопасности или снижающий вероятность корректного выполнения функций безопасности (см. ГОСТ Р МЭК 61508-4);

c) безопасное состояние определяют как состояние системы в целом, когда безопасность достигнута, т. е. когда риск, связанный с безопасностью, поддерживают на приемлемом уровне.

Например, промежуточное состояние D на рисунке 10 означает состояние, в котором система управления подушками безопасности отключена. Понятно, что FER в промежуточном состоянии D меньше, чем FER в начальном состоянии A, а именно отказ D, приводящий систему управления подушками безопасности в отключенное состояние, является безопасным отказом, учитывая, что начальное состояние A является безопасным состоянием системы. С другой стороны, если FER в промежуточном состоянии C больше, чем FER в начальном состоянии A, отказ UD может быть опасным отказом, приводящим систему в целом в состояние системы с более высоким риском, чем риск системы в начальном состоянии A.

Как правило, с точки зрения безопасных и опасных отказов объектов, связанных с безопасностью, которые составляют систему E/E/PE, связанную с безопасностью, безопасные состояния системы в целом разделяют на следующие три типа [5]:

- неизменное состояние;
- изменяющееся состояние;
- взаимно изменяющиеся состояния.

Предположим, что E/E/PE система, связанная с безопасностью, предназначена для защиты от одной или нескольких опасностей для достижения безопасных состояний системы в целом, тогда можно утверждать следующее:

1) Если безопасное состояние системы в отношении опасности (или риска) обеспечивает то, что E/E/PE система, связанная с безопасностью, находится только в активном или неактивном состоянии и эта особенность E/E/PE системы не изменяется, в то время как система в целом находится под воздействием опасности (или риска), тогда это безопасное состояние системы является неизменным в отношении опасности (или риска) и отказа системы E/E/PE, связанной с безопасностью (см. 3.1.2.2, примечания 1—3). Пока система безопасности E/E/PE, связанная с безопасностью, поддерживает неизменное безопасное состояние системы, у нее могут произойти как безопасные, так и опасные отказы. Некоторые химические технологические установки включают в себя технические системы безопасности (т. е. E/E/PE системы, связанные с безопасностью), что является примерами неизменного безопасного состояния системы [5].

2) Если безопасное состояние системы в отношении опасности (или риска) обеспечивает E/E/PE система, связанная с безопасностью, которая переходит из активного состояния в неактивное или из неактивного в активное состояние или в обоих направлениях, пока система в целом подвергается опасности (или риску), тогда безопасное состояние системы является изменяющимся в отношении опасности (или риска) и отказа системы E/E/PE, связанной с безопасностью. Пока E/E/PE система, связанная с безопасностью, поддерживает изменяющееся безопасное состояние системы, у нее не должны возникать безопасные отказы. Например, автоматизированная система рулевого управления автомобилем (т. е. типичная система E/E/PE, связанная с безопасностью) состоит из электротехнических элементов, таких как датчики, контроллеры и исполнительные механизмы (см. 9.1). Эта система управляет направлением движения автомобиля в соответствии с различными условиями для создания

безопасных маршрутов, где безопасное состояние системы, т. е. безопасный маршрут, является изменяющимся. Поэтому любой отказ автоматизированной системы рулевого управления автомобиля может быть опасным, потому что безопасное состояние системы является изменяющимся [5], [8].

3) Предположим, что отказ системы E/E/PE, связанной с безопасностью, связан с безопасным состоянием системы S1 по отношению к опасности H1 (или риску R1) и безопасным состоянием системы S2 по отношению к опасности H2 (или риску R2) и S1 — неизменное безопасное состояние системы, достигнутое за счет того, что E/E/PE система, связанная с безопасностью, находится в активном или неактивном состоянии. Таким образом, если S2 является неизменным безопасным состоянием системы, которое обеспечено тем, что система E/E/PE, связанная с безопасностью, находится в неактивном или активном состоянии, или если S2 является изменяющимся состоянием, система в целом находится в изменяющемся состоянии по отношению к H1 (или R1) и H2 (или R2), а опасности H1 и H2 являются взаимно обратными опасностями по отношению к отказу E/E/PE системы, связанной с безопасностью. Безопасное состояние системы в целом должно быть изменено в зависимости от взаимообратных опасностей, т. е. безопасные состояния системы в зависимости от взаимообратных опасностей являются взаимно изменяющимися. Если E/E/PE система, связанная с безопасностью, должна поддерживать взаимно изменяющиеся безопасные состояния системы S1 и S2, тогда безопасный отказ для S1 является опасным для S2 (см., например, таблицу B.1) [5], [7]—[9].

Например, если автоматизированная система управления тормозами автомобиля, которая состоит из таких электротехнических элементов, как датчики, контроллеры и исполнительные механизмы, в результате отказа не может остановить автомобиль при опасном приближении к автомобилю, движущемуся впереди, в результате может произойти заднее столкновение, в то же время при отказе автоматизированной системы управления тормозами автомобиль может внезапно остановиться и его может ударить сзади другой автомобиль. Следовательно, обе опасности (столкновение с автомобилем впереди и удар сзади) являются взаимообратными опасностями в отношении отказа автоматизированной системы управления тормозами, и безопасные состояния системы по отношению к этим взаимным опасностям являются взаимно изменяющимися. Таким образом, система автоматизированного управления тормозами автомобиля должна управлять взаимно изменяющимися безопасными состояниями системы для таких взаимно обратных опасностей, как:

- первичная опасность, вызванная невозможностью остановить автомобиль;
- взаимная опасность, вызванная ошибочной остановкой автомобиля.

В таблице B.1 показана взаимосвязь между режимами отказа автоматической системы управления тормозами, взаимно обратными опасностями, а также безопасными и опасными отказами [9].

Таблица B.1 — Соотношение между режимами отказа, опасностями и безопасными/опасными отказами

Опасности, которые необходимо контролировать	Режим отказа для автоматической системы управления тормозами	
	Режим отказа 1 (например, короткое замыкание)	Режим отказа 2 (например, нарушение контакта)
Первичная опасность	Безопасный отказ	Опасный отказ
Взаимообратная опасность	Опасный отказ	Безопасный отказ

В целом для объекта, связанного с безопасностью, справедливо следующее [7], [9]:

- если объект входит в систему со структурой «1 из 2» для первичной опасности, то он входит в систему со структурой «2 из 2» для взаимно обратной опасности.
- если установлены допустимые уровни риска для соответствующих взаимно обратных опасностей, структура и параметры системы, в том числе интенсивности и режимы отказов элементов, связанных с безопасностью, должны быть разработаны так, чтобы система соответствовала этим допустимым уровням риска, установленным на основе анализа FER для заданного начального состояния.

B.3 Сложность системы, связанной с безопасностью

Сложность системы, связанной с безопасностью, зависит не только от размера системы в целом (т. е количества компонентов системы), опасностей, создаваемых системой в целом и отказами по общей причине уровней защиты (включая исходные источники запросов), а также от сложности логики развития отказов, такой как логика последовательности отказов, которая определяет возникновение конечного события и появление конечных последствий риска (см. раздел 6, 9.1, 9.2, 9.5 и A.5). Кроме того, при обсуждении сложности систем, связанных с безопасностью, необходимо учитывать сложность безопасных состояний системы. Относительно сложности справедливо следующее:

a) система в целом с изменяющимися и/или взаимно изменяющимися безопасными состояниями системы является более сложной, чем система только с неизменными безопасными состояниями системы;

b) система, связанная с безопасностью со всеми видами отказов, такими как отказы D, UD и DU, имеет более высокий уровень сложности, чем система только с ограниченным количеством типов отказов (см. A.5);

c) система, связанная с безопасностью, включающая элементы, интенсивность отказов которых различна в рабочем и нерабочим состояниях, является более сложной, чем система, включающая элементы, интенсивности отказов которых являются постоянными, однако рассмотрение этих ситуаций выходит за рамки настоящего стандарта (см. рис. 15 и 9.3.1) [14], [15];

d) возможность того, что системе в целом присущ мета-риск, также является фактором сложности системы в целом, однако рассмотрение этой ситуации выходит за рамки настоящего стандарта (см. таблицу 1, раздел 6, 9.1, 9.5 и А.5).

В.4 Сопоставление традиционного и нового анализа

На рисунке В.1 показана типовая взаимосвязь между переменной интенсивностью запросов λ_M и HER, которая является функцией λ_M, $\varphi(\lambda_M)$, фиксированной структуры системы и других переменных (или параметров), таких как интенсивности отказов/ремонтов и завершения запросов в определенных условиях системы в целом, включая E/E/E систему, связанную с безопасностью, которая выполняет функцию конечного уровня безопасности.

На рисунке горизонтальная и вертикальная оси показывают интенсивность запросов λ_M и HER, $\varphi(\lambda_M)$ соответственно:

a) наклонная сплошная прямая линия и горизонтальная прямая линия показывают, что HER можно рассчитать по формулам $\varphi(\lambda_M) \approx P_a\lambda_M \approx P_a w_M$ и $\varphi(\lambda_M) \approx \lambda$ в соответствии с ГОСТ Р МЭК 61508-6:

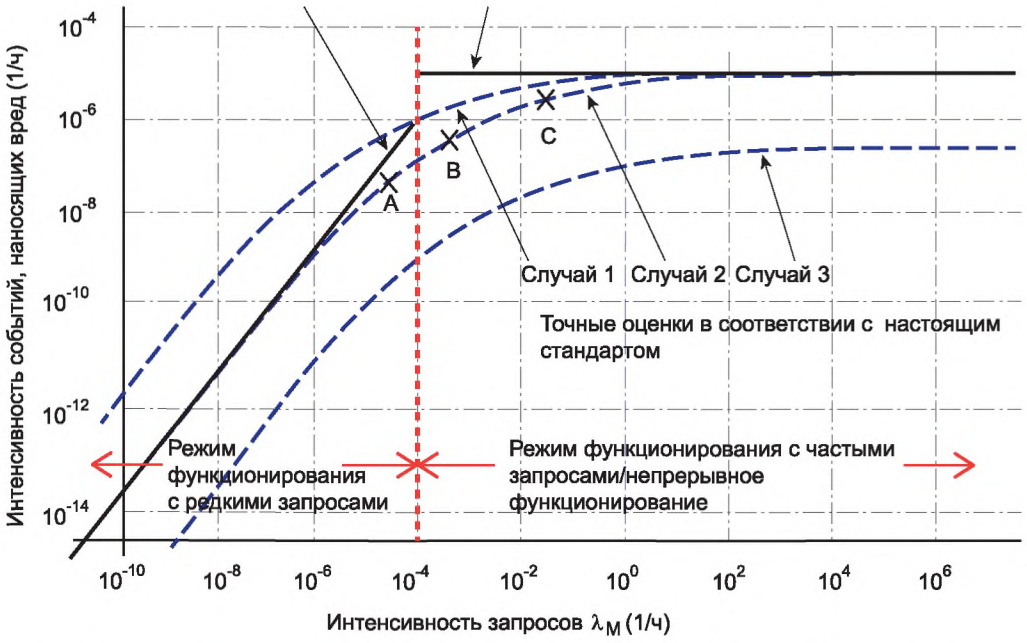
b) искривленные области в случаях 1—3 указывают на то, что HER $\varphi(\lambda_M)$ можно рассчитать, используя FER для исходного состояния в соответствии с настоящим стандартом.

Поскольку HER анализируют отдельно с использованием двух формул в соответствии с ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-5 и ГОСТ Р МЭК 61508-6, $\varphi(\lambda_M) \approx P_a\lambda_M \approx P_a w_M$ и $\varphi(\lambda_M) \approx \lambda$ для режимов с редкими и частыми запросами соответственно, часто возникают области разрыва HER, рассчитанных для этих режимов работы, показанные на рисунке В.1 (традиционный анализ).

Использование FER для заданного начального состояния обеспечивает получение непрерывной линии и более реалистичного анализа независимо от режима работы для HER, показанной на рисунке (новый анализ), поскольку не только интенсивности отказов и ремонтов системы, но и все параметры, включая интенсивность запросов и их завершений, значимо влияют на HER. Это позволяет выполнить анализ в соответствии с новым подходом. Таким образом:

- формула $\varphi(\lambda_M) \approx \lambda$ представляет верхний предел HER, который в общем случае может быть адаптирован к непрерывному режиму работы системы в целом, где HER — монотонно возрастающая функция $\varphi(\lambda_M)$ в конкретных условиях;

- на рисунке В.1 искривленные области (случаи 1—3) обычно формируются монотонно возрастающими функциями.



Примечание — В соответствии со стандартами серии ГОСТ Р МЭК 61508 $\varphi \approx P_a \lambda_M \approx P_a w_M$, $\varphi \approx \lambda$.

Рисунок В.1 — Сопоставление традиционного и нового анализа

Однако формула $\varphi(\lambda_M) \approx \lambda$ не обязательно представляет верхний предел HER для системы в целом, если $\varphi(\lambda_M)$ не является монотонно возрастающей функцией (см. рисунки А.4 и А.5).Таким образом, существуют значительные различия традиционного и нового анализа.

1) Если оба целевых показателя отказов PFD_{avg} и APF_{drg} больше HER и если интенсивность запросов является достаточно высокой, то FER для заданного начального состояния стремится к целевому показателю отказов PFH (см. случай 1 на рисунке В.1).

2) Однако если только один из целевых показателей PFD_{avg} или APF_{drg} больше HER и если интенсивность запросов является достаточно высокой, то новый анализ, который обеспечивает реалистичные и точные оценки HER, позволяет получить более низкие оценки, чем приближенные оценки, полученные в соответствии с традиционным анализом (см. случай 3 на рисунке В.1).

3) Если интенсивность запросов является достаточно низкой и если только целевой показатель PFD_{avg} больше HER, традиционный анализ может дать хорошие приближения HER (см. случай 2 на рисунке В.1).

4) Однако если оба целевых показателя PFD_{avg} и APF_{drg} больше HER или если только APF_{drg} больше HER, то новый анализ позволяет получить существенно более низкие или более высокие оценки, чем приближенные оценки, полученные в соответствии с традиционным анализом в зависимости от конкретных условий системы в целом (см. 7.2.3, 9.3.3 и случаи 1 и 3 на рисунке В.1).

В.5 Разделение режима работы

Как правило, HER, φ, может быть функцией значительного числа переменных (или параметров), таких как интенсивность отказов/ремонтов, интенсивность запросов λ_M, интенсивность завершений запроса μ_M, частота запросов w_M, интенсивность восстановлений m и экспозиция риска T с точки зрения анализа риска (см., например, рисунок 10). Если эти переменные, кроме интенсивности запросов λ_M, фиксированы, то φ является функцией λ_M, т. е. $\varphi = \varphi(\lambda_M)$;

a) если функция HER, $\varphi(\lambda_M)$, является непрерывной и монотонно возрастающей, то систему в целом называют монотонно возрастающей системой относительно риска и наоборот, это показано в виде изогнутых линий (случаи 1—3) на рисунке В.1;

b) однако $\varphi(\lambda_M)$ не всегда монотонна для системы в целом, как показано в приложении А, где точки перегиба расположены в местах пересечения λ_M и $\varphi(\lambda_M)$ (см. рисунок А.4) [8], [7], [9], [18]. В этом случае неправильно просто начертить линию, чтобы разделить режим работы на две части, потому что HER в области промежуточных значений интенсивности запросов может быть выше, чем в области с более высокой интенсивностью запросов и/или в области с более низкой интенсивностью запросов (см. рисунок А.4 и А.5);

c) в связи с этим необходимо установить процедуру выбора подходящего режима работы для того, чтобы требования, относящиеся к уровню полноты безопасности, полностью соответствовали таблице В.2.

В.6 Допустимая интенсивность опасных (наносящих вред) событий и остаточный риск

Если E/E/PE система, связанная с безопасностью, выполняет функции безопасности конечного уровня защиты для обеспечения безопасного состояния системы в целом, остаточный риск в результате контроля/снижения риска должен быть ниже допустимого уровня риска, т. е. HER, соответствующая отказам E/E/PE системы, связанной с безопасностью, должна быть ниже допустимого уровня:

a) предположим, например, что для снижения риска системы в целом систему E/E/PE, связанную с безопасностью, эксплуатируют в соответствии со случаем 2 на рисунке В.1. Таким образом, три точки функционирования A, B и C могут быть представлены комбинацией λ_M [1/ч] и φ[1/ч], т. е. «λ_M и φ» как «$3 \cdot 10^{-5}$ и $4 \cdot 10^{-8}$», «$4 \cdot 10^{-4}$ и $3 \cdot 10^{-7}$» и «$3 \cdot 10^{-2}$ и $2 \cdot 10^{-6}$» соответственно;

b) если допустимая HER остаточного риска, например установлена равной 10^{-6} [1/ч], тогда точки A и B удовлетворяют допустимой HER остаточного риска для безопасной работы, но HER рабочей точки C не соответствует допустимому уровню остаточного риска (см. 3.1.1, примечание 3).

В.7 Процедура определения уровня полноты безопасности (SIL) объекта

Преодолеть трудности, связанные с разделением режимов, соответствующих целевым показателям отказов и определения уровня полноты безопасности SIL, упомянутого выше, позволяет определить подход настоящего стандарта:

a) сначала целевой показатель снижения риска φ/λ_M вводят с использованием FER для заданного начального состояния, как описано в 7.2.3. Здесь λ_M — интенсивность запросов, рассматриваемого уровня защиты; φ — интенсивность запросов следующего уровня защиты, если рассматриваемым уровнем защиты является промежуточный уровень защиты или FER для заданного начального состояния, если рассматриваемым уровнем защиты является FPL (см. 9.2 и 9.3). Показатели φ/λ_M и φ являются общими целевыми показателями для оценки производительности работы объекта в режимах редких запросов, частых запросов или непрерывной работы соответственно. Показатели PFD_{avg} и PFH в ГОСТ Р МЭК 61508 (все части) являются приближенными значениями φ/λ_M и φ соответственно. Приближения действительны при описанных выше условиях;

b) исходя из вышеизложенного, процедура выбора режимов работы и определения SIL объекта состоит в следующем [20]:

- устанавливают φ/λ_M и φ в качестве целевых показателей отказов объекта для режима работы с редкими запросами и для режима работы с частыми запросами или непрерывной работы соответственно;

- выбирают SIL X(X = 1, 2, 3 или 4) и SIL Y(Y = 1, 2, 3 или 4), используя φ/λ_M и φ в соответствии с таблицей В.2 соответственно;

- выбирают более низкий SIL из выбранных SIL *X* и SIL *Y* объекта, если $X \neq Y$;
- выбирают SIL *Y* объекта, если $X = Y$ (поскольку стандарты по функциональной безопасности, такие как ГОСТ Р МЭК 61508 (все части) и ГОСТ Р МЭК 61511 (все части), обычно требуют назначения SIL *Y* объекта с более высокими требованиями по сравнению с назначенным SIL *X* при условии $X = Y$).

Т а б л и ц а В.2 — Уровни полноты безопасности (SIL) в соответствии с ГОСТ Р МЭК 61508 (все части)

SIL	Целевые показатели отказов	
	Режим работы с редкими запросами PFD_{avg} или отношение φ/λ_M (SIL X)	Режим работы с частыми запросами или режим непрерывной работы PFH, или интенсивность опасных/вредных событий φ [1/ч] (SIL Y)
4	$\geq 10^{-5}$ до $< 10^{-4}$ C (SIL 4)	$\geq 10^{-9}$ до $< 10^{-8}$
3	$\geq 10^{-4}$ до $< 10^{-3}$ B (SIL 3)	$\geq 10^{-8}$ до $< 10^{-7}$ A (SIL 3)
2	$\geq 10^{-3}$ до $< 10^{-2}$ A (SIL 2)	$\geq 10^{-7}$ до $< 10^{-6}$ B (SIL 2)
1	$\geq 10^{-2}$ до $< 10^{-1}$	$\geq 10^{-6}$ до $< 10^{-5}$ C (SIL 1)

Предположим, например, что комбинацию φ/λ_M (SIL *X*) и φ(SIL *Y*) [1/ч], т. е. «φ/λ_M (SIL X) – φ(SIL Y) » оценивают в трех точках A, B и C вдоль кривой, соответствующей случаю 2 на рисунке B.1. Таким образом:

1) «$1{,}3 \cdot 10^{-3}$ (SIL 2) – $4 \cdot 10^{-8}$ (SIL 3)» в точке A;
2) «$7{,}5 \cdot 10^{-4}$ (SIL 3) – $3 \cdot 10^{-7}$ (SIL 2)» в точке B;
3) «$6{,}6 \cdot 10^{-5}$ (SIL 4) – $2 \cdot 10^{-6}$ (SIL 1)» в точке C.

Таким образом, для объекта выбирают SIL из SIL *X* и SIL *Y*, а именно из SIL 2 (SIL *X*), SIL 2 (SIL *Y*) и SIL 1 (SIL *Y*) в точках A, B и C соответственно. В соответствии с B.6 известно, что если объект находится в точке C (SIL 1) для соответствия системы в целом допустимому остаточному риску, объекту должен быть назначен более высокий SIL (возможно, SIL 2).

B.8 Выводы и замечания

Настоящий стандарт помогает рационально определить уровень полноты безопасности (SIL) системы в целом, где соответствующие HER представлены не только монотонно возрастающими функциями переменной λ_M, как показано на рисунках A.4 и B.1.

Таким образом, настоящий стандарт обеспечивает:

- теоретические основы взаимосвязи целевых показателей отказов объекта (например, E/E/PE системы, связанной с безопасностью) и HER;
- способ целостного и простого анализа HER для оценки производительности объекта для контроля за риском и/или снижением риска;
- руководство по правильной оценке и анализу риска и выводу соответствующей оценки функциональной безопасности.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе

Таблица ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО 9000—2015	IDT	ISO 9000:2015 «Системы менеджмента качества. Основные положения и словарь»
ГОСТ Р 51901.12—2007 (МЭК 60812:2006)	MOD	IEC 60812:2006 «Техника анализа надежности систем. Метод анализа вида и последствий отказа»
ГОСТ Р 27.12—2019	MOD	IEC 61882:2016 «Исследования опасности и работоспособности (HAZOP). Руководство по применению»
ГОСТ Р 51897—2011	IDT	ISO Guide 73:2009 «Менеджмент рисков. Словарь»
ГОСТ Р ИСО 31000—2010	IDT	ISO 31000:2009 «Менеджмент риска. Принципы и руководство»
ГОСТ Р ИСО/МЭК 31010—2011	IDT	IEC/ISO 31010:2009 «Менеджмент риска. Методы оценки риска»
ГОСТ Р МЭК 62502—2014	IDT	IEC 62502:2010 «Менеджмент риска. Анализ дерева событий»
ГОСТ Р 27.010—2019	MOD	IEC 61703:2016 «Математические выражения для показателей безотказности, готовности, ремонтопригодности и обеспеченности технического обслуживания и ремонта»
ГОСТ Р 51901.14—2007	IDT	IEC 61078:2006 «Менеджмент риска. Структурная схема надежности и булевы методы»
ГОСТ Р 27.302—2009	IDT	IEC 61025:2006 «Надежность в технике. Анализ дерева неисправностей»
ГОСТ Р МЭК 61165—2019	IDT	IEC 61165:2016 «Надежность в технике. Применение марковских методов»
ГОСТ Р МЭК 61508-1—2012	IDT	IEC 61508-1:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
ГОСТ Р МЭК 61508-2—2012	IDT	IEC 61508-2:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
ГОСТ Р МЭК 61508-3—2012	IDT	IEC 61508-3:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
ГОСТ Р МЭК 61508-4—2012	IDT	IEC 61508-4:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
ГОСТ Р МЭК 61508-5—2012	IDT	IEC 61508-5:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»
ГОСТ Р МЭК 61508-6—2012	IDT	IEC 61508-6:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3»
ГОСТ Р МЭК 61508-7—2012	IDT	IEC 61508-7:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»

Окончание таблицы ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р МЭК 61511-1—2018	IDT	IEC 61511-1:2016 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования»
ГОСТ Р МЭК 61511-2—2018	IDT	IEC 61511-2:2016 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1»
ГОСТ Р МЭК 61511-3—2018	IDT	IEC 61511-3:2016 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности»
ГОСТ Р 57149—2016	IDT	ISO/IEC Guide 51:2014 «Аспекты безопасности. Руководящие указания по включению их в стандарты»
Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: - IDT — идентичные стандарты; - MOD — модифицированные стандарты.		

Библиография

[1] МЭК 60050-192:2015 Международный электротехнический словарь. Часть 192. Надежность (International electrotechnical vocabulary — Part 192: Dependability)

[2] Sato Y., Henley E.J., Inoue K. An action-chain model for the design of hazard-control systems, IEEE Trans. on Reliability.— Vol.—39. — No.2.— p.151—159 — 1990

[3] Kawahara T., Ichitsuka A., Sato Y. State transition Model of Safety-Related Systems with Automatic Diagnosis and its Formulation for Functional Safety Assessment. — IEICE Trans. —Vol.J86-A.— No.3.— 241-249. — March 2003

[4] Yoshimura I., Sato Y.: Safety-Integrity Levels Model for Safety-Related Systems in Dynamic Demand State IEICE Trans.— Vol.J86-A.— No.11.—1188-1196. — Nov. 2003

[5] Yoshimura I., Sato Y. Safety Achieved by the Safe Failure Fraction (SFF) inIEC 61508, IEEE Trans. on Reliability .— Vol.57.— No.4. — 662-669. — Dec. 2008

[6] Yoshimura I., Sato Y. Estimation of Calendar-Time- and Process-Operative-TimeHazardous-Event Rates for the Assessment of Fatal Risk Int. Jour. of Performability Engineering Vol.5 No. 4 July 2009. — 377-386

[7] Takeichi M., Suyama K., Sato Y. Functional Safety Assessment of Air Bag Systemsfor Automobiles Trans. Soc. of Automotive Engs. of Japan. —Vol.44. — No.2. — 627-633. — March 2013

[8] Kushibiki T., Sato. Y. Functional Safety Assessment of the Motor Vehicles Steer-byWire Systems with both Faults Detectable only by Demands and Commission FaultsJSME Trans.(C).— Vol.76.— No.762. — 388-396. — Feb. 2010

[9] Takeichi M., Suyama K., Sato Y. Functional Safety Assessment of Pre-CrashSystems for Reciprocal Hazards, JSME Trans.(C), — Vol.79. — No.806. —3839-3853. — Oct. 2013

[10] Vesely W.E., Narumu R.E. PREP and KITT. — Computer cords for automatic evaluation of fault trees. — IN-1349. — 1970

[11] Henley E.J., Kumamoto H. Reliability Engineering and Risk Assessment.— EnglewoodCliffs. — Prentice Hall. — 1981

[12] Sato Y., Inoue K., Kumamoto H., The safety assessment of human-robot systems (3rd Report). On the quantification of consecutive failure logic. — Bulletin of JSME. — Vol.29, No.257. — Nov., 3945-3951. — 1986

[13] Fussell J.B., Aber E.F., Rahl R.G. On the quantitative analysis of priority AND failurelogic. — IEEE Trans. Reliability. — Vol.R-25.— No.5.— 324-326, 1976

[14] Yoshimura I., Sato Y. Safety-Integrity Levels of Safety-Related System with Selfdiagnosis Functions in Dynamic Demand State. — Jour. Reliability Engineering Association of Japan. — Vol.151. — No.3. — 219-227. — May 2006

[15] Yoshimura I., Sato Y. Estimation of Hazardous Event Rate for Safety-Related Systems with Self-diagnosis Function. — Jour. Japan Society for Safety Engineering. — Vol.46. — No.1. — 16-23. — Jan. 2007

[16] 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 Modelling (AIWARM 2004). — Hiroshima.— 577-584.— 2004

[17] Shimodaira T., Sato Y., Suyama K. Estimation of Hazardous Event Rate for Repairable 1-out-of-2 Safety-Related Systems Based on State transition Models.— IEICE Trans. — Vol.J88-A. — No.8. — 962-973.— Aug. 2005

[18] Muta H., Sato Y. Functional Safety Assessment of Safety-related Systems with Nonperfect Proof-tests. — IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences. — Vol. E97-A. — No. 8. — 1739-1746. — Aug. 2014

[19] Misumi Y., Sato Y., Estimation of average hazardous-event-frequency for allocationof safety-integrity, Reliability Engineering & System Safety. — 66 (1999). — 135-144. — 1999

[20] Shimodaira T., Sato Y., Suyama K. Estimation of Average Hazardous-Event Rate for Steady-State Demands and Determination of SIL, JSME Trans.(C). — Vol.72.— No.715. — 953-959.— March 2006

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

Ключевые слова: надежность в технике, состояние, событие, частота события, интенсивность события, вероятностный анализ риска

БЗ 1—2020/87

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 28.11.2019. Подписано в печать 31.01.2020. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 7,44. Уч.-изд. л. 6,97.
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.

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

gost.e-ecolog.ru