ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59773— 2021

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Порядок применения комплекса стандартов ГОСТ 34332. Примеры расчетов

(IEC 61508-6:2010, NEQ)
(ISO/IEC Guide 51:2014, NEQ)

Издание официальное

Москва
Российский институт стандартизации
2021

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «РСТ») совместно с Международной ассоциацией «Системсервис» (МА «Системсервис»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 439 «Средства автоматизации и системы управления»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 20 октября 2021 г. № 1184-ст

4 В настоящем стандарте учтены основные нормативные положения следующих международных документов:

МЭК 61508-6:2010 «Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2:2010 и МЭК 61508-3:2010» (IEC 61508-6:2010 «Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3», NEQ);

ISO/IEC Guide 51:2014 «Аспекты безопасности. Руководящие указания по включению их в стандарты» (ISO/IEC Guide 51:2014 «Safety aspects — Guidelines for their inclusion in standards», NEQ)

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

© Оформление. ФГБУ «РСТ», 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
4 Порядок применения требований комплекса стандартов ГОСТ 34332 3
4.1 Пользователи стандартов 3
4.2 Полный жизненный цикл Э/Э/ПЭ СБЗС систем 3
4.3 Менеджмент функциональной безопасности 4
5 Примеры расчетов 4
Приложение А (справочное) Порядок применения требований ГОСТ 34332.3 и ГОСТ 34332.4 5
Приложение Б (справочное) Методы оценки вероятностей отказа аппаратных средств 12
Приложение В (справочное) Примеры расчета охвата диагностикой и доли безопасных отказов 67
Приложение Г (справочное) Методика и примеры количественного определения влияния отказов аппаратных средств по общей причине в Э/Э/ПЭ СБЗС системах 70
Приложение Д (справочное) Применение таблиц полноты безопасности программного обеспечения в соответствии с ГОСТ 34332.4 83
Библиография 99

Введение

Современные здания и сооружения (объекты капитального строительства) представляют собой сложные системы, включающие в свой состав систему строительных конструкций и ряд инженерных систем в разных сочетаниях, в том числе для жизнеобеспечения, реализации технологических процессов, энерго- и ресурсосбережения, обеспечения безопасности и другие системы. Эти системы взаимодействуют друг с другом, с внешней и внутренней средами, образуя единое целое и выполняя свои функции назначения.

Объекты капитального строительства жестко привязаны к местности. Рабочие характеристики зданий, сооружений и входящих в них систем могут быть реализованы, проверены и использованы только в том месте, в котором объекты построены и системы установлены.

Безопасность зданий и сооружений обеспечивается применением совокупности мер, мероприятий и средств снижения риска причинения вреда до приемлемого уровня риска и его поддержания в течение периода эксплуатации или использования этих объектов. К средствам снижения риска относятся системы, связанные с безопасностью зданий и сооружений (СБЗС системы), и системы, неполный перечень которых представлен в ГОСТ 34332.1—2017 (приложение А, раздел А.3). Среди СБЗС систем наиболее распространенными являются системы, содержащие электрические и/или электронные и/или программируемые электронные (Э/Э/ПЭ) компоненты. Такие системы, именуемые Э/Э/ПЭ СБЗС системами, в течение многих лет применяют для выполнения функций безопасности. Кроме них и вместе с ними используют системы, основанные на неэлектрических (гидравлических, пневматических) технологиях, а также прочие средства уменьшения риска. Для решения задач безопасности зданий и сооружений во всех больших объемах применяют программируемые электронные (ПЭ) СБЗС системы.

Следующими по важности характеристиками систем после характеристик назначения являются характеристики безопасности. Важнейшей характеристикой безопасности систем признана их функциональная безопасность.

В настоящем стандарте представлен порядок применения требований комплекса стандартов ГОСТ 34332 к Э/Э/ПЭ СБЗС системам на стадиях их жизненного цикла и приведены примеры расчетов.

Комплекс стандартов ГОСТ 34332 ориентирован на обеспечение соблюдения требований безопасности зданий и сооружений, в том числе объектов транспортных инфраструктур, установленных техническими регламентами Таможенного союза [1] — [3].

Настоящий стандарт распространяется на Э/Э/ПЭ СБЗС системы, подсистемы и составляющие этих систем, включая сенсоры, исполнительные устройства и интерфейс человек—машина, рассчитан на любой диапазон сложности СБЗС систем и ориентирован на комплексное обеспечение безопасности и антитеррористической защищенности объектов защиты — зданий и сооружений.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Порядок применения комплекса стандартов ГОСТ 34332. Примеры расчетов

Functional safety of building/construction safety-related systems.
Procedure for application of GOST 34332 set of standards. Examples of calculations

Дата введения — 2021—12—01

1 Область применения

1.1 Настоящий стандарт содержит информацию и руководящие указания по применению требований, рекомендаций и справочных материалов к электрическим, электронным, программируемым электронным (Э/Э/ПЭ) системам, связанным с безопасностью зданий и сооружений (Э/Э/ПЭ СБЗС системам) и к программному обеспечению этих систем, установленных и представленных в комплексе стандартов ГОСТ 34332, а также примеры расчетов.

Примечания

1 К Э/Э/ПЭ СБЗС системам относятся системы, неполный перечень которых перечислен в ГОСТ 34332.1—2017 (пункт 5.3.3 и раздел А.3).

2 Э/Э/ПЭ СБЗС системы ориентированы на комплексное обеспечение безопасности и антитеррористической защищенности зданий и сооружений.

1.2 Настоящий стандарт применяют совместно со стандартами комплекса ГОСТ 34332.

1.3 Настоящий стандарт не распространяется на Э/Э/ПЭ СБЗС систему, которая является единственной одиночной системой, способной осуществить необходимое снижение риска на объекте, и требуемая полнота безопасности этой системы ниже, чем определено уровнем полноты безопасности (УПБ) 1 — самым низким уровнем, приведенным в ГОСТ 34332.2—2017 (таблицы 1 и 2).

1.4 Настоящий стандарт рекомендуется для применения пользователями стандартов комплекса ГОСТ 34332 (юридическими и физическими лицами, чьи действия влияют на обеспечение функциональной безопасности Э/Э/ПЭ СБЗС систем и обеспечение безопасности и антитеррористической защищенности объектов на стадиях их жизненных циклов).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 34332.1—2017 Безопасность функциональная систем, связанных с безопасностью зданий и сооружений. Часть 1. Основные положения

ГОСТ 34332.2—2017 Безопасность функциональная систем, связанных с безопасностью зданий и сооружений. Часть 2. Общие требования

ГОСТ 34332.3—2021 Безопасность функциональная систем, связанных с безопасностью зданий и сооружений. Часть 3. Требования к системам

ГОСТ 34332.4—2021 Безопасность функциональная систем, связанных с безопасностью зданий и сооружений. Часть 4. Требования к программному обеспечению

ГОСТ 34332.5—2021 Безопасность функциональная систем, связанных с безопасностью зданий и сооружений. Часть 5. Меры по снижению риска, методы оценки

Издание официальное

ГОСТ 34100.3.1—2017/ISO/IEC Guide 98-3/Suppl 1:2008 Неопределенность измерения. Часть 3. Руководство по выражению неопределенности измерения. Дополнение 1. Трансформирование распределений с использованием метода Монте-Карло

ГОСТ МЭК 61508-3—2018 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р 51901.12—2007 (МЭК 60812:2006) Менеджмент риска. Метод анализа видов и последствий отказов

ГОСТ Р МЭК 61508-1—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

ГОСТ Р МЭК 61508-2—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам электрическим/электронным/программируемым электронным, связанным с безопасностью

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 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 применены термины по ГОСТ 34332.1, ГОСТ 34332.2, ГОСТ 34332.3, ГОСТ 34332.4, ГОСТ 34332.5.

3.2 В настоящем стандарте применены следующие сокращения:

АС — аппаратное(ые) средство(а);

ЖЦ — жизненный(ые) цикл(ы);

ИЭ — исполнительный элемент;

КСБ — комплексная система безопасности;

ПЛК — программируемый логический контроллер;

ПО — программное обеспечение;

ПЭ — программируемая(ое) электронная(ое) (система или средство);

СБ система — связанная с безопасностью система;

СБЗС система — связанная с безопасностью зданий и сооружений система;

ТР — технический регламент;

ТР ТС — технический регламент Таможенного союза;

ТС — Таможенный союз;

УО — управляемое оборудование;

УПБ — уровень полноты безопасности;

УПБ ПО — уровень полноты безопасности программного обеспечения;

ФБ — функциональная безопасность;

Э/Э/ПЭ — электрическая(ое), электронная(ое), программируемая электронная(ое) (по отношению к системе, подсистеме, оборудованию или компоненту);

Э/Э/ПЭ СБЗС система — электрическая и/или электронная, и/или программируемая система, связанная с безопасностью здания или сооружения;

MUT — среднее значение времени работы (Mean Up Time);

MDT — среднее значение времени простоя (Mean Down Time);

MTBF — среднее время между отказами (Mean Time Between Failure);

MTTF — среднее время до отказа (Mean Time To Failure);

PFD_{SYS} — средняя вероятность отказа по запросу ФБ для Э/Э/ПЭ СБЗС системы;

PFD_S — средняя вероятность отказа по запросу для подсистемы датчиков;
PFD_L — средняя вероятность отказа по запросу для логической подсистемы;
PFD_{FE} — средняя вероятность отказа по запросу для подсистемы исполнительных элементов;
PFH_{SYS} — средняя частота опасного отказа для ФБ Э/Э/ПЭ системы, связанной с безопасностью;
PFH_S — средняя частота опасного отказа для подсистемы датчиков;
PFH_L — средняя частота опасного отказа для логической подсистемы;
PFH_{FE} — средняя частота опасного отказа для подсистемы исполнительных элементов.

4 Порядок применения требований комплекса стандартов ГОСТ 34332

4.1 Пользователи стандартов

4.1.1 Пользователями настоящего стандарта и стандартов всего комплекса ГОСТ 34332 являются лица (подразделения, организации), влияющие на обеспечение функциональной безопасности Э/Э/ПЭ СБЗС систем и безопасности объектов защиты на стадиях ЖЦ систем и объектов.

Примечание — К пользователям стандартов относятся:

- инвесторы, заказчики, исполнители реализации проектов объектов защиты (зданий и сооружений) и входящих в их состав Э/Э/ПЭ СБЗС систем, владельцы, эксплуатанты, пользователи объектов защиты и лица, осуществляющие техническое обслуживание и ремонт Э/Э/ПЭ СБЗС систем;
- лица, осуществляющие на стадиях ЖЦ Э/Э/ПЭ СБЗС систем верификацию, аудит или оценку соответствия требованиям ФБ;
- лица, осуществляющие страхование объектов защиты от природных и/или техногенных, или антропогенных опасностей и угроз.

4.1.2 Пользователям стандартов ГОСТ 34332 следует ознакомиться со всеми действующими стандартами комплекса ГОСТ 34332 и/ими должны быть тщательно изучены настоящий стандарт и разделы стандартов, связанные с теми стадиями ЖЦ Э/ЭПЭ СБЗС систем, которые относятся к ответственности конкретных лиц (подразделений, организаций) по созданию и применению Э/Э/ПЭ СБЗС систем в части обеспечения достижения и поддержания требуемой ФБ.

4.2 Полный жизненный цикл Э/Э/ПЭ СБЗС систем

4.2.1 Базовая структура полного ЖЦ Э/Э/ПЭ СБЗС систем установлена в ГОСТ 34332.2—2017 (раздел 7) и включает в себя в общем случае следующие стадии и этапы:

- разработка концепции;
- определение области применения;
- анализ опасностей и рисков;
- определение требований к ФБ;
- распределение требований безопасности;
- разработка проектной документации на СБЗС системы;
- разработка рабочей документации,
- планирование полной установки, интеграции и ввода в действие;
- планирование оценки и подтверждения соответствия;
- планирование эксплуатации и технического обслуживания систем;
- реализация Э/Э/ПЭ СБЗС систем;
- реализация СБЗС систем, основанных на неэлектрических технологиях (в случае их применения);
- реализация прочих средств уменьшения риска;
- оценка и подтверждение соответствия;
- эксплуатация, техническое обслуживание, ремонт, периодический контроль;
- видоизменение и модификация систем;
- вывод из эксплуатации и утилизация.

4.2.2 Структура полного ЖЦ Э/Э/ПЭ СБЗС систем конкретного объекта защиты (здания и сооружения) может быть дополнена, сокращена или изменена по отношению к базовой структуре при условии обоснования новой структуры и обеспечения выполнения целей и требований ГОСТ 34332.2.

4.2.3 Действия участников создания и применения Э/Э/ПЭ СБЗС систем на стадиях и этапах их ЖЦ синхронизируют с действиями участников создания и использования зданий и сооружений на соответствующих стадиях и этапах их ЖЦ.

4.2.4 Для эффективного взаимодействия участников создания и применения Э/Э/ПЭ СБЗС систем между собой и с участниками создания и использования зданий и сооружений на соответствующих стадиях ЖЦ организуют совместные рабочие группы специалистов различных профилей.

4.2.5 Верификацию, аудит и оценку соответствия Э/Э/ПЭ СБЗС систем и их составляющих следует осуществлять на всех стадиях и этапах ЖЦ систем.

4.3 Менеджмент функциональной безопасности

4.3.1 Всем организациям, вовлеченным в действия по созданию и применению Э/Э/ПЭ СБЗС систем по 4.1, рекомендуется осуществлять менеджмент ФБ на всех стадиях ЖЦ систем.

4.3.2 Менеджмент ФБ охватывает аспекты:

- полномочий и ответственности высшего руководства организации в отношении менеджмента ФБ;
- политики менеджмента ФБ;
- обеспечения руководства организации по менеджменту ФБ;
- обеспечения компетентности лиц, вовлеченных в действия по менеджменту ФБ;
- ответственности лиц и подразделений, вовлеченных в действия по менеджменту ФБ;
- выполнения процедур по менеджменту ФБ;
- контроля выполнения действий и процедур по менеджменту ФБ.

4.4 Порядок применения требований ГОСТ 34332.3 и ГОСТ 34332.4 представлен в приложении А.

5 Примеры расчетов

5.1 Методы оценки вероятностей отказа АС представлены в приложении Б.

5.2 Примеры расчета охвата диагностикой и доли безопасных отказов представлены в приложении В.

5.3 Методика и примеры количественного определения влияния отказов аппаратных средств по общей причине в Э/Э/ПЭ СБЗС системах представлены в приложении Г.

5.4 Применение таблиц полноты безопасности ПО в соответствии с ГОСТ 34332.4.

Приложение А
(справочное)

Порядок применения требований ГОСТ 34332.3 и ГОСТ 34332.4

А.1 Общие положения

Инженерная система здания или сооружения в случае неправильной работы может представлять опасность для людей, имущества и окружающей среды из-за возникновения опасных событий (например, пожара, взрыва, выброса токсичных веществ, попадания в механизмы и т. д.). Отказы оборудования могут возникать из-за физических отказов устройств (случайные отказы оборудования), либо систематических отказов (ошибки человека, допущенные в технических условиях и конструкции конкретной системы, при определенной комбинации входов систем приводят к систематическим отказам), либо некоторых внешних условий.

Общий подход, основанный на оценке рисков, для предотвращения и/или управления отказами в Э/Э/ПЭ СБЗС системах представлен в ГОСТ 34332.2.

Основная задача настоящего стандарта заключается в обеспечении оснащения объекта и его составляющих такими автоматическими Э/Э/ПЭ СБЗС системами, которые обеспечивают предотвращение:

- отказов систем управления, инициирующих другие события, которые, в свою очередь, могут привести к опасному событию;

- необнаруженных отказов СБЗС систем (например, в системах аварийного останова), делающих эти системы недоступными в момент необходимых действий, связанных с безопасностью.

Требование проведения анализа опасностей и рисков на уровне процесса/системы для определения суммарного снижения риска, необходимого для достижения соответствия критериям риска для данного применения, установлены в ГОСТ 34332.1—2017 (разделы 7 и 8) и ГОСТ 34332.2—2017 (раздел 7). Оценка риска основана на оценке как последствий (или серьезности), так и частоты (или вероятности) опасного события.

Требование использования степени снижения риска, установленной в процессе анализа, для необходимости определения одной или нескольких СБ систем и конкретных функций безопасности (каждая с заданной полнотой безопасности), для выполнения которых нужны эти системы, содержится в ГОСТ 34332.2.

Примечания

1 СБ система включает в себя АС, ПО и дополнительные средства (например, источники питания, датчики, устройства ввода/ввода, исполнительные элементы и др.) [см. ГОСТ 34332.1—2017 (пункт 3.44)].

2 УПБ определяется как один из четырех дискретных уровней. УПБ 4 является наивысшим, а УПБ 1 — низшим уровнем [см. ГОСТ 34332.1—2017 (пункт 3.52)].

В ГОСТ 34332.2—2017 (раздел 7) установлено, что величина уменьшения риска, определенная в результате анализа рисков, далее должна быть использована для определения следующего: сколько требуется СБЗС систем (одна или несколько); каким должен быть УПБ функции(ий) безопасности системы, для которой они необходимы (каждая из функций безопасности имеет определенный УПБ).

В ГОСТ 34332.3 и ГОСТ 34332.4 представлены требования к функциям безопасности и полноте безопасности, установленные в ГОСТ 34332.2 для любой Э/Э/ПЭ СБЗС системы, включая КСБ, а также действия на стадиях ЖЦ системы, которые:

- применяют при разработке технического задания, проектировании и внесении изменений в АС и ПО,

- сфокусированы на средствах предотвращения случайных отказов и/или управления случайными отказами АС и систематическими отказами (на ЖЦ Э/Э/ПЭ СБЗС системы и ПО этой системы).

Примечание — Для четкого структурирования требований настоящего стандарта применена модель процесса разработки, в которой каждый этап ЖЦ следует в определенном порядке с небольшим шагом. Однако может быть использован иной подход к ЖЦ, если планируется выполнение целей и требований, установленных в ГОСТ 34332.2—2017 (раздел 7).

ГОСТ 34332.3 и ГОСТ 34332.4 не содержат указаний, какой УПБ соответствует заданному требуемому приемлемому риску. Это решение зависит от многих факторов, включая характер применения, степень выполнения функций безопасности другими системами, а также социальные и экономические факторы (см. ГОСТ 34332.1 и ГОСТ 34332.2).

Требования ГОСТ 34332.3 и ГОСТ 34332.4 включают в себя:

- методы и средства, классифицированные в соответствии с УПБ, для избегания систематических отказов с применением превентивных мер.

Примечание — Требуемые методы и средства для каждого УПБ представлены в ГОСТ 34332.3—2017 (таблицы приложений А и В) и ГОСТ 34332.4;

- управление систематическими отказами (включая отказы ПО) и случайными отказами АС с применением конструктивных решений, таких как использование встроенных средств обнаружения неисправностей, введение

избыточности, а также дополнительных конструкторских и архитектурных решений (например, пространственное разнесение).

В ГОСТ 34332.3 гарантирование того, что цель обеспечения УПБ удовлетворена для опасных случайных отказов АС, основано:

- на требованиях к отказоустойчивости оборудования [см. ГОСТ 34332.3—2021 (таблицы 1 и 2)];
- охвате диагностикой и частоте проверочных испытаний подсистем и компонентов с помощью проведения анализа надежности с использованием соответствующих данных.

По ГОСТ 34332.3 и ГОСТ 34332.4 гарантирование того, что цель полноты безопасности удовлетворена для систематических сбоев, достигается:

- правильным применением процедур управления безопасностью;
- использованием компетентного персонала;
- применением указанных видов ЖЦ систем безопасности, включая указанные методы и средства.

Примечание — Могут быть использованы средства, альтернативные описанным в настоящем стандарте, при условии, что при планировании обеспечения безопасности документально оформляется обоснование применения альтернативных средств (см. ГОСТ 34332.2);

- выполнением предусмотренных действий по реализации стадий ЖЦ системы безопасности, включая предусмотренные методы и средства;
- применением независимой оценки функциональной безопасности.

Примечание — Независимая оценка не всегда подразумевает проведение оценки третьей стороной [см. ГОСТ 34332.2—2017 (раздел 8)].

В ГОСТ 34332.3 формализованы требования к обеспечению полноты безопасности АС Э/Э/ПЭ СБЗС систем, включая датчики и исполнительные устройства. Методы и средства, направленные против систематических отказов АС, включают в себя соответствующую комбинацию средств по предотвращению неисправностей и управлению отказами. Если для обеспечения ФБ необходимы действия оператора, то должны быть приведены требования к интерфейсу оператора. В ГОСТ 34332.3 для обнаружения случайных отказов АС также определены методы и средства диагностического тестирования, реализуемые на уровне АС и ПО (например, диверсификация).

В ГОСТ 34332.4 формализованы требования к обеспечению полноты безопасности как встроенного ПО (включая диагностические средства обнаружения неисправностей), так и прикладного ПО. В ГОСТ 34332.4 предусмотрено использование комбинированного подхода, ориентированного на предотвращение ошибок (обеспечение качества) и устойчивость к ошибкам (за счет архитектуры ПО), так как не существует способа проверки отсутствия отказов в достаточно сложном СБ ПО и особенно предотвращения ошибок в технических условиях и в проекте. ГОСТ 34332.4 требует принятия таких принципов разработки ПО, как проектирование сверху вниз, модульность, проверка на каждой стадии ЖЦ, проверка программных модулей и библиотек программных модулей, а также четкое документирование для облегчения проверки и подтверждения соответствия. Для различных уровней ПО требуются различные уровни гарантии того, что эти и связанные с ними принципы были правильно реализованы.

Разработчик(ки) ПО всей Э/Э/ПЭ СБЗС системы, включая КСБ объекта, должен (должны) четко представлять себе архитектуру применяемой программируемой электроники, когда требуется нахождение компромиссов между архитектурами АС и ПО при оценке их вклада в обеспечение безопасности [см. ГОСТ 34332.3—2021 (рисунки 4 и 5)].

А.2 Функциональные шаги применения ГОСТ 34332.3

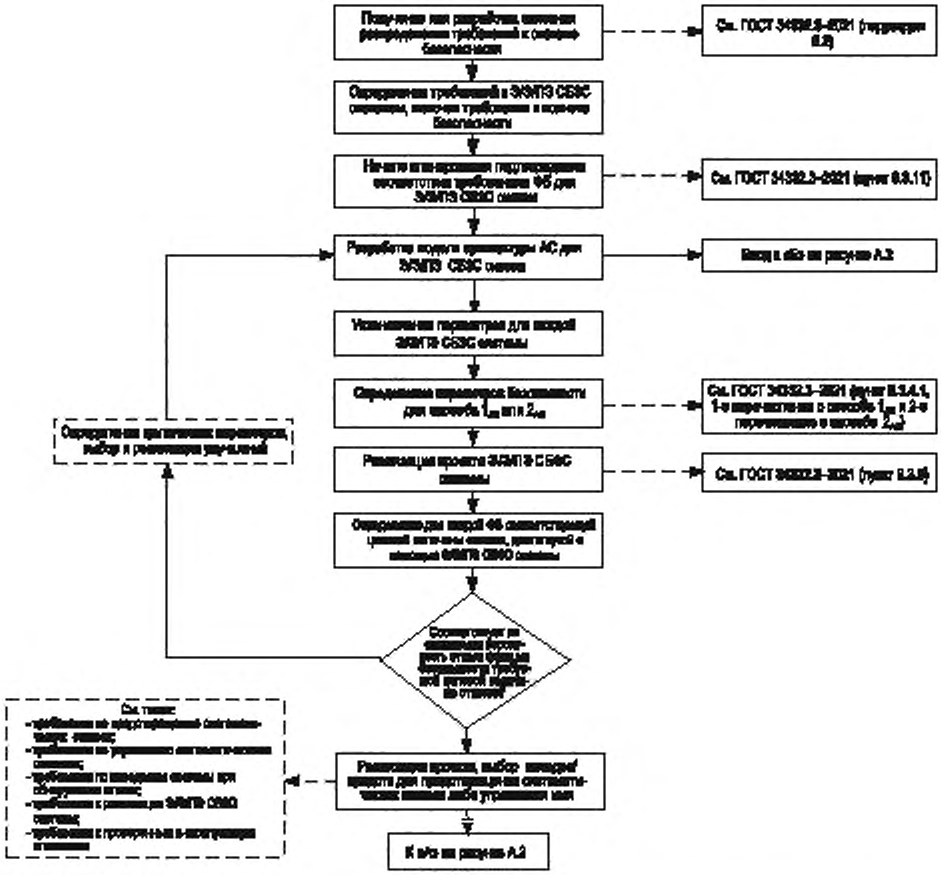
Функциональные шаги применения ГОСТ 34332.3 представлены в настоящем приложении на рисунках А.1 и А.2. Функциональные шаги применения ГОСТ 34332.4 представлены на рисунке А.3.

Функциональные шаги применения ГОСТ 34332.3 следующие:

- определение распределения требований к системе безопасности (ГОСТ 34332.2). При необходимости выполняют обновление планирования подтверждения соответствия системе безопасности в процессе разработки Э/Э/ПЭ СБЗС системы;
- определение требований к Э/Э/ПЭ СБЗС системам, включая требования к полноте безопасности для каждой функции безопасности [ГОСТ 34332.2—2017 (подраздел 8.2)];
- определение требований к ПО и передача их поставщику и/или разработчику ПО для применения в соответствии с ГОСТ 34332.4.

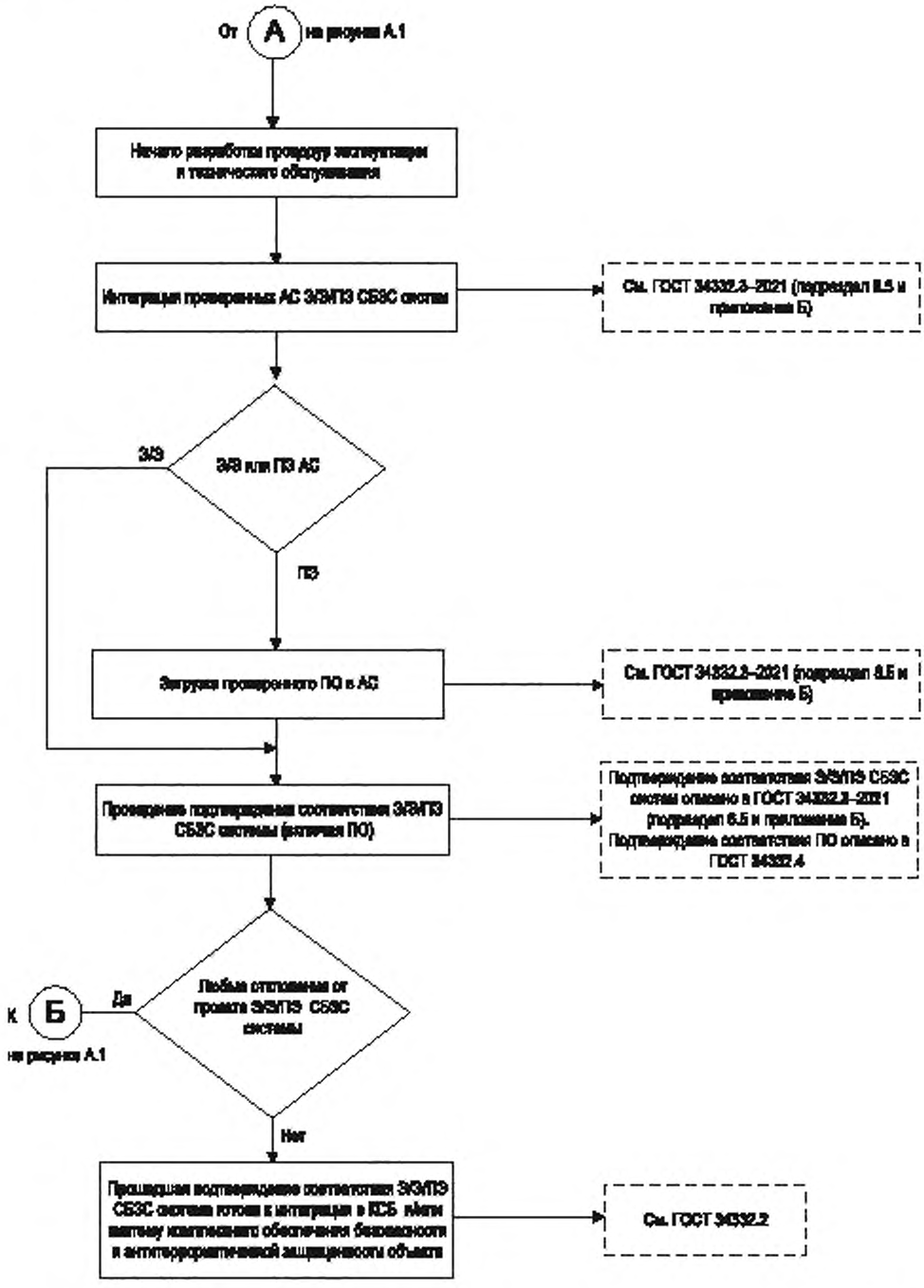
Примечание — На данной стадии необходимо рассмотреть возможность одновременных отказов в системе управления УО и Э/Э/ПЭ СБЗС системе(ах) [см. ГОСТ 34332.1—2017 (пункт Д.3.6.5 приложения Д)]. Такие отказы могут быть результатом отказов компонентов по общей причине, например из-за влияния окружающей среды. Наличие подобных отказов может привести к бóльшим по сравнению с ожидаемым значением остаточного риска;

- начало планирования подтверждения соответствия требованиям ФБ для Э/Э/ПЭ СБЗС системы [см. ГОСТ 34332.3—2021 (пункт 8.3.11)].



Примечание — В ПЭ СБЗС системах для ПО выполняют аналогичные действия (см. рисунок А.3).

Рисунок А.1 — Функциональные шаги применения ГОСТ 34332.3 (лист 1)



Примечание — В ПЭ СБЗС системах для ПО выполняют аналогичные действия (см. рисунок А.3).

Рисунок А.2 — Функциональные шаги применения ГОСТ 34332.3 (лист 2)

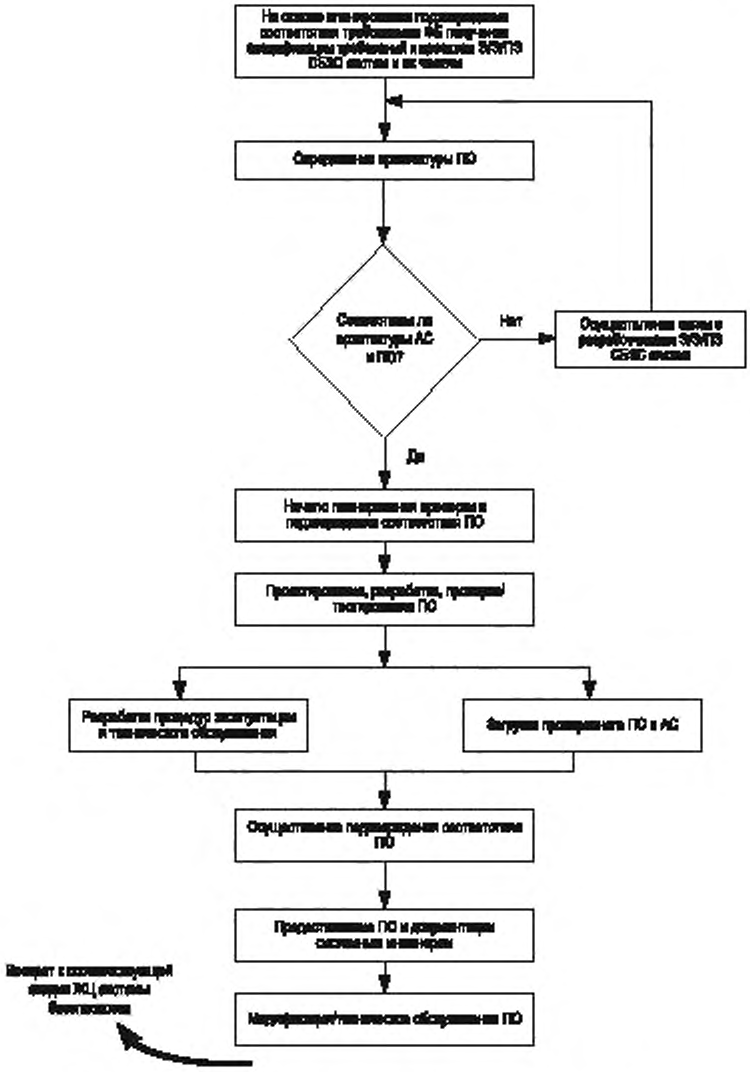


Рисунок А.3 — Функциональные шаги применения ГОСТ 34332.4

- задание архитектуры (конфигурации) логической подсистемы, датчиков и исполнительных устройств. Вместе с поставщиком/разработчиком ПО проведение анализа архитектуры АС, ПО и влияния на безопасность компромиссов между АС и ПО (см. ГОСТ МЭК 61508-3—2018, рисунок 4). При необходимости повторение анализа;

- разработка модели архитектуры АС для Э/Э/ПЭ СБЗС системы. Эту модель разрабатывают, проверяя отдельно каждую ФБ, и определяют подсистему (компонент), используемую(ый) для реализации этой функции;

- установление параметров для каждой подсистемы (компонента), используемой(го) в Э/Э/ПЭ СБЗС системе. Для каждой подсистемы (компонента) определяют:

а) временной интервал между тестовыми испытаниями для отказов, которые не обнаруживаются автоматически,

б) среднее время восстановления,

в) охват диагностикой [см. ГОСТ 34332.3—2021 (приложение В)],

г) вероятность отказа,

д) долю безопасных отказов [см. ГОСТ 34332.3—2021 (приложение В)];

е) требуемые архитектурные ограничения: для способа 1_{AC} [см. ГОСТ 34332.3—2021 (пункт 8.3.4.1, 1-е перечисление)] и приложение В, для способа 2_{AC} (см. ГОСТ 34332.3—2021, пункт 8.3.4.1, 2-е перечисление)];

- создание модели расчета безотказности для каждой ФБ, которая должна быть реализована Э/Э/ПЭ СБЗС системой.

Примечание — Модель расчета безотказности представляет собой математическую формулу, показывающую взаимосвязь между безотказностью и соответствующими параметрами, связанными с оборудованием и условиями его использования;

- расчет прогнозируемой безотказности для каждой ФБ с использованием соответствующей методики. Сравнение результата с заданными характеристиками отказов, определенными во 2-м перечислении данного пункта, и требованиями для способа 1_{AC} [см. ГОСТ 34332.3—2021 (пункт 8.3.4.1, 1-е перечисление)] или способа 2_{AC} [см. ГОСТ 34332.3—2021 (пункт 8.3.4.1, 2-е перечисление)]. Если прогнозируемая безотказность не соответствует заданным характеристикам отказов и/или требованиям способа 1_{AC} или способа 2_{AC}, то изменяют:

а) если возможно, один или несколько параметров подсистемы [возвращаются к 6-му перечислению данного пункта], и/или

б) архитектуру АС [возвращаются к 4-му перечислению данного пункта].

Примечание — Существует множество методов моделирования, и аналитик должен выбрать наиболее соответствующий (перечень тех методов, которые могут быть использованы, приведен в приложении В);

- реализация проекта Э/Э/ПЭ СБЗС системы. Выбирают методы и средства для управления систематическими отказами АС, отказами, вызванными влиянием окружающей среды, и эксплуатационными отказами [см. ГОСТ 34332.3—2021 (приложение А)];

- загрузка проверенного ПО (см. ГОСТ 34332.4) в соответствующие АС [см. ГОСТ 34332.3—2021 (подраздел 8.4 и приложение Б)], параллельная разработка рабочих инструкций для пользователей и документации для обслуживающего персонала по техническому обслуживанию системы (см. ГОСТ Р МЭК 61508-2 и ГОСТ 34332.3—2021 (подраздел 8.7 и приложение Б)]. Учет аспектов, связанных с ПО (см. А.3 и 6-е перечисление данного пункта);

- проведение подтверждения соответствия ФБ Э/Э/ПЭ СБЗС системы [см. ГОСТ 34332.3—2021 (подраздел 8.6) и приложение Б] вместе с разработчиком(ами) ПО [см. ГОСТ 34332.4—2021 (подраздел 7.7)];

- передача АС и результатов подтверждения соответствия Э/Э/ПЭ СБЗС системы системным инженерам для дальнейшей интеграции всей системы;

- если в процессе эксплуатации Э/Э/ПЭ СБЗС системы требуется модернизация/видоизменение, то при необходимости — повторное возвращение к ГОСТ 34332.3—2021 (подраздел 8.6).

В течение ЖЦ системы безопасности объекта для Э/Э/ПЭ СБЗС систем выполняют множество различных действий. Среди них верификация [см. ГОСТ 34332.3—2021 (подраздел 8.8)] и оценка ФБ (см. ГОСТ Р МЭК 61508-1—2012, раздел 8).

При выполнении приведенных выше действий для Э/Э/ПЭ СБЗС системы выбирают методы и средства обеспечения безопасности, соответствующие требуемому УПБ. Для помощи в выборе таких методов и средств составлены таблицы, упорядочивающие различные методы/средства в соответствии с четырьмя УПБ (см. ГОСТ Р МЭК 61508-2—2012, приложение В). Краткий обзор каждого из методов и средств со ссылками на источники информации о них, включая перекрестные ссылки на эти таблицы, представлены в ГОСТ 34332.5—2021 (приложения А и Б).

Один из возможных методов расчета вероятностей отказа АС для Э/Э/ПЭ СБЗС систем представлен в приложении Б.

Примечание — При выполнении приведенных выше действий допускается применять средства, альтернативные указанным в настоящем стандарте, при условии, что оправдывающие обстоятельства документально оформлены в процессе планирования подтверждения соответствия системе безопасности [см. ГОСТ 34332.2—2017 (раздел 6)].

А.3 Функциональные шаги применения ГОСТ 34332.4

Можно выделить следующие функциональные шаги применения ГОСТ 34332.4 (см. рисунок А.3):

- определение требований для Э/Э/ПЭ СБЗС систем и соответствующих компонентов планирования подтверждения соответствия системе безопасности [см. ГОСТ 34332.2—2017 (подраздел 7.10)]; при необходимости — выполнение обновления планирования подтверждения соответствия системе безопасности в процессе разработки ПО.

Примечание — На предыдущих стадиях ЖЦ:

- определены требуемые ФБ и соответствующие им УПБ (см. [ГОСТ 34332.2—2017 (подразделы 7.8 и 7.9)];

- распределены функции безопасности для назначенных систем Э/Э/ПЭ, связанных с безопасностью (см. [ГОСТ 34332.2—2017 (подраздел 7.6)]);

- определение архитектуры ПО для всех ФБ, реализуемых программно [см. ГОСТ 34332.4—2021 (подраздел 7.4 и приложение А)];

- проведение вместе с поставщиком/разработчиком Э/Э/ПЭ СБЗС системы анализа архитектуры АС и ПО, а также влияния на безопасность компромиссов между АС и ПО [см. ГОСТ 34332.4—2021 (рисунок 3)]. При необходимости анализ повторяют;

- проведение планирования проверки и подтверждения соответствия безопасности для ПО [см. ГОСТ 34332.4—2021 (подразделы 7.3 и 7.9)];

- проведение проектирования, разработки, проверки и тестирования ПО в соответствии:

а) с планом подтверждения соответствия ФБ для ПО,

б) УПБ ПО,

в) ЖЦ СБ ПО;

- завершение действий по окончательной проверке ПО и интеграции проверенного ПО в соответствующие АС [см. ГОСТ 34332.4—2021 (подраздел 7.5)] и параллельная разработка процедур по аспектам ПО для пользователей и обслуживающего персонала системы, выполняемые при эксплуатации системы [см. ГОСТ 34332.4—2021 (подраздел 7.6)], а также 10-е перечисление пункта А.2;

- проведение вместе с разработчиком АС [см. ГОСТ 34332.4—2021 (подраздел 7.7)] подтверждения соответствия ПО в интегрированных Э/Э/ПЭ СБЗС системах [см. ГОСТ 34332.4—2021 (подраздел 7.7)];

- передача результатов подтверждения соответствия Э/Э/ПЭ системы системным инженерам для дальнейшей интеграции всей системы безопасности;

- если в процессе эксплуатации потребуется модернизация ПО Э/Э/ПЭ СБЗС системы, то выполняют возврат к соответствующей стадии, как описано в ГОСТ 34332.4—2021 (подраздел 7.8).

В процессе ЖЦ СБ ПО выполняют множество различных действий, среди них верификация [см. ГОСТ 34332.4—2021 (подраздел 7.9)] и оценка ФБ [см. ГОСТ 34332.2—2017 (раздел 8)].

В процессе выполнения приведенных выше действий выбирают методы и средства, обеспечивающие безопасность ПО, соответствующие требуемому УПБ. Для оказания помощи в выборе таких методов и средств составлены таблицы, упорядочивающие различные методы/средства в соответствии с четырьмя УПБ [см. ГОСТ 34332.4—2021 (приложение А)]. Краткое описание каждого из методов и средств со ссылками на источники информации о них, включая перекрестные ссылки на эти таблицы, представлено в ГОСТ 34332.5—2021 (приложение В).

Обработанные примеры применения таблиц полноты безопасности приведены в приложении Е, а в ГОСТ 34332.5 включено описание вероятностного подхода к определению полноты безопасности ПО для уже разработанного ПО [(см. ГОСТ 34332.5—2021 (приложение Г)].

Примечание — При выполнении приведенных выше действий допускается применять средства, альтернативные указанным в настоящем стандарте, при условии, что соответствующее обоснование документально оформлено в процессе планирования подтверждения соответствия системе безопасности [см. ГОСТ 34332.2—2017 (раздел 6)].

Приложение Б
(справочное)

Методы оценки вероятностей отказа аппаратных средств

Б.1 Общие положения

В настоящем приложении рассмотрены методы расчета вероятностей отказа АС Э/Э/ПЭ СБЗС систем, указанных в ГОСТ 34332.2—ГОСТ 34332.4. Данная информация носит справочный характер и не должна быть рассмотрена как единственно возможные методы оценки. Однако в настоящем приложении описан относительно простой подход к оценке характеристик Э/Э/ПЭ СБЗС систем и приведены руководящие указания по использованию альтернативных методов, взятых из классических методов расчета надежности.

Примечание — Архитектуры систем, представленные в настоящем стандарте, являются примерами и не должны быть рассмотрены как исчерпывающие, так как существует множество других архитектур, которые также могут быть использованы.

Существует значительное число методов, непосредственно применимых для анализа полноты безопасности АС Э/Э/ПЭ СБЗС систем. Как правило, их делят на группы в соответствии со следующими характеристиками:

- статические (логические) и динамические (состояния/переходы) модели;
- аналитические модели и моделирование на основе метода Монте-Карло.

Логические модели включают в себя все модели, описывающие статические логические связи между элементарными отказами и полным отказом системы. Блок-схемы надежности [см. ГОСТ 34332.5—2021 (Б.6.4) и ГОСТ Р 51901.12] и дерево отказов [см. ГОСТ 34332.5—2021 (Б.6.5.5, Б.6.5.9 и Б.6.5.10)] относятся к логическим моделям.

Модели состояний-переходов включают в себя все модели, описывающие поведение системы (переход из состояния в состояние) в соответствии с произошедшими событиями (отказами, ремонтами, тестированием и т. д.). Модели Маркова [см. ГОСТ 34332.5—2021 (Б.6.5.6)], сети Петри [см. ГОСТ 34332.5—2021 (Б.2.3.3 и Б.6.5.10)] и формальные языки принадлежат к моделям состояний/переходов. Представлены два марковских подхода: упрощенный подход, основанный на специальной формуле приложения В, и общий подход, позволяющий провести непосредственный расчет графов Маркова (Б.5.2). Если для систем безопасности марковский подход не применим, то вместо него может быть использован метод Монте-Карло. На современных компьютерах расчет возможен даже для уровня УПБ 4. В подразделах Б.5.3 и Б.5.4 даны руководящие указания по применению метода Монте-Карло [см. ГОСТ 34332.5—2021 (Б.6.5.8)] для моделей поведения, использующих сети Петри и формальные языки моделирования.

Упрощенный подход, который представлен первым, основан на графическом представлении блок-схемы надежности и специальной формулы Маркова, выведенной из работ Тейлора с учетом относительно консервативных гипотез, описанных в Б.3.1.

Все эти методы могут быть использованы для большинства Э/Э/ПЭ СБЗС систем. При определении того, какой метод использовать для конкретного применения, очень важно, чтобы пользователь конкретного метода был компетентен в его применении, и это может оказаться более важным, чем непосредственно используемый метод. Аналитик отвечает за то, чтобы гипотеза, лежащая в основе любого конкретного метода, была выполнена корректно для рассматриваемого применения либо была внесена какая-либо необходимая корректировка для достижения соответствующего реалистичного консервативного результата. В случае недостаточной надежности данных или превалирующего числа отказов по общей причине может быть достаточным использование простейшей(го) модели/метода. Важна возможная потеря точности, которую определяют в каждом конкретном случае.

Если для проведения расчетов используют ПО, то специалист, выполняющий расчет, должен понимать формулы/методы, используемые в программном пакете, чтобы быть уверенным в том, что они применимы в каждом конкретном случае.

Специалист также должен проверить программный пакет путем сравнения результатов расчета нескольких тестовых примеров, полученных с помощью программного пакета и ручным способом.

Если отказ системы управления УО инициирует обращение к Э/Э/ПЭ СБЗС системе, то вероятность возникновения опасного события зависит также от вероятности отказа системы управления УО. В этой ситуации необходимо рассмотреть возможность одновременного отказа компонентов системы управления УО и Э/Э/ПЭ СБЗС системы из-за механизмов отказа по общей причине. При неправильном анализе наличие подобных отказов может привести к большим по сравнению с ожидаемым значениям остаточного риска.

Б.2 Основные вероятностные расчеты

Б.2.1 Введение

Блок-схема надежности, показанная на рисунке Б.1, представляет систему (контур) безопасности, состоящую из трех датчиков (*A*, *B*, *C*), одного логического решающего устройства (*D*), двух исполнительных элементов (*E*, *F*) и демонстрирующую наличие в ней отказов по общей причине (*CCF*).

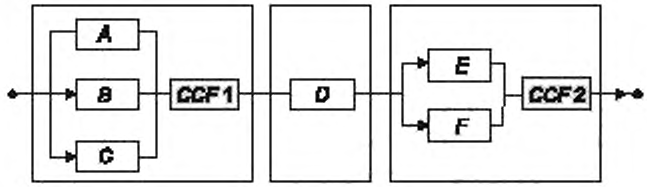


Рисунок Б.1 — Блок-схема надежности полного контура безопасности

Эта блок-схема облегчает выявление пяти комбинаций отказов, ведущих к отказу Э/Э/ПЭ СБЗС системы. Каждую из них именуют минимальным сечением:

- (*A*, *B*, *C*) — тройной отказ;
- (*E*, *F*) — двойной отказ;
- (*D*), (*CCF*1), (*CCF*2) — одинарные отказы.

Б.2.2 Э/Э/ПЭ СБЗС система с низкой интенсивностью запросов

Когда Э/Э/ПЭ СБЗС система используется в режиме с низкой интенсивностью запросов согласно настоящему стандарту требуется, чтобы была дана оценка средней вероятности опасных отказов по запросу (т. е. средней неготовности) PFD_{avg}. Это просто отношение MDT*(T)*/*T*, где MDT*(T)* означает время простоя Э/Э/ПЭ СБЗС системы на отрезке времени [0, *T*].

Для систем безопасности вероятность отказа, как правило, крайне низка и вероятность одновременного наличия двух минимальных сечений ничтожна. Поэтому суммарное значение средних периодов простоя всех минимальных сечений дает консервативную оценку среднего времени простоя всей системы. Исходя из блок-схемы на рисунке Б.1 имеем:

$$MDT \approx MDT^{ABC} + MDT^{D} + MDT^{EF}. \quad (Б.1)$$

Деление на *T* дает:

$$PFD = PFD_{avg}^{ABC} + PFD_{avg}^{D} + PFD_{avg}^{EF}. \quad (Б.2)$$

Таким образом, для последовательно соединенных компонентов вычисления PFD_{avg} похожи на вычисления, которые выполняют с обычными вероятностями, очень малыми по сравнению с 1.

Однако для параллельно соединенных компонентов, где потеря функциональности возможна только при множественном отказе, таком как (*E*, *F*), очевидно, что MDT^{EF} не представляется возможным вычислить непосредственно из MDT^{E} и MDT^{F}. MDT системы MDT(*E*, *F*) следует вычислять, используя выражение:

$$MDT^{EF} = \int_{0}^{T} PFD^{E}(t) PFD^{F}(t)\,dt. \quad (Б.3)$$

Поэтому обычные вероятностные вычисления (посредством сложения и умножения) не действительны для PFD_{avg} вычислений (посредством интегрирования) параллельных компонентов. PFD_{avg} не обладает такими же свойствами, как истинная вероятность, и его ассимиляция с реальной вероятностью может привести к неадекватным результатам. В частности, невозможно получить PFD_{avg} Э/Э/ПЭ СБЗС системы, комбинируя традиционным способом $PFD_{avg,i}$ его компонентов. Поскольку это иногда поощряется коммерческими поставщиками булевых программных пакетов, аналитики должны быть предельно внимательными для того, чтобы избежать таких неадекватных вычислений, которые нежелательны при работе с безопасностью.

Пример — Для канала с избыточностью (1oo2) с интенсивностью опасных необнаруженных отказов λ_{DU} и интервалом между контрольными испытаниями τ расчет по некорректной вероятностной модели может дать $(\lambda_{DU} \cdot \tau)^2/4$, когда в действительности она должна быть равна $(\lambda_{DU} \cdot \tau)^2/3$.

Вычисления могут быть выполнены аналитически или с использованием метода Монте-Карло. В настоящем приложении описано, каким образом выполнить эти вычисления, используя общепринятые модели надежности, основанные на логических подходах (блок-схемы надежности или дерево отказов) или на моделях состояний-переходов (сети Маркова, сети Петри и т. д.).

Б.2.3 Режим работы Э/Э/ПЭ СБЗС системы с высокой интенсивностью запросов или с непрерывным запросом

Б.2.3.1 Общая формула PFH

Когда Э/Э/ПЭ СБЗС систему используют в режиме с высокой интенсивностью запросов или с непрерывным запросом, согласно настоящему стандарту необходимы вычисления значения средней частоты опасных отказов PFH. Это среднее значение так называемой безусловной интенсивности отказов (также именуемое частотой отказов) $w(t)$ за интересующий период вычисляют по формуле

$$\mathrm{PFH}(T) = \frac{1}{T}\int_0^T w(t)\,\mathrm{d}t. \qquad (Б.4)$$

Если Э/Э/ПЭ СБЗС система работает в режиме с непрерывным запросом и является основным средством обеспечения безопасности, то отказ всей СБЗС системы ведет непосредственно к потенциально опасной ситуации. Следовательно, при вычислениях можно считать, что отказы, приводящие к отказу ФБ всей системы, СБЗС система отказ не исправляет. Однако если отказ всей СБЗС системы не ведет непосредственно к потенциальной опасности при наличии других средств безопасности или к отказу оборудования, то возможно рассмотреть обнаружение отказа в СБЗС системе и ее ремонт при расчете снижения риска этой системой.

Б.2.3.2 Вероятность появления отказа (например, в случае единственного средства, работающего в режиме с непрерывным запросом)

Данный случай используют, когда Э/Э/ПЭ СБЗС система работает в режиме с непрерывным запросом и является основным средством обеспечения безопасности. Таким образом, непосредственно после ее отказа может возникнуть потенциально опасная ситуация. Ни один отказ всей системы не допустим в рассматриваемом периоде.

В этом случае средняя частота опасных отказов PFH может быть рассчитана с использованием вероятности появления отказа, деленной на величину рассматриваемого периода времени:

$$F(T):\quad \mathrm{PEF}(T) = \frac{1 - exp\left[-\int_0^T \Lambda(t)\,\mathrm{d}t\right]}{T} = \frac{F(T)}{T}. \qquad (Б.5)$$

Интенсивность полного отказа системы $\Lambda(t)$ может зависеть от времени или быть константой.

Если она зависит от времени, то среднюю частоту опасных отказов $\mathrm{PFH}(T)$ вычисляют по формуле

$$\mathrm{PFH}(T) = \frac{1 - exp\left[-\Lambda_{as} T\right]}{T} \approx \Lambda_{avg}. \qquad (Б.6)$$

Если система выполнена из компонентов, полностью и быстро восстанавливаемых, с постоянными интенсивностями отказов и ремонта (например, в случае обнаруживаемых опасных отказов), то $\Lambda(t)$ быстро достигает своего постоянного асимптотического значения Λ_{as}. Когда $\mathrm{PFH}(T) << 1$, значение $\mathrm{PFH}(T)$ вычисляют по формуле

$$\mathrm{PFH}(T) = \frac{1 - exp\left[-\Lambda_{as} T\right]}{T} \approx \Lambda_{avg} \approx \frac{1}{\mathrm{MTTF}}. \qquad (Б.7)$$

Асимптотическое значение Λ_{as} существует только тогда, когда Э/Э/ПЭ СБЗС система, работающая в непрерывном режиме, включает в себя только безопасные и *DD*-отказы (например, быстро обнаруживаемые и исправимые). Не рассматривают ремонт тех отказов, которые могут привести к полному отказу ФБ. Для конфигурации с резервированием, где применимы контрольные проверки, асимптотическая интенсивность отказов не применима, и должны быть использованы формулы (Б.4)—(Б.6). Выбор конкретного случая выполняет аналитик.

Б.2.3.3 Неготовность (например, при наличии нескольких средств обеспечения безопасности)

Когда Э/Э/ПЭ СБЗС система работает в режиме с непрерывным запросом и не является единственным средством обеспечения безопасности, отказы лишь увеличивают частоту запросов к другим средствам обеспечения безопасности, также как и тогда, когда она работает в режиме высокой интенсивности запросов и при этом в период ожидания запроса существует возможность выявить (автоматически или вручную) и устранить отказ, который может привести к непосредственному отказу ФБ. В этом случае отказы всей системы могут быть исправлены, и PFH может быть рассчитана исходя из значений готовности $A(t)$ и условной интенсивности отказа системы $\Lambda v(t)$.

Если система создана из компонентов, которые могут быть полностью и быстро исправлены (например, когда в любой ситуации, ведущей к ухудшению работы, существует большая вероятность быстро вернуть все в нормальное рабочее состояние), то ее $\Lambda v(t)$ быстро достигает асимптотического значения Λ_{vas}, которое в дополнение ко всему является неплохим приближением к действительной асимптоте интенсивности отказа всей системы Λ_{as}, введенной в Б.2.3.2.

В результате получают:

$$PFH = \frac{1}{MUT + MDT} = \frac{1}{MTBF} \approx \frac{1}{MUT} \approx \frac{1}{MTTF}. \quad (Б.8)$$

Б.2.3.4 Обсуждение интенсивности отказов

В формулах Б.6 и Б.8 используют интенсивность отказов всей системы $\Lambda(t)$, вычисление которой не очень простое, поэтому необходимо отметить нижеприведенные положения.

Для вычисления интенсивности отказов структуры, состоящей из последовательно соединенных компонентов, следует сложить интенсивности отказов каждого из компонентов. Исходя из блок-схемы, показанной на рисунке Б.1, интенсивность полного отказа Э/Э/ПЭ СБЗС системы можно вычислить по формуле

$$\Lambda(t) = \Lambda^{abc} + \lambda^{CCF1}(t) + \lambda^{d}(t) + \Lambda^{ef} + \lambda^{CCF2}(t), \quad (Б.9)$$

где $\Lambda(t)$ — интенсивность полного отказа Э/Э/ПЭ СБЗС системы.

$\Lambda^{ab}(t)$, $\lambda^{CCF1}(t)$, $\lambda^{d}(t)$, $\lambda^{ef}(t)$ и $\lambda^{CCF2}(t)$ — интенсивность отказов пяти минимальных сечений для Э/Э/ПЭ СБЗС системы.

Для параллельных структур все сложнее, так как в этом случае отсутствуют простые соотношения с интенсивностями отказов отдельных компонентов. Например, рассмотрим сечение (*E*, *F*):

- если *E* и *F* не могут быть мгновенно восстановлены (например, в случае *DU*-отказов), $\lambda^{EF}(t)$ изменяется непрерывно от 0 до λ (интенсивность отказов *E* или *F*). Асимптотическое значение достигается, когда один из двух компонентов откажет. Это довольно длительный процесс, т. к. это проявляется, когда *t* становится более $1/\lambda$. Данное значение не будет достигнуто, если *E* и *F* периодически проверяют с периодом $\tau \ll \frac{1}{\lambda}$;

- если *E* и *F* могут быть восстановлены в относительно короткий период времени (например, в случае *DD*-отказов), $\lambda^{EF}(t)$ очень быстро достигает асимптотического значения $\Lambda_{as}^{EF} = 2\Lambda^2/\mu$, которое может быть использовано как эквивалент постоянной интенсивности отказов. Это значение достигается, когда *t* становится в два-три раза больше, чем значения компонентов MTTR. Данный случай полностью и быстро восстанавливаемых систем описан в Б.2.3.2 и Б.2.3.3.

Таким образом, в общем случае оценка интенсивностей отказов всей системы требует более сложных вычислений, чем для более простой последовательной структуры.

Б.3 Метод блок-схемы надежности при постоянной интенсивности отказов

Б.3.1 Основная гипотеза

Расчеты основаны на следующих предположениях:

- значение результирующей средней вероятности отказа выполнения функции безопасности по запросу для системы менее 10^{-1} или значение результирующей средней частоты опасного отказа для системы менее 10^{-5} в час.

Примечание — Предположение означает, что такая Э/Э/ПЭ СБЗС система удовлетворяет требованиям ГОСТ 34332.2—2017 (см. таблицы 2 и 3) и УПБ 1;

- частота отказов компонентов постоянна в течение срока службы системы;
- подсистема датчиков (подсистема ввода) состоит из реального(ых) датчика(ов) и других компонентов и соединительных проводов вплоть до компонента(ов), но не включая его (их), где сигналы впервые объединяются с помощью процедуры голосования или другой процедуры (например, при конфигурации каналов из двух датчиков, представленной на рисунке Б.2).

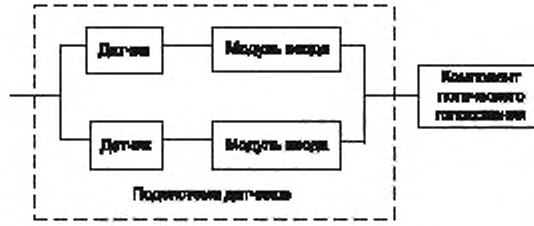


Рисунок Б.2 — Пример конфигурации для двух каналов датчиков

- логическая подсистема включает в себя компонент(ы), в котором(ых) сигналы вначале объединяются, и все другие компоненты вплоть до тех компонентов включительно, откуда результирующий(ие) сигнал(ы) передается(ются) подсистеме исполнительных элементов;

- подсистема исполнительных элементов (подсистема вывода) включает в себя компоненты и соединения, которые обрабатывают исполнительный(ые) сигнал(ы), получаемый(ые) от логической подсистемы, а также исполнительный(ые) компонент(ы);

- значения частот отказов АС, применяемых в качестве исходных данных для расчетов и таблиц, задаются для одного канала подсистемы (например, при использовании датчиков в виде архитектуры 2oo3 частота отказов задается для одного датчика, а влияние архитектуры 2oo3 рассчитывается дополнительно);

- значения частот отказов и охват диагностикой одинаковы для всех каналов в голосующей группе;

- общая частота отказов АС канала подсистемы является суммой значений частоты опасных и частоты безопасных отказов для данного канала, которые полагают равными.

Примечание — Это предположение влияет на долю безопасных отказов [см. ГОСТ 34332.3—2021 (приложение В)], но доля безопасных отказов не влияет на рассчитанные значения вероятности отказа, приведенные в данном приложении;

- для каждой ФБ существуют эффективные средства тестирования и устранения отказов (т. е. все отказы, оставшиеся невыявленными, обнаруживаются при тестировании), влияние неидеального тестирования в соответствии с Б.3.2.2.5;

- интервал времени между тестовыми испытаниями должен быть, по крайней мере, на порядок больше, чем MRT;

- для каждой подсистемы существует единый интервал времени между тестовыми испытаниями и MRT;

- ожидаемый интервал времени между запросами на выполнение ФБ должен быть, по крайней мере, на порядок больше интервала времени между тестовыми испытаниями;

- для всех подсистем, работающих в режиме с низкой интенсивностью запросов, и для архитектур 1oo2, 1oo2*D* и 1oo3, функционирующих в режиме с высокой интенсивностью запросов или с непрерывным запросом, доля отказов, заданная охватом диагностикой, обнаруживается и устраняется за MTTR, приведенное в требованиях к полноте безопасности АС.

Пример — Если предполагаемое MTTR равно 8 ч, то оно включает в себя продолжительность диагностического тестирования, которое обычно не превышает 1 ч, а оставшаяся часть среднего времени восстановления — это MRT.

Примечание — Для канальных архитектур 1oo2, 1oo2D и 1oo3 предполагается выполнение любого ремонта в оперативном режиме. Если конфигурация Э/Э/ПЭ СБЗС системы при любом обнаруживаемом отказе обеспечивает переход УО в безопасное состояние, то это уменьшает среднюю вероятность отказа при запросе. Степень уменьшения вероятности зависит от охвата диагностикой;

- для канальных архитектур 1oo1 и 2oo2, работающих в режиме с высокой интенсивностью запросов или с непрерывным запросом, Э/Э/ПЭ СБЗС система всегда переходит в безопасное состояние после обнаружения опасного отказа. Для этого ожидаемый интервал времени между запросами должен быть, по крайней мере, на порядок больше временного интервала диагностического тестирования или сумма временных интервалов диагностического тестирования и временных интервалов перехода УО в безопасное состояние должна быть меньше, чем время безопасной работы;

- если отказ источника питания приводит к обесточиванию Э/Э/ПЭ СБЗС системы и инициирует переход в безопасное состояние, то источник питания не влияет на среднюю вероятность отказа по запросу системы; если для перехода в безопасное состояние на систему подается питание или у источника питания существуют режимы отказов, которые могут приводить к небезопасной работе Э/Э/ПЭ СБЗС системы, то при оценке следует учитывать источник питания;

- если используется терминальный канал, то он ограничивается лишь той частью рассматриваемой системы, которой обычно является либо датчик, либо логическая подсистема, либо подсистема логических элементов;
- параметры и их обозначения представлены в таблице Б.1.

Таблица Б.1 — Параметры, используемые в настоящем приложении, и диапазоны их значений (применяются к архитектурам 1oo1, 1oo2, 2oo2, 1oo2*D* и 2oo3)

Обозначение	Параметр, единица измерения	Диапазон параметров в соответствии с таблицами Б.2—Б.5 и Б.10 – Б.13
T_1	Интервал времени между контрольными проверками, ч	1 мес (730 ч)[1]. 3 мес (2190 ч)[1]. 6 мес (4380 ч). 1 год (8760 ч). 2 года (17 520 ч)[2]. 10 лет (87 600 ч)[2]
MRT	Среднее время ремонта, ч	8 Примечание — MTTR =MRT = 8 ч основано на предположении, что время на обнаружение опасного отказа, основанное на автоматическом обнаружении,<< MRT
MTTR	Среднее время восстановления, ч	8 Примечание — MTTR = MRT = 8 ч основано на предположении, что время на обнаружение опасного отказа, основанное на автоматическом обнаружении, << MRT
DC	Охват диагностикой, дробь (в формулах), % (в остальных случаях)	0 %; 60 %; 90 %; 99 %
β	Доля необнаруженных отказов по общей причине (в таблицах Б.2—Б.5 и Б.10—Б.13 предполагается $\beta = 2 \cdot \beta_D$), дробь (в формулах), % (в остальных случаях)	2 %; 10 %; 20 %
β_D	Доля отказов, обнаруженных диагностическими тестами и имеющих общую причину (в таблицах Б.2—Б.5 и Б.10—Б.13 предполагается $\beta = 2 \cdot \beta_D$), дробь (в формулах), % (в остальных случаях)	1 %; 5 %; 10 %
λ_{ou}	Интенсивность опасных отказов для канала подсистемы, отказ/ч	$0{,}05 \cdot 10^{-6}$; $0{,}25 \cdot 10^{-6}$; $0{,}5 \cdot 10^{-6}$; $2{,}5 \cdot 10^{-6}$; $5 \cdot 10^{-6}$; $25 \cdot 10^{-6}$
PFD_G	Средняя вероятность отказа по запросу для группы голосующих каналов (если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входит в состав только одной голосующей группы, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно)	—
PFD_S	Средняя вероятность отказа по запросу для подсистемы датчиков	—
PFD_L	Средняя вероятность отказа по запросу для логической подсистемы	—
$PFDF_E$	Средняя вероятность отказа по запросу для подсистемы исполнительных элементов	—
PFD_{SYS}	Средняя вероятность отказа по запросу для функции безопасности Э/Э/ПЭ СБЗС системы	—

Окончание таблицы Б.1

Обозначение	Параметр, единица измерения	Диапазон параметров в соответствии с таблицами Б.2—Б.5 и Б.10—Б.13
PFH_G	Средняя частота опасных отказов для группы голосующих каналов (если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входит в состав только одной голосующей группы, то PFH_G эквивалентна PFH_S, PFH_L или PFH_{FE} соответственно), отказ/ч	—
PFH_S	Средняя частота опасных отказов для подсистемы датчиков, отказ/ч	—
PFH_L	Средняя частота опасных отказов для логической подсистемы, отказ/ч	—
PFH_{FE}	Средняя частота опасных отказов для подсистемы исполнительных элементов, отказ/ч	—
PFH_{SYS}	Средняя частота опасных отказов для функции безопасности Э/Э/ПЭ СБЗС системы, отказ/ч	—
λ	Общая интенсивность отказов для канала подсистемы, отказ/ч	—
λ_D	Интенсивность опасных отказов для канала подсистемы, равная 0,5λ (в предположении 50 % опасных отказов и 50 % безопасных отказов), отказ/ч	—
λ_{DD}	Интенсивность обнаруженных опасных отказов для канала подсистемы (это сумма всех интенсивностей обнаруженных опасных отказов для канала подсистемы), отказ/ч	—
λ_{DU}	Интенсивность необнаруженных опасных отказов для канала подсистемы (это сумма всех интенсивностей необнаруженных опасных отказов для канала подсистемы), отказ/ч	—
λ_{SD}	Интенсивность обнаруженных безопасных отказов для канала подсистемы (это сумма всех интенсивностей обнаруженных безопасных отказов для канала подсистемы), отказ/ч	—
t_{CE}	Эквивалентное среднее время простоя канала для архитектур 1oo1, 1oo2, 2oo2 и 2oo3 (это объединенное время простоя для всех компонентов канала подсистемы), ч	—
t_{GE}	Эквивалентное среднее время простоя голосующей группы для архитектур 1oo1, 1oo2, 2oo2 и 2oo3 (это объединенное время простоя для всех каналов в голосующей группе), ч	—
t_{CE}'	Эквивалентное среднее время простоя канала для архитектуры 1oo2D (это объединенное время простоя для всех компонентов канала подсистемы), ч	—
t_{GE}'	Эквивалентное среднее время простоя голосующей группы для архитектуры 1oo2D (это суммарное время простоя для всех каналов в голосующей группе), ч	—
T_2	Интервал времени между запросами, ч	—
K	Доля успеха при автоматическом тестировании схемы в 1oo2D системе	—
PTC	Охват контрольными проверками	—
[1] Только режим высокой интенсивности запросов и режим с непрерывным запросом. [2] Только режим низкой интенсивности запросов.		

Б.3.2 Средняя вероятность отказа по запросу (для режима с низкой интенсивностью запросов)

Б.3.2.1 Процедура расчета

Среднюю вероятность отказа ФБ для Э/Э/ПЭ СБЗС системы определяют посредством вычисления и объединения средних вероятностей отказов по запросу для всех подсистем, совокупность которых обеспечивает ФБ. Так как рассматриваемые в настоящем приложении вероятности невелики, то средняя вероятность отказа по запросу для ФБ Э/Э/ПЭ СБЗС системы (см. рисунок Б.3) PFD_{SYS} может быть вычислена по формуле

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}. \quad (Б.10)$$



Рисунок Б.3 — Структура подсистем Э/Э/ПЭ СБЗС системы

Для определения средней вероятности отказа по запросу для каждой из подсистем необходимо строго придерживаться следующей процедуры для каждой подсистемы:

- разработка структурной схемы, изображающей компоненты подсистемы датчиков (подсистемы ввода), компоненты логической подсистемы или компоненты подсистемы исполнительных элементов (подсистемы вывода). Компонентами подсистемы датчиков, например, могут быть датчики, защитные экраны, входные согласующие цепи; компонентами логической подсистемы — процессоры и сканеры, а компонентами подсистемы исполнительных элементов — выходные согласующие цепи, экраны и исполнительные механизмы. Каждую подсистему представляют как одну либо более голосующих групп 1oo1, 1oo2, 2oo2, 1oo2*D* или 2oo3;
- применение соответствующих таблиц Б.2—Б.5, в которых приведены шестимесячные, годовые, двухлетние и 10-летние интервалы между процедурами тестирования. Данные таблицы предполагают, что среднее время восстановления для любого отказа после его обнаружения равно 8;
- для каждой голосующей группы в подсистеме осуществление выбора из таблиц Б.2—Б.5:

а) архитектуры (например, 2oo3),

б) охвата диагностикой для каждого канала (например, 60 %),

в) интенсивности опасных отказов в час, λ_D для каждого канала (например, $2,5 \cdot 10^{-6}$),

г) факторов отказа по общей причине β-факторов (β и β_D) для взаимосвязи между каналами в рассматриваемой архитектуре (например, 2 % и 1 % соответственно).

Примечания

1 Предполагается, что все каналы в голосующей группе имеют одинаковые охват диагностикой и интенсивность отказов (см. Б.1).

2 В таблицах Б.2—Б.5 (см. также таблицы Б.10—Б.13) предполагается, что β-фактор в отсутствие диагностических тестов (также применяемый для необнаруженных опасных отказов при использовании диагностических тестов) в два раза больше β-фактора для отказов, обнаруживаемых диагностическими тестами β_D;

- получение исходя из данных таблиц Б.2—Б.5 средней вероятности отказа для голосующей группы;
- если функция безопасности зависит от нескольких голосующих групп датчиков или исполнительных элементов, то совокупную среднюю вероятность отказа для подсистемы датчиков или подсистемы исполнительных элементов PFD_S или PFD_{FE} вычисляют по следующим формулам:

$$PFD_S = \sum_i PFD_{Gi}; \text{ и } PFD_{FE} = \sum_j PFD_{Gj}, \quad (Б.11)$$

где PFD_{Gi} и PFD_{Gj} — средние вероятности отказа для каждого из голосующей группы датчиков или исполнительных элементов, соответственно.

Эти формулы используют во всех уравнениях как для PFD, так и для интенсивности отказов системы, которые являются функцией интенсивности отказов компонентов и среднего времени простоя MDT. Если система состоит из нескольких элементов и требуется определить общую PFD комбинации всех элементов или интенсивность отказов системы, то при вычислениях обычно применяют единое значение MDT. Однако каждый элемент может иметь различные механизмы обнаружения отказов с разными MDT, и разные элементы могут иметь разные MDT для одних и тех же механизмов обнаружения отказов. В этом случае необходимо вычислить единое значение MDT, которое отражает все элементы в цепочке. Это можно выполнить, рассматривая полные цепочки интенсивности от-

казов всей системы и пропорционально распределяя индивидуальные значения MDT для элементов в соответствии с вкладом их интенсивностей отказов в общую интенсивность отказов.

Например, при наличии двух элементов в последовательности, один с интервалом между контрольными проверками T_1, а другой с интервалом между контрольными проверками T_2, эквивалентное единое значение для *MDT* вычисляют по формулам:

$$\lambda_T = \lambda_1 + \lambda_2; \tag{Б.12}$$

$$\mathrm{MDT}_E = \frac{\lambda_1}{\lambda_T}\left(\frac{T_1}{2}\right) + \frac{\lambda_2}{\lambda_T}\left(\frac{T_2}{2}\right). \tag{Б.13}$$

Б.3.2.2 Архитектуры для режима с низкой интенсивностью запросов

Примечания

1 В настоящем пункте справедливые для нескольких архитектур формулы приводят в том случае, если их используют впервые.

2 Формулы настоящего пункта справедливы для предположений, перечисленных в Б.3.1.

3 Приведенные примеры являются типичными конфигурациями и не являются исчерпывающими.

Б.3.2.2.1 Архитектура 1oo1

Данная архитектура предполагает использование одного канала, и любой опасный отказ приводит к нарушению ФБ при возникновении запроса на ее выполнение.

На рисунках Б.4 и Б.5 представлены соответствующие структурные схемы. Интенсивность опасного отказа для канала λ_D вычисляют по формуле

$$\lambda_D = \lambda_{DU} + \lambda_{DD}. \tag{Б.14}$$



Рисунок Б.4 — Структурная схема архитектуры 1oo1

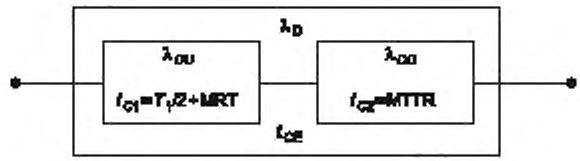


Рисунок Б.5 — Структурная схема надежности для архитектуры 1oo1

На рисунке Б.5 показано, что канал можно рассматривать как состоящий из двух компонентов: один — с интенсивностью опасных отказов λ_{DU}, обусловленной необнаруженными отказами, а другой — с интенсивностью опасных отказов λ_{DD}, обусловленной обнаруженными отказами. Эквивалентное среднее время простоя канала t_{GE} можно рассчитать, суммируя времена простоя для двух компонентов t_{C1} и t_{C2}, прямо пропорционально вкладу каждого компонента в вероятность отказа канала, по формуле

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \mathrm{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\mathrm{MRT}, \tag{Б.15}$$

Для каждой архитектуры интенсивность необнаруженных опасных отказов λ_{DU} и интенсивность обнаруженных опасных отказов λ_{DD} определяют следующим образом:

$$\lambda_{DU} = \lambda_D(1-DC); \quad (Б.16)$$

$$\lambda_{DD} = \lambda_D DC. \quad (Б.17)$$

Среднюю вероятность отказа выполнения функции безопасности канала PFD в течение времени простоя t_{CE} определяют исходя из выражения:

$$PFD = 1 - e^{-\lambda_D t_{CE}} \approx \lambda_D t_{CE} \ll 1. \quad (Б.18)$$

Следовательно, среднюю вероятность отказа по запросу для архитектуры 1oo1 PFD_S вычисляют по формуле

$$PFD_S = (\lambda_{DU} + \lambda_{DD}) t_{CE}. \quad (Б.19)$$

Б.3.2.2.2 Архитектура 1oo2

Данная архитектура представляет собой два канала, соединенных параллельно, где любой из каналов может выполнить ФБ. Следовательно, для нарушения ФБ опасные отказы должны возникнуть в обоих каналах. Предполагается, что любое диагностическое тестирование только сообщает о найденных сбоях и не может изменить ни выходные состояния каналов, ни результат голосования.

На рисунках Б.6 и Б.7 представлены соответствующие структурные схемы. Значение t_{CE} вычисляют в соответствии с Б.3.2.2.1, но необходимо вычислить также и эквивалентное время простоя системы t_{GE} по формуле

$$\lambda_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR. \quad (Б.20)$$

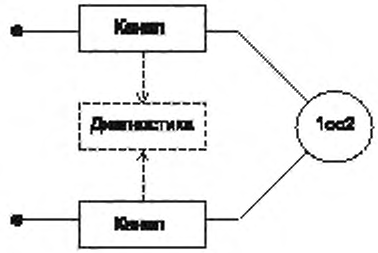


Рисунок Б.6 — Структурная схема архитектуры 1oo2

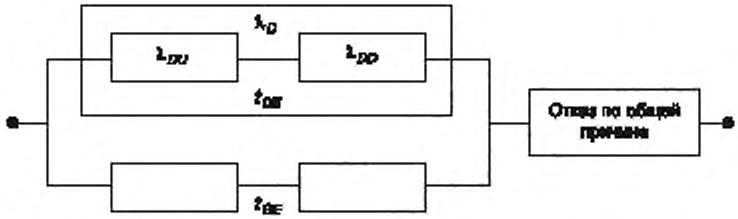


Рисунок Б.7 — Структурная схема надежности для архитектуры 1oo2

Для данной архитектуры средняя вероятность отказа по запросу PFD_G равна:

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right). \quad (Б.21)$$

Б.3.2.2.3 Архитектура 2oo2

Данная архитектура представляет собой два канала, соединенных параллельно, и для выполнения функции безопасности необходима работа обоих каналов. Предполагается, что любое диагностическое тестирование только сообщает об обнаруженных сбоях и не может изменить ни выходные состояния каналов, ни результат голосования.

На рисунках Б.8 и Б.9 представлены соответствующие структурные схемы. Значение t_{CE} вычисляют в соответствии с Б.3.2.2.1, а среднюю вероятность отказа по запросу PFD_G для данной архитектуры определяют как:

$$PFD_G = 2\lambda_D t_{CE}. \quad (Б.22)$$

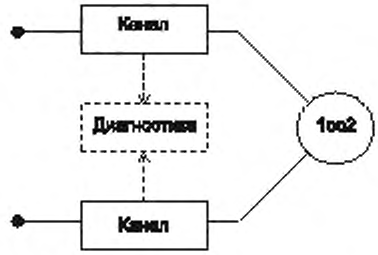


Рисунок Б.8 — Структурная схема архитектуры 2oo2

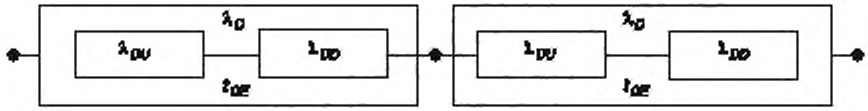


Рисунок Б.9 — Структурная схема надежности для архитектуры 2oo2

Б.3.2.2.4 Архитектура 1oo2*D*

Данная архитектура представляет собой два канала, соединенных параллельно. При нормальной работе для выполнения функции безопасности по запросу необходимы оба канала. Кроме того, если диагностическое тестирование обнаруживает отказ в любом канале, то результаты анализа устанавливаются таким образом, чтобы общее выходное состояние совпадало с результатом, выдаваемым другим каналом. Если диагностическое тестирование обнаруживает отказы в обоих каналах или несоответствие между ними, причина которого не может быть идентифицирована, то выходной сигнал переводит систему в безопасное состояние. Для обнаружения несоответствия между каналами каждый канал может определять состояние другого канала не зависящим от другого канала способом. Сравнение канала/механизма переключения не может быть эффективным на 100 %, поэтому параметр *K* представляет собой эффективность межканального сравнения/механизма переключения, т. е. выход может оставаться таким же, как и для архитектуры 2oo2, даже если в одном из каналов обнаружен отказ.

Примечание — Параметр *K* следует определить с помощью анализа причин и последствий отказов FMEA (от английского «failure modes and effects analysis»).

Для каждого канала интенсивность обнаруженных безопасных отказов λ_{SD} определяют как:

$$\lambda_{SD} = \lambda_S DC. \quad (Б.23)$$

На рисунках Б.10 и Б.11 представлены соответствующие структурные схемы. Значения эквивалентного среднего времени простоя отличаются от значений, приведенных для других архитектур в Б.3.2.2, поэтому их обозначают как t_{CE} и t_{GE} и вычисляют по следующим формулам:

$$t_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + \text{MRT}\right) + \left(\lambda_{DD} + \lambda_{SD}\right)\text{MTTR}}{\lambda_{DU} + \left(\lambda_{DD} + \lambda_{SD}\right)}; \quad (Б.24)$$

$$t_{GE}' = \frac{T_1}{2} + \text{MRT}. \qquad (Б.25)$$

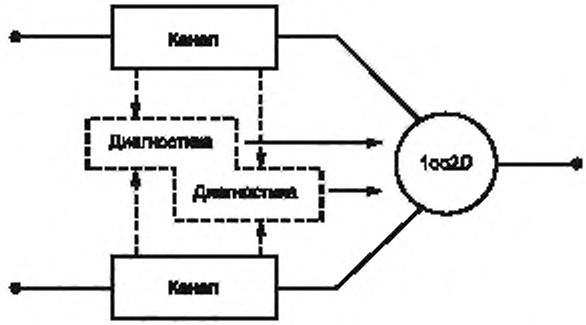


Рисунок Б.10 — Структурная схема архитектуры 1oo2*D*

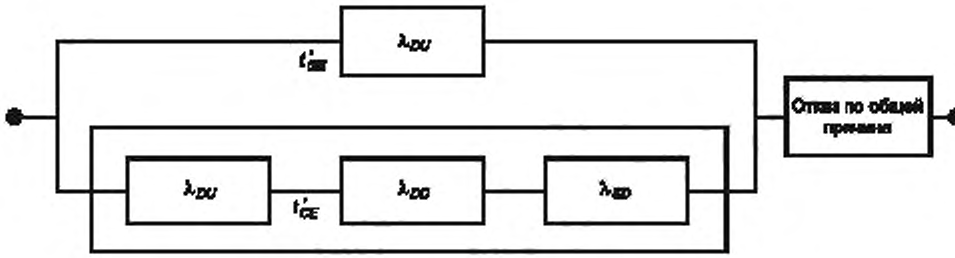


Рисунок Б.11 — Структурная схема надежности для архитектуры 1oo2*D*

Среднюю вероятность отказа по запросу PFD_G для данной архитектуры вычисляют по формуле

$$\text{PFD}_\text{G} = 2(1-\beta)\lambda_{DU}\left((1-\beta)\lambda_{DU} + \left(1-\beta_D\right)\lambda_{DD} + \lambda_{SD}\right)t_{CE}' + 2(1-K)\lambda_{DD}t_{CE}' + \beta\lambda_{DU}\left(\frac{T_1}{2} + \text{MRT}\right). \qquad (Б.26)$$

Б.3.2.2.5 Архитектура 2oo3

Данная архитектура состоит из трех каналов, соединенных параллельно с мажорированием выходных сигналов таким образом, что выходное состояние не меняется, если результат, выдаваемый одним из каналов, отличается от результата, выдаваемого двумя другими каналами.

Предполагается, что любое диагностическое тестирование только фиксирует найденные сбои и не может изменить ни выходные состояния каналов, ни результат голосования.

На рисунках Б.12 и Б.13 представлены соответствующие структурные схемы. Значение t_{CE} вычисляют по Б.3.2.2.1, а значение t_{GE} — по Б.3.2.2.2. Среднюю вероятность отказа по запросу PFD_G для данной архитектуры вычисляют по формуле

$$\text{PFD}_\text{G} = 6\left(\left(1-\beta_D\right)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE}t_{GE} + \beta_D\lambda_{DD}\text{MTTR} + \beta\lambda_{DU}\left(\frac{T_1}{2} + \text{MRT}\right). \qquad (Б.27)$$

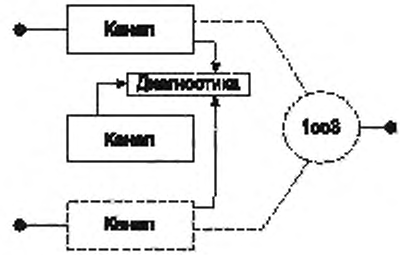


Рисунок Б.12 — Структурная схема архитектуры 2oo3

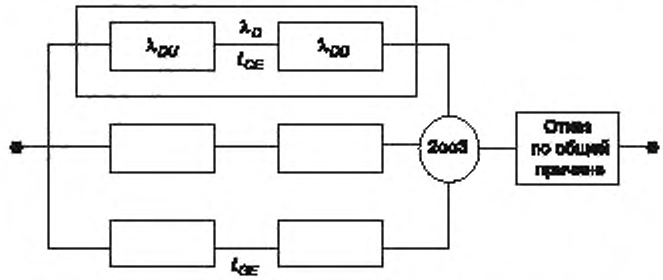


Рисунок Б.13 — Структурная схема надежности для архитектуры 2oo3

Б.3.2.2.6 Архитектура 1oo3

Данная архитектура состоит из трех каналов, соединенных параллельно со схемой голосования для выходных сигналов, так что выходной сигнал соответствует схеме голосования 1oo3.

Предполагается, что любая диагностическая проверка только сообщает о найденных отказах и не меняет выходных состояний или выхода схемы голосования.

Значение t_{CE} вычисляют по Б.3.2.2.1, а значение t_{GE} — по Б.3.2.2.2. Средняя вероятность отказа по запросу PFD_G для данной архитектуры равна

$$PFD_G = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} \text{MTTR} + \beta\lambda_{DU}\left(\frac{T_1}{2} + \text{MRT}\right),$$

где $t_{G2E} = \frac{\lambda_{GU}}{\lambda_D}\left(\frac{T_1}{4} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}.$

Б.3.2.3 Подробные таблицы для режима с низкой интенсивностью запросов

Значения средних вероятностей отказов по запросу для различных интервалов между контрольными испытаниями при среднем времени ремонта 8 ч представлены в таблицах Б.2—Б.5.

Примечание — В таблицах Б.2—Б.5 «E» означает основание степенной функции (число 10), а последующие знаки и числа (например, «-06», «00», «02») — показатели степени. Таким образом, «E-06» означает «10^{-6}», «E-00» — «10^0», а «E02» — «10^2».

Таблица Б.2 — Средняя вероятность отказа по запросу для шестимесячного интервала между контрольными проверками при среднем времени ремонта 8 ч

Архитектура	DC, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0	1,1E-04			5,5E-04			1,1E-03		
	60	4,4E-05			2,2E-04			4,4E-04		
	90	1,1E-05			5,7E-05			1,1E-04		
	99	1,5E-06			7,5E-06			1,5E-05		
1oo2	0	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	90	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo2 (см. примечание 2)	0	2,2E-04			1,1E-03			2,2E-03		
	60	8,8E-05			4,4E-04			8,8E-04		
	90	2,3E-05			1,1E-04			2,3E-04		
	99	3,0E-06			1,5E-05			3,0E-05		
1oo2D (см. примечание 3)	0	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60	1,4E-06	4,9E-06	9,3E-06	7,1E-06	2,5E-05	4,7E-05	1,4E-05	5,0E-05	9,3E-05
	90	4,3E-07	1,3E-06	2,4E-06	2,2E-06	6,6E-06	1,2E-05	4,3E-06	1,3E-05	2,4E-05
	99	6,0E-08	1,5E-07	2,6E-07	3,0E-07	7,4E-07	1,3E-06	6,0E-07	1,5E-06	2,6E-06
2oo3	0	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,6E-05	1,1E-04	2,7E-05	1,1E-04	2,2E-04
	60	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	90	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo3	0	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04
	60	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	90	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo1 (см. примечание 2)	0	5,5E-03			1,1E-02			5,5E-02		
	60	2,2E-03			4,4E-03			2,2E-02		
	90	5,7E-04			1,1E-03			5,7E-03		
	99	7,5E-05			1,5E-04			7,5E-04		
1oo2	0	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	90	1,2E-05	5,6E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04	1,5E-04	6,0E-04	1,2E-03
	99	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,4E-05	6,6E-05	1,3E-04
2oo2 (см. примечание 2)	0	1,1E-02			2,2E-02			> 1E-01		
	60	4,4E-03			8,8E-03			4,4E-02		
	90	1,1E-03			2,3E-03			1,1E-02		
	99	1,5E-04			3,0E-04			1,5E-03		
1oo2D (см. примечание 3)	0	1,5E-04	5,8E-04	1,1E-03	3,8E-04	1,2E-03	2,3E-03	5,0E-03	9,0E-03	1,4E-02
	60	7,7E-05	2,5E-04	4,7E-04	1,7E-04	5,2E-04	9,5E-04	1,3E-03	3,0E-03	5,1E-03
	90	2,2E-05	6,6E-05	1,2E-04	4,5E-05	1,3E-04	2,4E-04	2,6E-04	6,9E-04	1,2E-03
	99	3,0E-06	7,4E-06	1,3E-05	6,0E-06	1,5E-05	2,6E-05	3,0E-05	7,4E-05	1,3E-04

Окончание таблицы Б.2

Архитектура	DC, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0	2,3E-04	6,5E-04	1,2E-03	6,8E-04	1,5E-03	2,5E-03	1,3E-02	1,5E-02	1,9E-02
	60	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,3E-03	3,9E-03	5,9E-03
	90	1,2E-05	5,7E-05	1,1E-04	2,7E-05	1,2E-04	2,3E-04	2,4E-04	6,8E-04	1,2E-03
	99	1,3E-06	6,5E-06	1,3E-05	2,7E-06	1,3E-05	2,6E-05	1,5E-05	6,7E-05	1,3E-04
1oo3	0	1,1E-04	5,5E-04	1,1E-03	2,2E-04	1,1E-03	2,2E-03	1,4E-03	5,7E-03	1,1E-02
	60	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	90	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и $K = 0{,}98$.

Таблица Б.3 — Средняя вероятность отказа по запросу для одногодичного интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	DC, %	λ_D = 0 5E-07			λ_D = 2 5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0	2,2E-04			1,1E-03			2,2E-03		
	60	8,8E-05			4,4E-04			8,8E-04		
	90	2,2E-05			1,1E-04			2,2E-04		
	99	2,6E-06			1,3E-05			2,6E-05		
1oo2	0	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60	1,8E-06	8,8E-06	1,8E-05	9,0E-06	4,4E-05	8,8E-05	1,9E-05	8,9E-05	1,8E-04
	90	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
	99	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
2oo2 (см. примечание 2)	0	4,4E-04			2,2E-03			4,4E-03		
	60	1,8E-04			8,8E-04			1,8E-03		
	90	4,5E-05			2,2E-04			4,5E-04		
	99	5,2E-06			2,6E-05			5,2E-05		
1oo2*D* (см. примечание 3)	0	4,5E-06	2,2E-05	4,4E-05	2,4E-05	1,1E-04	2,2E-04	5,OE-05	2,2E-04	4,4E-04
	60	2,8E-06	9,8E-06	1,9E-05	1,4E-05	4,9E-05	9,3E-05	2,9E-05	9,9E-05	1,9E-04
	90	8,5E-07	2,6E-06	4,8E-06	4,3E-06	1,3E-05	2,4E-05	8,5E-06	2,6E-05	4,8E-05
	99	1,0E-07	2,8E-07	5,0E-07	5,2E-07	1,4E-06	2,5E-06	1,OE-06	2,8E-06	5,OE-06

Окончание таблицы Б.3

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-08		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,2E-05	2,4E-04	4,5E-04
	60	1,8E-06	8,8E-06	1,8E-05	9,5E-06	4,5E-05	8,8E-05	2,1E-05	9,1E-05	1,8E-04
	90	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1 E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
	99	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo3	0	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	60	1,8E-06	8,8E-06	1,8E-05	8,8E-06	4,4E-05	8,8E-05	1,8E-05	8,8E-05	1,8E-04
	90	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo1 (см. примечание 2)	0	1,1E-02			2,2E-02			>1E-01		
	60	4,4E-03			8,8E-03			4,4E-02		
	90	1,1E-03			2,2E-03			1,1E-02		
	99	1,3E-04			2,6E-04			1,3E-03		
1oo2	0	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60	1,1E-04	4,6E-04	9,0E-04	2,8E-04	9,7E-04	1,8E-03	3,4E-03	6,6E-03	1,1E-02
	90	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
	99	2,4E-06	1,2E-05	2,4E-05	4,9E-06	2,4E-05	4,8E-05	2,6E-05	1,2E-04	2,4E-04
2oo (см. примечание 2)	0	2,2E-02			4,4E-02			>1E-01		
	60	8,8E-03			1,8E-02			8,8E-02		
	90	2,2E-03			4,5E-03			2,2E-02		
	99	2,6E-04			5,2E-04			2,6E-03		
1oo2*D* (см. примечание 3)	0	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,9E-03	1,8E-02	2,5E-02	3,4E-02
	60	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03	3,9E-03	7,1E-03	1,1E-02
	90	4,4E-05	1,3E-04	2,4E-04	9,1E-05	2,7E-04	4,8E-04	5,8E-04	1,4E-03	2,5E-03
	99	5,2E-06	1,4E-05	2,5E-05	1,0E-05	2,8E-05	5,0E-05	5,4E-05	1,4E-04	2,5E-04
2oo3	0	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,8E-03	5,6E-03	4,8E-02	5,0E-02	5,3E-02
	60	1,6E-04	5,1E-04	9,4E-04	4,8E-04	1,1E-03	2,0E-03	8,4E-03	1,1E-02	1,5E-02
	90	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
	99	2,5E-06	1,2E-05	2,4E-05	5,1E-06	2,4E-05	4,8E-05	3,1E-05	1,3E-04	2,5E-04
1oo3	0	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,7E-02	1,3E-02	2,3E-02
	60	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03	1,0E-03	4,5E-03	8,9E-03
	90	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03
	99	2,4E-06	1,2E-05	2,4E-05	4,8E-06	2,4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и $K = 0,98$.

Таблица Б.4 — Средняя вероятность отказа по запросу для двухлетнего интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0	4,4E-04			2,2E-03			4,4E-03		
	60	1,8E-04			8,8E-04			1,8E-03		
	90	4,4E-05			2,2E-04			4,4E-04		
	99	4,8E-06			2,4E-05			4,8E-05		
1oo2	0	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60	3,5E-06	1,8E-05	3,5E-05	1,9E-05	8,9E-05	1,8E-04	3,9E-05	1,8E-04	3,5E-04
	90	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	99	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
2oo2 (см. примечание 2)	0	8,8E-04			4,4E-03			8,8E-03		
	60	3,5E-04			1,8E-03			3,5E-03		
	90	8,8E-05			4,4E-04			8,8E-04		
	99	9,6E-06			4,8E-05			9,6E-05		
1oo2*D* (см. примечание 3)	0	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	9,0E-04
	60	5,7E-06	2,0E-05	3,7E-05	2,9E-05	9,9E-05	1,9E-04	6,0E-05	2,0E-04	3,7E-04
	90	1,7E-06	5,2E-06	9,6E-06	8,5E-06	2,6E-05	4,8E-05	1,7E-05	5,2E-05	9,6E-05
	99	1,9E-07	5,4E-07	9,8E-07	9,5E-07	2,7E-06	4,9E-06	1,9E-06	5,4E-06	9,8E-06
2oo3	0	9,5E-06	4,4E-05	8,8E-05	6,2E-05	2,3E-04	4,5E-04	1,6E-04	5,0E-04	9,3E-04
	60	3,6E-06	1,8E-05	3,5E-05	2,1E-05	9,0E-05	1,8E-04	4,?E-05	1,9E-04	3,6E-04
	90	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	99	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,3E-07	4,6E-06	9,2E-06
1oo3	0	8,8E-06	4,4E-05	8,8E-05	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04
	60	3,5E-06	1,8E-05	3,5E-05	1,8E-05	8,8E-05	1,8E-04	3,5E-05	1,8E-04	3,5E-04
	90	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
1oo1 (см. примечание 2)	0	2,2E-02			4,4E-02			>1E-01		
	60	8,8E-03			1,8E-02			8,8E-02		
	90	2,2E-03			4,4E-03			2,2E-02		
	99	2,4E-04			4,8E-04			2,4E-03		
1oo2	0	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60	2,8E-04	9,7E-04	1,8E-03	7,5E-04	2,1E-03	3,8E-03	1,2E-02	1,8E-02	2,5E-02
	90	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	99	4,7E-06	2,3E-05	4,6E-05	9,5E-06	4,6E-05	9,2E-05	5,4E-05	2,4E-04	4,6E-04

Окончание таблицы Б.4

Архитектура	DC, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo2 (см. примечание 2)	0	4,4E-02			8,8E-02			>1E-01		
	60	1,8E-02			3,5E-02			>1E-01		
	90	4,4E-03			8,8E-03			4,4E-02		
	99	4,8E-04			9,6E-04			4,8E-03		
1oo2*D* (см. примечание 3)	0	1,1E-03	2,7E-03	4,8E-03	3,4E-03	6,6E-03	1,1E-02	6,7E-02	7,7E-02	9,0E-02
	60	3,8E-04	1,1E-03	1,9E-03	9,6E-04	2,3E-03	4,0E-03	1,3E-02	1,9E-02	2,6E-02
	90	9,0E-05	2,6E-04	4,8E-04	1,9E-04	5,4E-04	9,8E-04	1,5E-03	3,2E-03	5,3E-03
	99	9,6E-06	2,7E-05	4,9E-05	1,9E-05	5,4E-05	9,8E-05	1,0E-04	2,8E-04	5,0E-04
2oo3	0	2,3E-03	3,7E-03	5,6E-03	8,3E-03	1,1E-02	1,4E-02	1,9E-01	1,8E-01	1,7E-01
	60	4,8E-04	1,1E-03	2,0E-03	1,6E-03	2,8E-03	4,4E-03	3,2E-02	3,5E-02	4,0E-02
	90	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1 E-04	9,4E-04	2,4E-03	4,0E-03	6,0E-03
	99	4,8E-06	2,3E-05	4,6E-05	1,0E-05	4,7E-05	9,2E-05	6,9E-05	2,5E-04	4,8E-04
1oo3	0	4,6E-04	2,2E-03	4,4E-03	1,0E-03	4,5E-03	8,9E-03	2,4E-02	3,7E-02	5,5E-02
	60	1,8E-04	8,8E-04	1,8E-03	3,6E-04	1,8E-03	3,5E-03	3,1E-03	9,9E-03	1,8E-02
	90	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	99	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и $K = 0,98$.

Таблица Б.5 — Средняя вероятность отказа по запросу для десятилетнего интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0	2,2E-03			1,1E-02			2,2E-02		
	60	8,8E-04			4,4E-03			8,8E-03		
	90	2,2E-04			1,1E-03			2,2E-03		
	99	2,2E-05			1,1E-04			2,2E-04		
1oo2	0	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60	1,9E-05	8,9E-05	1,8E-04	1,1E-04	4,6E-04	9,0E-04	2,7E-04	9,6E-04	1,8E-03
	90	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	99	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
2oo2 (см. примечание 2)	0	4,4E-03			2,2E-02			4,4E-02		
	60	1,8E-03			8,8E-03			1,8E-02		
	90	4,4E-04			2,2E-03			4,4E-03		
	99	4,5E-05			2,2E-04			4,5E-04		
1oo2*D* (см. примечание 3)	0	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60	2,9E-05	9,9E-05	1,9E-04	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03
	90	8,4E-06	2,6E-05	4,8E-05	4,3E-05	1,3E-04	2,4E-04	9,0E-05	2,6E-04	4,8E-04
	99	8,9E-07	2,6E-06	4,8E-06	4,5E-06	1,3E-05	2,4E-05	8,9E-06	2,6E-05	4,8E-05
2oo3	0	6,2E-05	2,3E-04	4,5E-04	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,7E-03	5,6E-03
	60	2,1E-05	9,0E-05	1,8E-04	1,6E-04	5,0E-04	9,3E-04	4,7E-04	1,1E-03	2,0E-03
	90	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,3E-05	2,4E-04	4,5E-04
	99	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
1oo3	0	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03
	60	1,8E-05	8,8E-05	1,8E-04	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03
	90	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	99	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
1oo1 (см. примечание 2)	0	>1E-01			>1E-01			>1E-01		
	60	4,4E-02			8,8E-02			>1E-01		
	90	1,1E-02			2,2E-02			>1E-01		
	99	1,1E-03			2,2E-03			1,1E-02		
1oo2	0	1,8E-02	2,4E-02	3,2E-02	6,6E-02	7,4E-02	8,5E-02	>1E-01	>1E-01	>1E-01
	60	3,4E-03	6,6E-03	1,1E-02	1,2E-02	1,8E-02	2,5E-02	>1E-01	>1E-01	>1E-01
	90	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,8E-03	4,9E-03	1,8E-02	2,5E-02	3,5E-02
	99	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03

Окончание таблицы Б.5

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo2 (см. примечание 2)	0	>1E-01			>1E-01			>1E-01		
	60	8,8E-02			>1E-01			>1E-01		
	90	2,2E-02			4,4E-02			>1E-01		
	99	2,2E-03			4,5E-03			2,2E-02		
1oo2*D* (см. примечание 3)	0	1,8E-02	2,5E-02	3,3E-02	6,6E-02	7,7E-02	9,0E-02	1,6E+00	1,5E+00	1,4E+00
	60	3,9E-03	7,1E-03	1,1E-02	1,3E-02	1,9E-02	2,6E-02	2,6E-01	2,7E-01	2,8E-01
	90	5,7E-04	1,4E-03	2,5E-03	1,5E-03	3,1E-03	5,2E-03	2,0E-02	2,7E-02	3,5E-02
	99	4,6E-05	1,3E-04	2,4E-04	9,5E-05	2,7E-04	4,9E-04	6,0E-04	1,5E-03	2,5E-03
2oo3	0	4,8E-02	5,0E-02	5,3E-02	1,9E-01	1,8E-01	1,7E-01	4,6E+00	4,0E+00	3,3E+00
	60	8,3E-03	1,1E-02	1,4E-02	3,2E-02	3,5E-02	4,0E-02	7,6E-01	7,1E-01	6,6E-01
	90	6,9E-04	1,5E-03	2,6E-03	2,3E-03	3,9E-03	5,9E-03	4,9E-02	5,4E-02	6,0E-02
	99	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
1oo3	0	4,7E-02	1,3E-02	2,3E-02	2,4E-02	3,7E-02	5,5E-02	2,5E+00	2,0E+00	1,6E+00
	60	1,0E-03	4,5E-03	8,9E-03	3,0E-03	9,8E-03	1,8E-02	1,7E-01	1,8E-01	1,9E-01
	90	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,8E-03	1,3E-02	2,4E-02
	99	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и K = 0,98.

Б.3.2.4 Пример режима с низкой интенсивностью запросов

Рассматривают функцию безопасности, для реализации которой нужна система с УПБ 2. Построенный на основе предыдущего опыта первоначальный вариант архитектуры всей системы включает одну группу из трех аналоговых датчиков давления с архитектурой 2oo3 на входе. Логическая подсистема рассматриваемой системы представляет собой ПЭ систему с избыточностью с архитектурой 1oo2*D* и управляет одним закрывающим и одним дренажным клапанами, так как для обеспечения функции безопасности необходима работа как закрывающего, так и дренажного клапана. Архитектура всей системы представлена на рисунке Б.14. Для этой системы оценивают сначала функцию безопасности PFD_{SYS} при одногодичном периоде контрольных испытаний. Таблицы Б.6—Б.8 являются фрагментами таблицы Б.3 для соответствующих данных на рисунке Б.14.

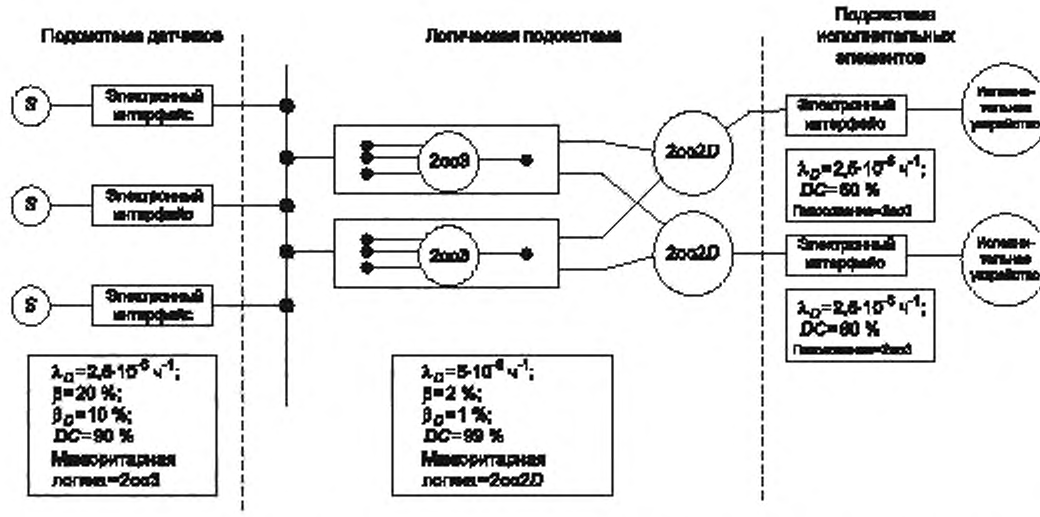


Рисунок Б.14 — Архитектура системы рассматриваемого примера для режима с низкой интенсивностью запросов

Таблица Б.6 — Средняя вероятность отказа по запросу для подсистемы датчиков в рассматриваемом примере для режима с низкой интенсивностью запросов (интервал контрольных испытаний равен одному году, а среднее время ремонта — 8 ч)

Архитектура	*DC*, %	λ_D = 2,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0	6,8E-04	1,5E-03	2,5E-03
	60	1,6E-04	5,1E-04	9,4E-04
	90	2,7E-05	1,2E-04	2,3E-04
	99	2,5E-06	1,2E-05	2,4E-05
Примечание — Настоящая таблица представляет собой фрагмент таблицы Б.3.				

Таблица Б.7 — Средняя вероятность отказа по запросу для логической подсистемы в примере для режима с низкой интенсивностью запросов (интервал контрольных испытаний равен одному году, а среднее время ремонта — 8 ч)

Архитектура	*DC*, %	λ_D = 0,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2*D*	0	1,1E-03	2,7E-03	4,8E-03
	60	2,0E-04	9,0E-04	1,8E-03
	90	4,5E-05	2,2E-04	4,4E-04
	99	4,8E-06	2,4E-05	4,8E-05
Примечание — Настоящая таблица представляет собой фрагмент таблицы Б.3.				

Таблица Б.8 — Средняя вероятность отказа по запросу для подсистемы исполнительных элементов в примере для режима с низкой интенсивностью запросов (интервал контрольных испытаний равен одному году, а среднее время ремонта — 8 ч)

Архитектура	*DC*, %	λ_D = 2,5E-06	λ_D = 0,5E-05
1oo1	0	1,1E-02	2,2E-02
	60	4,4E-03	8,8E-03
	90	1,1E-03	2,2E-03
	99	1,3E-04	2,6E-04
Примечание — Настоящая таблица представляет собой фрагмент таблицы Б.3.			

Данные, представленные в таблицах Б.6—Б.8, позволяют получить следующие значения:
- для подсистемы датчиков $PFD_S = 2{,}3 \cdot 10^{-4}$;
- логической подсистемы $PFD_L = 4{,}8 \cdot 10^{-6}$;
- подсистемы исполнительных элементов

$$PFD_{FE} = 4{,}4 \cdot 10^{-3} + 8{,}8 \cdot 10^{-3} = 1{,}3 \cdot 10^{-2}.$$

Следовательно, для функции безопасности

$$PFD_{SYS} = 2{,}3 \cdot 10^{-4} + 1{,}0 \cdot 10^{-5} + 1{,}3 \cdot 10^{-2} + 1{,}3 \cdot 10^{-2}.$$

≡ уровень полноты безопасности соответствует УПБ 1.

Для перевода системы на УПБ 2 выполняют одно из следующих действий:
- уменьшают интервал между контрольными проверками до 6 мес:

$PFD_S = 1{,}1 \cdot 10^{-4}$;
$PFD_L = 6{,}0 \cdot 10^{-5}$;
$PFD_{FE} = 2{,}2 \cdot 10^{-3} + 4{,}4 \cdot 10^{-3} = 6{,}6 \cdot 10^{-3}$;
$PFD_{SYS} = 6{,}7 \cdot 10^{-4}$

≡ уровень полноты безопасности соответствует УПБ 2;

- заменяют архитектуру 1oo1 закрывающего клапана, представляющего собой выходное устройство с низкой надежностью, на 1oo2, предполагая, что $\beta = 10$ % и $\beta_D = 5$ %:

$PFD_S = 2{,}3 \cdot 10^{-4}$;
$PFD_L = 1{,}0 \cdot 10^{-5}$;
$PFD_{FE} = 4{,}4 \cdot 10^{-3} + 9{,}7 \cdot 10^{-4} = 5{,}4 \cdot 10^{-3}$;
$PFD_{SYS} = 5{,}6 \cdot 10^{-3}$

≡ уровень полноты безопасности соответствует УПБ 2.

Б.3.2.5 Влияние неидеальных контрольных проверок

Отказы в системе безопасности, которые не обнаружены ни диагностическими тестами, ни контрольными проверками, могут быть выявлены другими методами, реализуемыми в таких ситуациях, как появление опасного события, требующего вмешательства ФБ, или во время капитального ремонта оборудования. Если отказы не будут обнаружены при помощи таких методов, следует предположить, что они останутся на весь срок службы оборудования. Обозначают обычный период между контрольными проверками T_1; долю отказов, обнаруженных контрольными проверками [охват контрольными проверками — PTS (от английского «proof test coverage» — охват контрольными проверками)], — как T_2, а часть отказов, не обнаруженных контрольными проверками, как 1 — PTS. Эти последние отказы, которые не могут быть выявлены в ходе контрольных проверок, будут обнаружены только при запросах к СБЗС системе, выполняемых с интервалом T_2. Таким образом, период контрольных проверок T_1 и время между запросами T_2 определяют эффективное время простоя.

Пример такой зависимости приведен для архитектуры 1oo2 (где T_2 — время между запросами к системе), определяемой по формулам:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \mathrm{MRT}\right) + \frac{\lambda_{DU}(1-\mathrm{PTC})}{\lambda_D}\left(\frac{T_2}{2} + \mathrm{MRT} + \frac{\lambda_{DD}}{\lambda_d}\mathrm{MTTR}\right); \quad (Б.28)$$

$$t_{GE} = \frac{T_{DU}(\text{PTC})}{\lambda_D}\left(\frac{T_1}{3} + \text{MRT}\right) + \frac{\lambda_{DU}(1-\text{PTC})}{\lambda_d}\left(\frac{T_2}{3} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}; \quad (Б.29)$$

$$\text{PFD}_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD}\text{MTTR} + \beta\lambda_{DU}(\text{PTC})\left(\frac{T_1}{2} + \text{MRT}\right) + \beta\lambda_{DU}(1-\text{PTC})\left(\frac{T_2}{2} + \text{MRT}\right). \quad (Б.30)$$

Результаты расчетов для системы с архитектурой 1oo2 со 100 %-ным охватом одногодичными (T_1 = 1 год) контрольными проверками в сравнении с 90 %-ным охватом контрольными проверками, где период запросов T_2 предполагается равным 10 годам, приведены в таблице Б.9. В рассматриваемом примере расчеты проводились при следующих предположениях: интенсивность отказов 0,5·10 в час; β = 10 %; β_D = 5 %.

Таблица Б.9 — Результаты расчетов (неидеальные контрольные испытания)

Архитектура	DC, %	λ_D = 0,5E-05	
		Охват диагностикой 100 %	Охват диагностикой 90 %
		β = 10 % β_D = 5 %	β = 10 % β_D = 5 %
1oo2	0	2,7E-03	6,0E-03
	60	9,7E-04	2,0E-03
	90	2,3E-04	4,4E-04
	99	2,4E-05	4,4E-05

Б.3.3 Средняя интенсивность опасных отказов (для режима работы с высокой интенсивностью запросов или с непрерывным запросом)

Б.3.3.1 Метод определения вероятности отказа функции безопасности для Э/Э/ПЭ системы, работающей в режиме с высокой интенсивностью запросов или с непрерывным запросом, аналогичен методу вычисления для режима с низкой интенсивностью запросов (см. Б.2.1), за исключением того, что среднюю вероятность отказа по запросу PFD_{SYS} заменяют на среднюю частоту опасного отказа в час PFH_{SYS}.

Общую вероятность опасного отказа функции безопасности для Э/Э/ПЭ СБЗС системы PFH_{SYS} определяют вычислением интенсивностей опасных отказов для всех подсистем, совокупность которых обеспечивает ФБ, и суммированием полученных значений. Так как рассматриваемые в настоящем приложении вероятности малы, то используют формулу

$$\text{PFH}_{SYS} = \text{PFH}_S + \text{PFH}_L + \text{PFH}_{FE}. \quad (Б.31)$$

Б.3.3.2 Архитектуры для режима работы с высокой интенсивностью запросов или с непрерывным запросом

Примечания

1 В настоящем пункте справедливые для нескольких архитектур формулы приводят в том случае, если их используют впервые (см. также Б.3.2.2).

2 Формулы настоящего пункта справедливы для предположений, перечисленных в Б.3.1.

Б.3.3.2.1 Архитектура 1oo1

На рисунках Б.4 и Б.5 представлены соответствующие структурные схемы, представленные в Б.3.2.2.1. Значения λ_D, t_{CE}, λ_{DU} и λ_{DD} вычисляют по формулам (Б.14), (Б.15), (Б.16) и (Б.17) соответственно.

Если предполагается, что СБЗС система переводит УО в безопасное состояние при обнаружении любого сбоя, то для архитектуры 1oo1 справедливо следующее

$$\text{PFH}_G = \lambda_{DU}.$$

Б.3.3.2.2 Архитектура 1oo2

На рисунках Б.6 и Б.7 представлены соответствующие структурные схемы. Значение t_{CE} вычисляют по формуле (Б.15), приведенной в Б.3.2.2.1. Если подразумевается, что СБЗС система переводит УО в безопасное состояние непосредственно после обнаружения отказа в обоих каналах и принимают консервативный подход, то PFH_G вычисляют по формуле

$$PFH_G = 2\left(\left(1-\beta_D\right)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)\lambda_{DU} + \beta\lambda_{DU}. \quad (Б.32)$$

Б.3.3.2.3 Архитектура 2oo2

Соответствующие структурные схемы представлены на рисунках Б.8 и Б.9. Если предполагается, что при обнаружении любого отказа каждый канал переводится в безопасное состояние, то для архитектуры 2oo2 применяют выражение

$$PFH_G = 2\lambda_{DU}. \quad (Б.33)$$

Б.3.3.2.4 Архитектура 1oo2*D*

Соответствующие структурные схемы представлены на рисунках Б.10 и Б.11. Для расчетов применяют выражения

$$\lambda_{SD} = \frac{\lambda}{2}DC; \quad (Б.34)$$

$$t_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right) + \left(\lambda_{DD} + \lambda_{SD}\right)\mathrm{MTTR}}{\left(\lambda_{DU} + \lambda_{DD} + \lambda_{SD}\right)}; \quad (Б.35)$$

$$PFH_G = 2(1-\beta)\lambda_{DU}\left((1-\beta)\lambda_{DU} + \left(1-\beta_D\right)\lambda_{DD} + \lambda_{SD}\right)\lambda_{CE} + 2(1-K)\lambda_{DD} + \beta\lambda_{DU}. \quad (Б.36)$$

Б.3.3.2.5 Архитектура 2oo3

Соответствующие структурные схемы представлены на рисунках Б.12 и Б.13. Значение t_{CE} вычисляют по формуле (Б.15), приведенной в Б.3.2.2.1. Если предполагается, что СБЗС система переводит УО в безопасное состояние непосредственно после обнаружения отказа в любом из каналов и принимается консервативный подход, то PFH_G вычисляют по формуле

$$PFH_G = 2(1-\beta)\lambda_{DU}\left((1-\beta)\lambda_{DU} + \left(1-\beta_D\right)\lambda_{DD} + \lambda_{SD}\right)\lambda_{CE} + 2(1-K)\lambda_{DD} + \beta\lambda_{DU}. \quad (Б.37)$$

Б.3.3.2.6 Архитектура 1oo3

Соответствующие структурные схемы представлены на рисунках Б.12 и Б.13.

Значение t_{CE} вычисляют по формуле (Б.15), приведенной в Б.3.2.2.1. Если предполагается, что СБЗС система переводит УО в безопасное состояние непосредственно после обнаружения отказа в трех каналах и принимается консервативный подход, то PFH_G вычисляют по формуле

$$PFH_G = 6\left(\left(1-\beta_D\right)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)(1-\beta)\lambda_{DU}t_{GE} + \beta\lambda_{DU}. \quad (Б.38)$$

Б.3.3.3 Подробные таблицы для режима работы с высокой интенсивностью запросов или с непрерывным запросом

Значения средних вероятностей отказов по запросу систем в режиме с высокой интенсивностью запросов или с непрерывным запросом для различных интервалов между контрольными испытаниями при среднем времени ремонта 8 ч представлены в таблицах Б.10—Б.13.

Таблица Б.10 — Средняя частота опасных отказов (в режиме работы с высокой интенсивностью запросов или с непрерывным запросом) для одномесячного интервала между контрольными проверками и среднего времени ремонта 8 ч

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (см. примечание 2)	0	5,0E-08			2,5E-07			5,0E-07		
	60	2,0E-08			1,0E-07			2,0E-07		
	90	5,0E-09			2,5E-08			5,0E-08		
	99	5,0E-10			2,5E-09			5,0E-09		
1oo2	0	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,0E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
2oo2 (см. примечание 2)	0	1,0E-07			5,0E-07			1,0E-06		
	60	4,0E-08			2,0E-07			4,0E-07		
	90	1,0E-08			5,0E-08			1,0E-07		
	99	1,0E-09			5,0E-09			1,0E-08		
1oo2*D* (см. примечание 3)	0	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60	1,6E-09	3,2E-09	5,2E-09	8,0E-09	1,6E-08	2,6E-08	1,6E-08	3,2E-08	5,2E-08
	90	1,9E-09	2,3E-09	2,8E-09	9,5E-09	1,2E-08	1,4E-08	1,9E-08	2,3E-08	2,8E-08
	99	2,0E-09	2,0E-09	2,1E-09	1,0E-08	1,0E-08	1,0E-08	2,0E-08	2,0E-08	2,1E-08
2oo3	0	1,0E-09	5,0E-09	1,0E-08	5,1E-09	2,5E-08	5,0E-08	1,1E-08	5,0E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,1E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo3	0	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,0E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo1 (см. примечание 2)	0	2,5E-06			5,0E-06			2,5E-05		
	60	1,0E-06			2,0E-06			1,0E-05		
	90	2,5E-07			5,0E-07			2,5E-06		
	99	2,5E-08			5,0E-08			2,5E-07		
1oo2	0	5,4E-08	2,5E-07	5,0E-07	1,2E-07	5,2E-07	1,0E-06	9,5E-07	2,9E-06	5,3E-06
	60	2,1E-08	1,0E-07	2,0E-07	4,3E-08	2,0E-07	4,0E-07	2,7E-07	1,1E-06	2,1E-06
	90	5,1E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07	5,5E-08	2,5E-07	5,0E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,1E-09	2,5E-08	5,0E-08

Окончание таблицы Б.10

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
2oo2 (см. примечание 2)	0	5,0E-06			1,0E-05			5,0E-05		
	60	2,0E-06			4,0E-06			2,0E-05		
	90	5,0E-07			1,0E-06			5,0E-06		
	99	5,0E-08			1,0E-07			5,0E-07		
1oo2*D* (см. примечание 3)	0	5,4E-08	2,5E-07	5,0E-07	1,2E-07	5,2E-07	1,0E-06	9,5E-07	2,9E-06	5,3E-06
	60	8,1E-08	1,6E-07	2,6E-07	1,6E-07	3,2E-07	5,2E-07	8,7E-07	1,7E-06	2,7E-06
	90	9,5E-08	1,2E-07	1,4E-07	1,9E-07	2,3E-07	2,8E-07	9,6E-07	1,2E-06	1,4E-06
	99	1,0E-07	1,0E-07	1,0E-07	2,0E-07	2,0E-07	2,1E-07	1,0E-06	1,0E-06	1,0E-06
2oo3	0	6,3E-08	2,6E-07	5,1E-07	1,5E-07	5,5E-07	1,0E-06	1,8E-06	3,6E-06	5,9E-06
	60	2,2E-08	1,0E-07	2,0E-07	4,9E-08	2,1E-07	4,1E-07	4,2E-07	1,2E-06	2,2E-06
	90	5,2E-09	2,5E-08	5,0E-08	1,1E-08	5,1E-08	1,0E-07	6,6E-08	2,6E-07	5,1E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,4E-09	2,5E-08	5,0E-08
1oo3	0	5,0E-08	2,5E-07	5,0E-07	1,0E-07	5,0E-07	1,0E-06	5,1E-07	2,5E-06	5,0E-06
	60	2,0E-08	1,0E-07	2,0E-07	4,0E-08	2,0E-07	4,0E-07	2,0E-07	1,0E-06	2,0E-06
	90	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07	5,0E-08	2,5E-07	5,0E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и $K = 0,98$.

Таблица Б.11 — Средняя частота опасных отказов (в режиме работы с высокой интенсивностью запросов или с непрерывным запросом) для трехмесячного интервала между контрольными проверками и среднего времени ремонта 8 ч

Архитектура	*DC*, %	λ_D = 0.5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (см. примечание 2)	0	5,0E-08			2,5E-07			5,0E-07		
	60	2,0E-08			1,0E-07			2,0E-07		
	90	5,0E-09			2,5E-08			5,0E-08		
	99	5,0E-10			2,5E-09			5,0E-09		
1oo2	0	1,0E-09	5,0E-09	1,0E-08	5,1E-09	2,5E-08	5,0E-08	1,1E-08	5,0E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,1E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09

Продолжение таблицы Б.11

Архитектура	DC, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo2 (см. примечание 2)	0	1,0E-07			5,0E-07			1,0E-06		
	60	4,0E-08			2,0E-07			4,0E-07		
	90	1,0E-08			5,0E-08			1,0E-07		
	99	1,0E-09			5,0E-09			1,0E-08		
1oo2*D* (см. примечание 3)	0	1,0E-09	5,0E-09	1,0E-08	5,1E-09	2,5E-08	5,0E-08	1,1E-08	5,0E-08	1,0E-07
	60	1,6E-09	3,2E-09	5,2E-09	8,0E-09	1,6E-08	2,6E-08	1,6E-08	3,2E-08	5,2E-08
	90	1,9E-09	2,3E-09	2,8E-09	9,5E-09	1,2E-08	1,4E-08	1,9E-08	2,3E-08	2,8E-08
	99	2,0E-09	2,0E-09	2,1E-09	1,0E-08	1,0E-08	1,0E-08	2,0E-08	2,0E-08	2,1E-08
2oo3	0	1,0E-09	5,0E-09	1,0E-08	5,4E-09	2,5E-08	5,0E-08	1,2E-08	5,1E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,1E-09	1,0E-08	2,0E-08	4,3E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo3	0	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,0E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo1 (см. примечание 2)	0	2,5E-06			5,0E-06			2,5E-05		
	60	1,0E-06			2,0E-06			1,0E-05		
	90	2,5E-07			5,0E-07			2,5E-06		
	99	2,5E-08			5,0E-08			2,5E-07		
1oo2	0	6,3E-08	2,6E-07	5,1E-07	1,5E-07	5,4E-07	1,0E-06	1,8E-06	3,6E-06	5,9E-06
	60	2,2E-08	1,0E-07	2,0E-07	4,9E-08	2,1E-07	4,1E-07	4,2E-07	1,2E-06	2,2E-06
	90	5,1E-09	2,5E-08	5,0E-08	1,1E-08	5,0E-08	1,0E-07	6,4E-08	2,6E-07	5,1E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,2E-09	2,5E-08	5,0E-08
2oo2 (см. примечание 2)	0	5,0E-06			1,0E-05			5,0E-05		
	60	2,0E-06			4,0E-06			2,0E-05		
	90	5,0E-07			1,0E-06			5,0E-06		
	99	5,0E-08			1,0E-07			5,0E-07		
1oo2*D* (см. примечание 3)	0	6,3E-08	2,6E-07	5,1E-07	1,5E-07	5,4E-07	1,0E-06	1,8E-06	3,6E-06	5,9E-06
	60	8,2E-08	1,6E-07	2,6E-07	1,7E-07	3,3E-07	5,3E-07	1,0E-06	1,8E-06	2,8E-06
	90	9,5E-08	1,2E-07	1,4E-07	1,9E-07	2,3E-07	2,8E-07	9,6E-07	1,2E-06	1,4E-06
	99	1,0E-07	1,0E-07	1,0E-07	2,0E-07	2,0E-07	2,1E-07	1,0E-06	1,0E-06	1,0E-06
2oo3	0	9,0E-08	2,8E-07	5,3E-07	2,6E-07	6,3E-07	1,1E-06	4,5E-06	5,9E-06	7,6E-06
	60	2,6E-08	1,1E-07	2,0E-07	6,6E-08	2,2E-07	4,2E-07	8,5E-07	1,6E-06	2,5E-06
	90	5,4E-09	2,5E-08	5,0E-08	1,2E-08	5,1E-08	1,0E-07	9,3E-08	2,9E-07	5,3E-07
	99	5,1E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,7E-09	2,6E-08	5,1E-08

Окончание таблицы Б.11

Архитектура	DC, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo3	0	5,0E-08	2,5E-07	5,0E-07	1,0E-07	5,0E-07	1,0E-06	5,5E-07	2,5E-06	5,0E-06
	60	2,0E-08	1,0E-07	2,0E-07	4,0E-08	2,0E-07	4,0E-07	2,0E-07	1,0E-06	2,0E-06
	90	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07	5,0E-08	2,5E-07	5,0E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и K = 0,98.

Таблица Б.12 — Средняя частота опасных отказов (в режиме работы с высокой интенсивностью запросов или с непрерывным запросом) для шестимесячного интервала между контрольными проверками и для среднего времени ремонта 8 ч

Архитектура	DC, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0	5,0E-08			2,5E-07			5,0E-07		
	60	2,0E-08			1,0E-07			2,0E-07		
	90	5,0E-09			2,5E-08			5,0E-08		
	99	5,0E-10			2,5E-09			5,0E-09		
1oo2	0	1,0E-09	5,0E-09	1,0E-08	5,3E-09	2,5E-08	5,0E-08	1,1E-08	5,1E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,2E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
2oo2 (см. примечание 2)	0	1,0E-07			5,0E-07			1,0E-06		
	60	4,0E-08			2,0E-07			4,0E-07		
	90	1,0E-08			5,0E-08			1,0E-07		
	99	1,0E-09			5,0E-09			1,0E-08		
1oo2*D* (см. примечание 3)	0	1,0E-09	5,0E-09	1,0E-08	5,3E-09	2,5E-08	5,0E-08	1,1E-08	5,1E-08	1,0E-07
	60	1,6E-09	3,2E-09	5,2E-09	8,0E-09	1,6E-08	2,6E-08	1,6E-08	3,2E-08	5,2E-08
	90	1,9E-09	2,3E-09	2,8E-09	9,5E-09	1,2E-08	1,4E-08	1,9E-08	2,3E-08	2,8E-08
	99	2,0E-09	2,0E-09	2,1E-09	1,0E-08	1,0E-08	1,0E-08	2,0E-08	2,0E-08	2,1E-08

Окончание таблицы Б.12

Архитектура	DC, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0	1,0E-09	5,0E-09	1,0E-08	5,8E-09	2,6E-08	5,1E-08	1,3E-08	5,3E-08	1,0E-07
	60	4,1E-10	2,0E-09	4,0E-09	2,1E-09	1,0E-08	2,0E-08	4,5E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,1E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo3	0	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,0E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo1 (см. примечание 2)	0	2,5E-06			5,0E-06			2,5E-05		
	60	1,0E-06			2,0E-06			1,0E-05		
	90	2,5E-07			5,0E-07			2,5E-06		
	99	2,5E-08			5,0E-08			2,5E-07		
1oo2	0	7,6E-08	2,7E-07	5,2E-07	2,1E-07	5,9E-07	1,1E-06	3,1E-06	4,7E-06	6,8E-06
	60	2,4E-08	1,0E-07	2,0E-07	5,7E-08	2,1E-07	4,1E-07	6,3E-07	1,4E-06	2,3E-06
	90	5,3E-09	2,5E-08	5,0E-08	1,1E-08	5,1E-08	1,0E-07	7,8E-08	2,7E-07	5,2E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,4E-09	2,5E-08	5,0E-08
2oo2 (см. примечание 2)	0	5,0E-06			1,0E-05			5,0E-05		
	60	2,0E-06			4,0E-06			2,0E-05		
	90	5,0E-07			1,0E-06			5,0E-06		
	99	5,0E-08			1,0E-07			5,0E-07		
1oo2*D* (см. примечание 3)	0	7,6E-08	2,7E-07	5,2E-07	2,1E-07	5,9E-07	1,1E-06	3,1E-06	4,7E-06	6,8E-06
	60	8,4E-08	1,6E-07	2,6E-07	1,8E-07	3,3E-07	5,3E-07	1,2E-06	2,0E-06	2,9E-06
	90	9,5E-08	1,2E-07	1,4E-07	1,9E-07	2,3E-07	2,8E-07	9,8E-07	1,2E-06	1,4E-06
	99	1,0E-07	1,0E-07	1,0E-07	2,0E-07	2,0E-07	2,1E-07	1,0E-06	1,0E-06	1,0E-06
2oo3	0	1,3E-07	3,2E-07	5,5E-07	4,2E-07	7,7E-07	1,2E-06	8,4E-06	9,2E-06	1,0E-05
	60	3,3E-08	1,1E-07	2,1E-07	9,1E-08	2,4E-07	4,4E-07	1,5E-06	2,1E-06	2,9E-06
	90	5,8E-09	2,6E-08	5,1E-08	1,3E-08	5,3E-08	1,0E-07	1,3E-07	3,2E-07	5,6E-07
	99	5,1E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	6,1E-09	2,6E-08	5,1E-08
1oo3	0	5,0E-08	2,5E-07	5,0E-07	1,0E-07	5,0E-07	1,0E-06	7,1E-07	2,7E-06	5,1E-06
	60	2,0E-08	1,0E-07	2,0E-07	4,0E-08	2,0E-07	4,0E-07	2,1E-07	1,0E-06	2,0E-06
	90	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07	5,0E-08	2,5E-07	5,0E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и $K = 0,98$.

Таблица Б.13 — Средняя частота опасных отказов (в режиме работы с высокой интенсивностью запросов или с непрерывным запросом) для одногодичного интервала между контрольными проверками и для среднего времени ремонта 8 ч

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0	5,0E-08			2,5E-07			5,0E-07		
	60	2,0E-08			1,0E-07			2,0E-07		
	90	5,0E-09			2,5E-08			5,0E-08		
	99	5,0E-10			2,5E-09			5,0E-09		
	0	1,0E-09	5,0E-09	1,0E-08	5,5E-09	2,5E-08	5,0E-08	1,2E-08	5,2E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,1E-09	1,0E-08	2,0E-08	4,3E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,1E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
2oo2 (см. примечание 2)	0	1,0E-07			5,0E-07			1,0E-06		
	60	4,0E-08			2,0E-07			4,0E-07		
	90	1,0E-08			5,0E-08			1,0E-07		
	99	1,0E-09			5,0E-09			1,0E-08		
1oo2*D* (см. примечание 3)	0	1,0E-09	5,0E-09	1,0E-08	5,5E-09	2,5E-08	5,0E-08	1,2E-08	5,2E-08	1,0E-07
	60	1,6E-09	3,2E-09	5,2E-09	8,1E-09	1,6E-08	2,6E-08	1,6E-08	3,2E-08	5,2E-08
	90	1,9E-09	2,3E-09	2,8E-09	9,5E-09	1,2E-08	1,4E-08	1,9E-08	2,3E-08	2,8E-08
	99	2,0E-09	2,0E-09	2,1E-09	1,0E-08	1,0E-08	1,0E-08	2,0E-08	2,0E-08	2,1E-08
2oo3	0	1,1E-09	5,1E-09	1,0E-08	6,6E-09	2,6E-08	5,1E-08	1,6E-08	5,5E-08	1,0E-07
	60	4,1E-10	2,0E-09	4,0E-09	2,3E-09	1,0E-08	2,0E-08	5,0E-09	2,1E-08	4,1E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,2E-10	2,5E-09	5,0E-09	1,1E-09	5,1E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo3	0	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07
	60	4,0E-10	2,0E-09	4,0E-09	2,0E-09	1,0E-08	2,0E-08	4,0E-09	2,0E-08	4,0E-08
	90	1,0E-10	5,0E-10	1,0E-09	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08
	99	1,0E-11	5,0E-11	1,0E-10	5,0E-11	2,5E-10	5,0E-10	1,0E-10	5,0E-10	1,0E-09
1oo1 (см. примечание 2)	0	2,5E-06			5,0E-06			2,5E-05		
	60	1,0E-06			2,0E-06			1,0E-05		
	90	2,5E-07			5,0E-07			2,5E-06		
	99	2,5E-08			5,0E-08			2,5E-07		
1oo2	0	1,0E-07	2,9E-07	5,4E-07	3,1E-07	6,8E-07	1,1E-06	5,8E-06	6,9E-06	8,5E-06
	60	2,9E-08	1,1E-07	2,1E-07	7,4E-08	2,3E-07	4,2E-07	1,1E-06	1,7E-06	2,6E-06
	90	5,5E-09	2,5E-08	5,0E-08	1,2E-08	5,2E-08	1,0E-07	1,0E-07	3,0E-07	5,4E-07
	99	5,1E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,6E-09	2,6E-08	5,0E-08

Окончание таблицы Б.13

Архитектура	*DC*, %	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-08		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo2 (см. примечание 2)	0	5,0E-06			1,0E-05			5,0E-05		
	60	2,0E-06			4,0E-06			2,0E-05		
	90	5,0E-07			1,0E-06			5,0E-06		
	99	5,0E-08			1,0E-07			5,0E-07		
1oo2*D* (см. примечание 3)	0	1,0E-07	2,9E-07	5,4E-07	3,1E-07	6,8E-07	1,1E-06	5,8E-06	6,9E-06	8,5E-06
	60	8,9E-08	1,7E-07	2,7E-07	1,9E-07	3,5E-07	5,4E-07	1,7E-06	2,3E-06	3,2E-06
	90	9,6E-08	1,2E-07	1,4E-07	1,9E-07	2,3E-07	2,8E-07	1,0E-06	1,2E-06	1,4E-06
	99	1,0E-07	1,0E-07	1,0E-07	2,0E-07	2,0E-07	2,1E-07	1,0E-06	1,0E-06	1,0E-06
2oo3	0	2,1E-07	3,8E-07	6,1E-07	7,3E-07	1,0E-06	1,4E-06	1,6E-05	1,6E-05	1,6E-05
	60	4,6E-08	1,2E-07	2,2E-07	1,4E-07	2,9E-07	4,7E-07	2,8E-06	3,2E-06	3,8E-06
	90	6,6E-09	2,6E-08	5,1E-08	1,6E-08	5,6E-08	1,0E-07	2,1E-07	3,9E-07	6,2E-07
	99	5,2E-10	2,5E-09	5,0E-09	1,1E-09	5,1E-09	1,0E-08	6,9E-09	2,7E-08	5,1E-08
1oo3	0	5,1E-08	2,5E-07	5,0E-07	1,1E-07	5,1E-07	1,0E-06	1,4E-06	3,2E-06	5,5E-06
	60	2,0E-08	1,0E-07	2,0E-07	4,0E-08	2,0E-07	4,0E-07	2,6E-07	1,0E-06	2,0E-06
	90	5,0E-09	2,5E-08	5,0E-08	1,0E-08	5,0E-08	1,0E-07	5,1E-08	2,5E-07	5,0E-07
	99	5,0E-10	2,5E-09	5,0E-09	1,0E-09	5,0E-09	1,0E-08	5,0E-09	2,5E-08	5,0E-08

Примечания

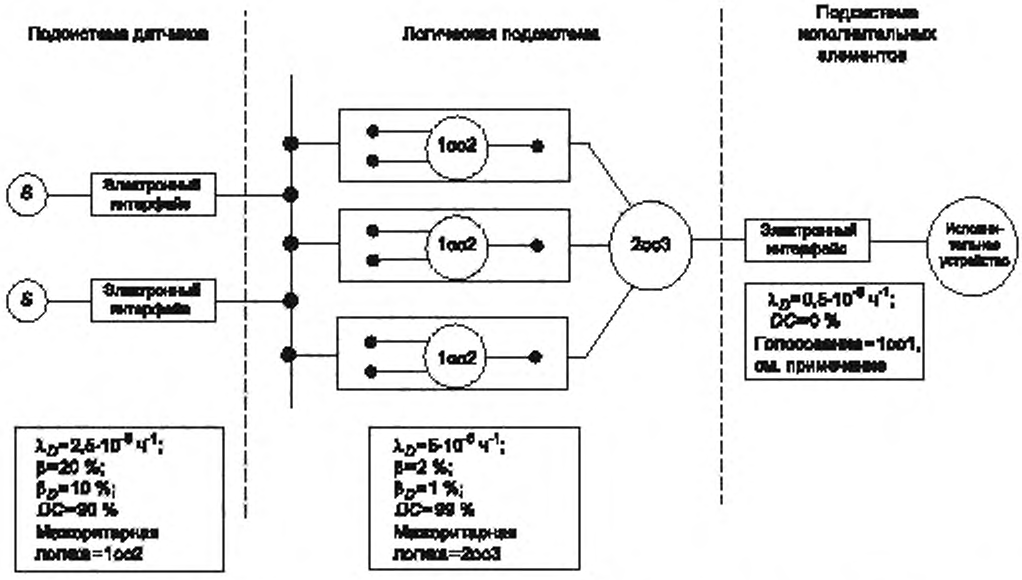
1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам (Б.9)—(Б.27) и с учетом предположений, перечисленных в Б.3.1. Если подсистема датчиков, логическая подсистема или подсистема исполнительных элементов входят в состав только одной группы голосующих каналов, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. Б.3.2.1).

2 В настоящей таблице предполагается, что $\beta = 2 \cdot \beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

3 Интенсивность безопасных отказов принимают равной интенсивности опасных отказов и $K = 0,98$.

Б.3.3.4 Пример режима работы с высокой интенсивностью запросов или в режиме с непрерывным запросом

Рассматривают ФБ, для реализации которой нужна система УПБ 2. Пусть первоначальный вариант архитектуры всей системы, построенный на основе предыдущего опыта, включает одну группу из двух датчиков с архитектурой 1oo2 на входе. Логическая подсистема рассматриваемой системы представляет собой ПЭ СБЗС систему с избыточностью с архитектурой 2oo3 и управляет одним закрывающим контактором. Архитектура описанной системы показана на рисунке Б.15. Для этой системы оценивают значение при шестимесячном интервале между контрольными проверками. Таблицы Б.14—Б.16 являются фрагментами таблицы Б.12 для соответствующих данных, приведенных на рисунке Б.15.



Примечание — Доля безопасных отказов для подсистемы исполнительных элементов превышает 60 %.

Рисунок Б.15 — Архитектура системы рассматриваемого примера для режима с высокой интенсивностью запросов или с непрерывным запросом

Таблица Б.14 — Средняя частота опасных отказов для подсистемы датчиков в рассматриваемом примере режима работы с высокой интенсивностью запросов или с непрерывным запросом (шестимесячный интервал контрольных проверок и среднее время ремонта 8 ч)

Архитектура	*DC*, %	λ_D =2,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2	0	7,6E-08	2,7E-07	5,2E-07
	60	2,4E-08	1,0E-07	2,0E-07
	90	5,3E-09	2,5E-08	5,0E-08
	99	5,0E-10	2,5E-09	5,0E-09
Примечание — Настоящая таблица представляет собой фрагмент таблицы Б.12.				

Таблица Б.15 — Средняя частота опасных отказов для логической подсистемы в рассматриваемом примере режима работы с высокой интенсивностью запросов или с непрерывным запросом (шестимесячный интервал контрольных проверок и среднее время ремонта 8 ч)

Архитектура	*DC*, %	λ_D = 0,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0	4,2E-07	7,7E-07	1,2E-06
	60	9,1E-08	2,4E-07	4,4E-07
	90	1,3E-08	5,3E-08	1,0E-07
	99	1,0E-09	5,0E-09	1,0E-08
Примечание — Настоящая таблица представляет собой фрагмент таблицы Б.12.				

Таблица Б.16 — Средняя частота опасных отказов для подсистемы исполнительных элементов в рассматриваемом примере режима работы с высокой интенсивностью запросов или с непрерывным запросом (шестимесячный интервал контрольных испытаний и среднее время ремонта 8 ч)

Архитектура	*DC*, %	λ_D = 0,5E-06
1oo1	0	5,0E-07
	60	2,0E-07
	90	5,0E-08
	99	5,0E-09
Примечание — Настоящая таблица представляет собой фрагмент таблицы Б.12.		

Данные таблиц Б.14—Б.16 позволяют получить следующие значения:
для подсистемы датчиков — $PFH_S = 5{,}2 \cdot 10^{-7}$ 1/ч;
логической подсистемы — $PFH_L = 1{,}0 \cdot 10^{-9}$ 1/ч;
подсистемы исполнительных элементов — $PFH_{PE} = 5{,}0 \cdot 10^{-7}$ 1/ч;
функции безопасности, следовательно, —
$PFH_{SUS} = (5{,}2 \cdot 10^{-7} + 1{,}0 \cdot 10^{-9} + 5{,}0 \cdot 10^{-7})$1/ч = $1{,}2 \cdot 10^{-6}$ 1/ч;
≡ уровень полноты безопасности — УПБ 1.

Для перевода системы на УПБ 2 выполняют одно из следующих действий:

- изменяют тип и способ установки входного датчика для улучшения защиты от отказа по общей причине. Таким образом, снижая значение β от 20 % до 10 %, а β_D от 10 % до 5 %, получают:

$PFH_S = 2{,}7 \cdot 10^{-7}$ 1/ч,
$PFH_L = 1{,}0 \cdot 10^{-9}$ 1/ч,
$PFH_{FE} = 5{,}0 \cdot 10^{-7}$ 1/ч,
$PFH_{SYS} = 7{,}7 \cdot 10^{-7}$ 1/ч,
≡ уровень полноты безопасности — УПБ 2;

- заменяют единственное выходное устройство двумя устройствами с архитектурой 1oo2 (β = 10 % и β_D = 5 %):

$PFH_S = 5{,}2 \cdot 10^{-7}$ 1/ч,
$PEH_S = 2{,}7 \cdot 10^{-7}$ 1/ч,
$PFH_L = 1{,}0 \cdot 10^{-9}$ 1/ч,
$PFH_{FE} = 5{,}0 \cdot 10^{-7}$ 1/ч,
$PFH_{SYS} = 5{,}7 \cdot 10^{-7}$ 1/ч
≡ уровень полноты безопасности — УПБ 2.

Б.4 Логический подход

Б.4.1 Общие положения

Логический подход представляет собой методы, использующие логические функции, которые связывают отказы отдельных компонентов с общим отказом системы. Основными логическими моделями, использующимися в надежности, являются блок-схемы надежности, деревья отказов, деревья событий и причинно-следственные диаграммы. В настоящем стандарте рассмотрены только первые два метода. Цель всех методов — это представление логической структуры системы, тем не менее в моделях этих методов не учитывается ее поведение во времени. Поэтому при проведении расчетов необходимо проявлять осторожность при рассмотрении характеристик поведения системы (например, зависимых от времени характеристик типа периодических контрольных проверок). Первым шагом для применения логических моделей становится отделение графического представления системы от вычислений. Это описано в предыдущем разделе, где блок-схема надежности использована для моделирования структуры системы, а расчеты на основе моделей Маркова — для оценки PFD или PFH. Далее будут рассмотрены вероятностные расчеты для методов блок-схемы надежности и дерева отказов.

Данный подход ограничен тем, что поведение компонентов считается достаточно независимым друг от друга.

Б.4.2 Модель блок-схемы надежности

Ранее рассмотрено несколько примеров блок-схемы надежности. Например, на рисунке Б.1 представлена полная СБЗС система, состоящая из трех датчиков (*A*, *B*, *C*), работающих по схеме 1oo3, одного логического решающего устройства (*D*) и двух исполнительных элементов (*E*, *F*), работающих по схеме 1oo2.

На рисунке Б.16 представлена простая СБЗС система с датчиками, работающими по схеме голосования 2oo3. Основная приемлемость такого графического представления объясняется тремя позициями: оно очень близко к физической структуре изучаемой системы, широко используется в инженерной среде и наглядно, что удобно для рассмотрения.

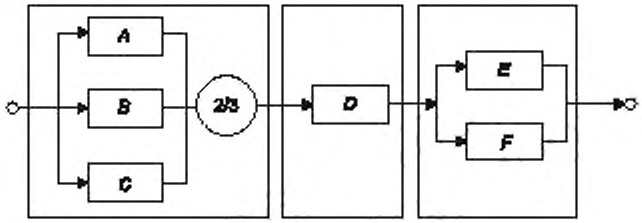


Рисунок Б.16 — Блок-схема надежности простой полной СБЗС системы с датчиками, организованными по схеме 2оо3

Основной недостаток блок-схемы надежности состоит в том, что этот метод в большей степени является методом представления, чем методом анализа [см. ГОСТ 34332.5—2021 (пункт Б.6.4)].

Б.4.3 Модель дерева отказов

Деревья отказов имеют такие же свойства, что и блок-схемы надежности, но в дополнение к последним они представляют собой эффективный дедуктивный (сверху вниз) метод анализа, помогающий инженерам по надежности разрабатывать модели шаг за шагом от события верхнего уровня (нежелательного или недопустимого) к отказам отдельных компонентов.

На рисунке Б.17 представлено дерево отказов, которое является идеальным аналогом блок-схемы надежности, приведенной на рисунке Б.1, но с указанными сверху вниз шагами анализа (например, отказ Э/Э/ПЭ СБЗС системы => отказ датчика => отказ датчика *A*). В дереве отказов элементы, работающие последовательно, соединены оператором «ИЛИ», а элементы, работающие параллельно (реализующие резервирование), — оператором «И» [см. ГОСТ 34332.5—2021 (пункты Б.6.6.5 и Б.6.6.9) и ГОСТ Р 51901.12].

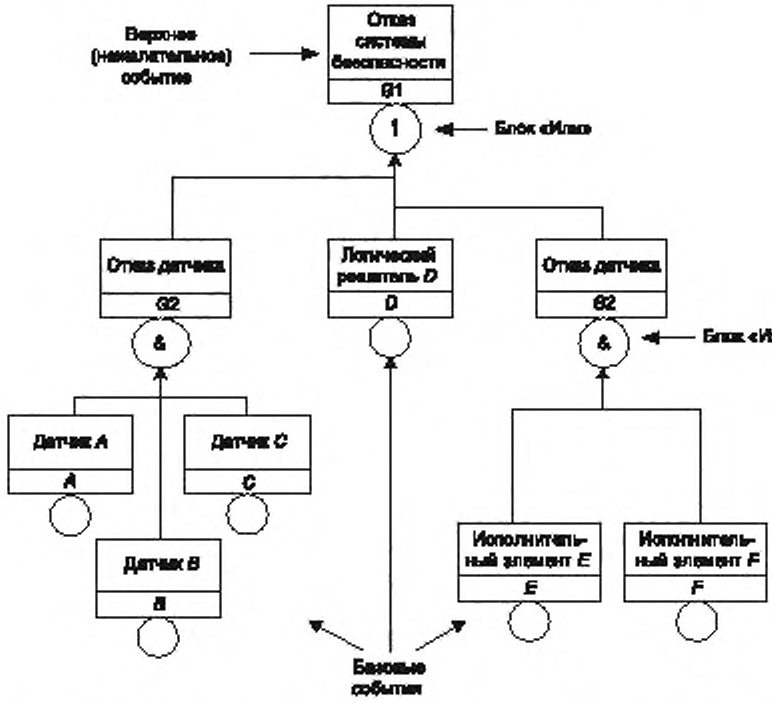
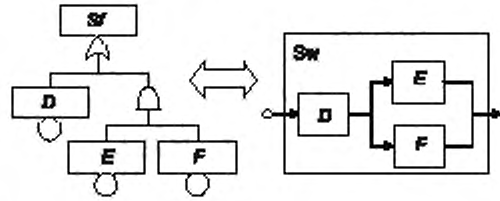


Рисунок Б.17 — Простое дерево отказов, эквивалентное блок-схеме, представленной на рисунке Б.1

Б.4.4 Расчет PFD

Б.4.4.1 Общие положения

Блок-схема надежности и дерево отказов представляют собой одно и то же, и расчеты могут быть выполнены похожим способом. На рисунке Б.18 показано небольшое сходство методов дерева отказов и блок-схемы надежности, которое будет использовано для демонстрации основных принципов вычислений.



Примечание — На рисунке курсивом обозначены отказавшие элементы, не курсивом — работающие.

Рисунок Б.18 — Эквивалентность дерева отказов и блок-схемы надежности

Дерево отказов описывают логической функцией $Sf = D \cap (E \cap F)$, где Sf — это отказ системы, а D, E и F — отказы отдельных компонентов. Блок-схема надежности описывается логической функцией $Sw = D \cap (E \cup F)$, где Sw — это правильно функционирующая система, а D, E и F — правильно функционирующие отдельные компоненты. Тогда $Sf = HESw$, а Sf и Sw представляют абсолютно идентичную информацию [т. е. являются дуальными (двойственными) логическими функциями].

Главное предназначение дерева отказов и блок-схемы надежности состоит в определении комбинаций отказов разных компонентов, ведущих к общему отказу системы. Они также называются минимальными сечениями, потому что указывают, где «разрезается» блок-схема надежности, в результате чего сигнал, поданный на вход, не достигнет выхода. В данном случае применяют два вида сечений: одиночный отказ (D) и двойной отказ (E, F).

Применяя методы теории вероятности к логическим функциям, можно непосредственно вычислить вероятность отказа рассматриваемой системы P_{Sf} по формуле

$$P_{Sf} = P(D) + P\left(E \cap F\right) - P\left(D \cap E \cap F\right) \tag{Б.39}$$

Если компоненты системы независимы, то получают следующую формулу

$$P_{Sf} = P_D + P_E P_F - P_D P_E P_F, \tag{Б.40}$$

где P_i — отказавший i-й компонент.

Формула (Б.41) является независимой от времени и отражает только логическую структуру системы.

Таким образом, и блок-схема надежности, и дерево отказов являются в основе своей статическими, т. е. моделями, независимыми от времени.

Тем не менее, если вероятность отказа каждого отдельного компонента в момент времени t не зависит от того, что происходит с другим компонентом в интервале [0, t], то указанная выше формула остается правильной в любой момент времени:

$$P_{Sf}(t) = P_D(t) + P_E(t)P_F(t) - P_D(t)P_E(t)P_F(t).$$

Аналитик должен проверить, применимы ли требуемые приближения и можно ли получить неготовность системы $U_{Sf}(t)$ в конкретный момент времени t, вычисляя ее по формуле

$$U_{Sf} = U_D(t) + U_E(t)U_E(t) - U_D(t)U_E(t)U_F(t). \tag{Б.41}$$

Исходя из этого можно сделать вывод о том, что деревья отказов и блок-схемы надежности позволяют вычислить мгновенную неготовность $U_{Sf}(t)$ Э/Э/ПЭ системы, и в соответствии с Б.2.2 можно вычислить $PFD_{avg}(T)$ по формуле

$$PFD_{avg}(T) = \frac{1}{T}MTD(T) = \frac{1}{T}\int_0^T U_{SI}(t)dt. \quad (Б.42)$$

Данный подход может быть применен и для минимальных сечений:
- одиночный отказ (*D*)

$$PFD^{D}(\tau) = \frac{1}{\tau}\int_0^{\tau}\lambda_D t dt = \lambda_D \tau/2;$$

- двойной отказ (*E*, *F*)

$$PFD^{EF}(\tau) = \frac{1}{\tau}\int_0^{\tau}\lambda_E\lambda_F t^2 dt = \lambda_E\lambda_F \tau^2/3.$$

Б.4.4.2 Вычисления, выполняемые для реализации методов дерева отказов или блок-схемы надежности

Формула (Б.42) является частным видом так называемой формулы Пуанкаре. Более общая формула, когда $S_I = U_I C_I$, где C_i представляет собой минимальные сечения системы, имеет вид:

$$P\left(\bigcup_{i=1}^{n} C_i\right) = \sum_{j=1}^{n} P(C_j) - \sum_{j=1}^{n}\sum_{i=1}^{j-1} P(C_j \cap C_i) \mp \sum_{j=3}^{n}\sum_{i=2}^{j-1}\sum_{k=1}^{i-1} P(C_j \cap C_i \cap C_k) - \ldots \quad (Б.43)$$

С увеличением числа отдельных компонентов число минимальных сечений растет экспоненциально. В данном случае формула Пуанкаре приводит к комбинаторному взрыву числа вычисляемых элементов, что вручную выполнить невозможно. Эта проблема анализировалась в течение последних 40 лет, и были созданы многочисленные алгоритмы для проведения подобных расчетов. В настоящее время эффективные разработки основаны на так называемой бинарной диаграмме решений BDD (Binary Decision Diagrams), которая получена из развитого Шенноном разложения логической функции.

В повседневной практике в различных отраслях промышленности (атомная, нефтяная, аэронавтика, автомобилестроение и т. д.) инженеры по надежности применяют множество коммерческих программных пакетов, основанных на моделях дерева отказов. Они могут быть использованы для расчета PFD_{avg}, но аналитик должен быть предельно внимательным, потому что иногда реализованные вычисления PFD_{avg} некорректны. Основной ошибкой является неправильное вычисление сочетания $PFD_{avg, i}$ отдельных компонентов (как правило, получаемых как $\lambda_i \tau/2$) для получения предполагаемого результата для PFD_{avg} всей системы. Как показано выше, результат оказывается неверным и неконсервативным.

Программные пакеты, основанные на методе дерева отказов, могут быть использованы для вычисления мгновенной неготовности системы $U_{SI}(t)$ исходя из мгновенной неготовности компонентов $U_i(t)$. После этого может быть вычислено среднее значение $U_{SI}(t)$ за определенный период времени для нахождения PFD_{avg}. В зависимости от используемого ПО это может быть сделано непосредственно программным пакетом или с помощью дополнительного вычисления.

Ранее описанный идеальный случай показан слева на рисунке Б.19:

$U_i(t) = \lambda\zeta$ и $\zeta = t$ по модулю τ.

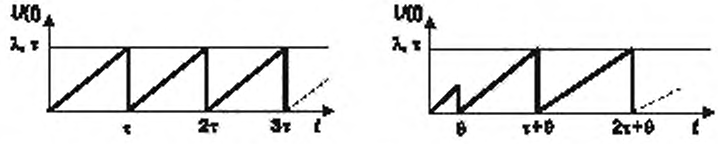


Рисунок Б.19 — Мгновенная неготовность $U(t)$ отдельного периодически проверяемого элемента

Эта так называемая «зубчатая» кривая увеличивается линейно от 0 до $\lambda\tau$ и повторно начинается с 0 после испытания или ремонта (которые считаются мгновенными, т. к. в это время УО не работает).

Когда в структурах с резервированием использовано несколько компонентов, испытания могут иметь график, представленный на рисунке Б.19, где первый интервал проверки отличается от других. Это не влияет на PFD_{avg} или на максимальные значения, которые в этих случаях равны $\lambda\tau/2$ и $\lambda\tau$.

В неидеальном случае кривые могут быть более сложными, чем показано на рисунке Б.19. В Б.5.2 даны руководящие указания по проектированию более точных зубчатых кривых, но для целей данного пункта вид кривых, представленных на рисунке Б.19, вполне приемлем.

На рисунке Б.20 показано применение данного подхода к небольшому дереву отказов, представленному на рисунке Б.18 (на рисунке Б.20 *DU* означает необнаруженные опасности, а *CF* — отказы по общей причине). Ранее упомянуто, что система имеет два дублирующих компонента (*E* и *F*) и что *D* — общая причина отказа этих компонентов. Для вычисления использовались следующие значения:

$$\lambda_{DU} = 3{,}5 \cdot 10^{-6}\ 1/ч,\ \tau = 4380\ ч \text{ и } \beta = 1\ \%.$$

Коэффициент β был выбран таким образом, чтобы быть уверенным, что *CCF* не превалирует в результирующем значении PFD_{avg}, и чтобы получить четкое понимание того, как в данном методе вычисляют PFD_{avg}.

Вид зубчатой кривой на входах *D*, *E* и *F* аналогичен левой кривой на рисунке Б.19. *CCF*(*D*) проверяют каждый раз одновременно с *E* или *F*. *E* и *F* проверяются в одно и то же время каждые 6 мес, также как и *CCF*(*D*).

Используя один из алгоритмов, разработанных для вычисления дерева отказов, довольно просто сформировать зубчатую кривую на выходах каждого логического блока. PFD_{avg} вычисляют путем усреднения результатов, полученных для события верхнего уровня. Это может быть выполнено, если использовать как программное обеспечение метода, так и расчет вручную. Полученное значение для $PFD_{avg} = 1{,}4 \cdot 10^{-4}$ по настоящему стандарту соответствует уровню УПБ 3 для режима работы с низкой интенсивностью запросов.

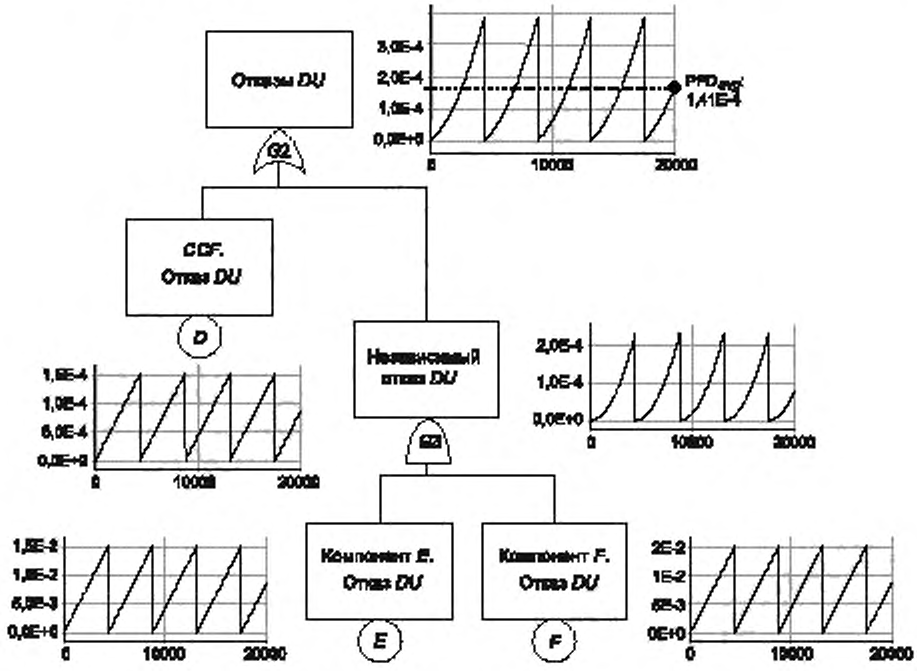


Рисунок Б.20 — Принцип вычисления PFD_{avg} при помощи дерева отказов

Как показано на рисунке Б.20, графики между проверками сглаживаются. Поэтому вычислить среднее значение несложно при условии, что определен и учтен момент проверки.

Следует отметить, что если реализовано резервирование, то зубчатые кривые событий верхнего уровня между проверками становятся нелинейными (т. е. интенсивность отказа всей системы не является постоянной величиной).

Также обращает на себя внимание оценка влияния на PFD_{avg} сдвига по времени испытаний, дублирующих компонент, вместо проведения их в одно и то же время. Это показано на рисунке Б.21, где проверки компонента *F* сдвинуты по времени относительно проверок компонента *D* на 3 мес.

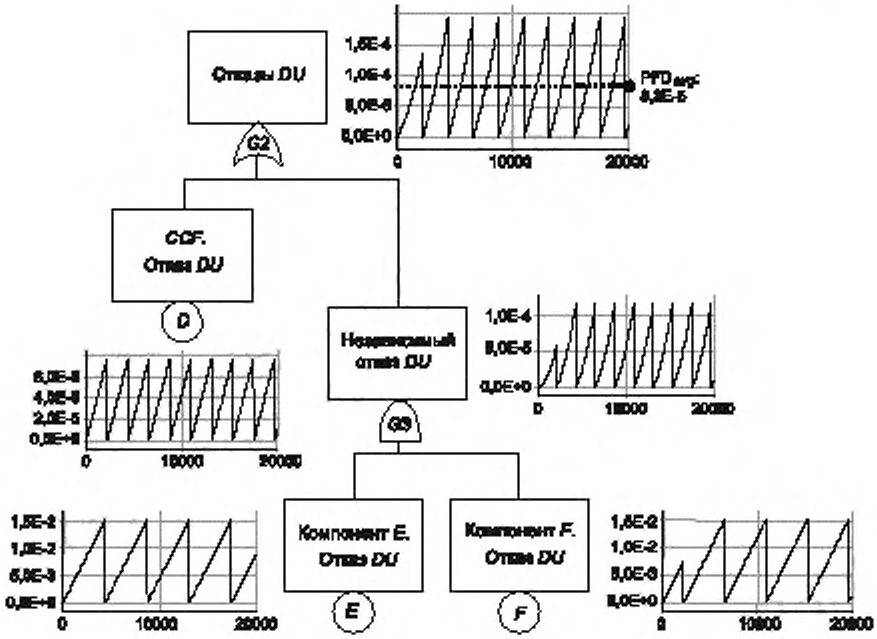


Рисунок Б.21 — Влияние смещения проверок

Это приводит к ряду важных последствий:

- *CCF* в данном случае проверяют каждые 3 мес (т .е. каждый раз, когда проверяют *E*, и каждый раз, когда проверяют *F*), и частота контрольных испытаний в два раза выше, чем в предыдущем случае;

- зубчатый график события верхнего уровня также имеет частоту контрольных проверок в два раза выше, чем раньше;

- зубчатый график имеет меньшие отклонения относительно среднего значения по сравнению с предыдущим случаем;

- PFD_{avg} снизилось до значения $8{,}3 \cdot 10^{-5}$; с этой новой политикой проверки система достигла УПБ 4.

Если проверки смещены относительно друг друга и реализованы корректные процедуры, то это увеличит вероятность обнаружения *CCF* и является эффективным методом уменьшения *CCF* для систем, работающих в режиме с низкой интенсивностью запросов. Это позволило улучшить значение УПБ с УПБ 3 до УПБ 4 (для отказов АС и при условии, что выполнены другие требования комплекса стандартов ГОСТ 34332).

На рисунке Б.22 представлена зубчатая кривая, полученная при последовательном добавлении к системе, смоделированной на рисунке Б.20, элемента *G* ($\lambda_{DU} = 7 \cdot 10^{-9}$ 1/ч при отсутствии проверок) и элемента *H* ($\lambda_{DU} = 7 \cdot 10^{-9}$ 1/ч, $\lambda_{DU} = 7 \cdot 10^{-8}$ 1/ч с контрольными проверками каждые два года).

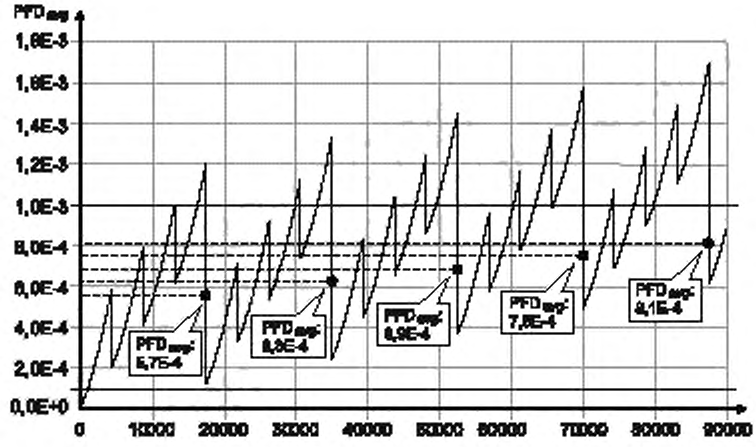


Рисунок Б.22 — Пример комплексного шаблона проверки

Влияние непроверяемого элемента *G* двоякое: PFD(*t*) не примет нулевое значение, если проверки проводят каждые два года и значение PFD_{avg} непрерывно возрастает (черные точки соответствуют PFD_{avg} в течение периода, ограниченного соответствующей пунктирной линией).

Даже если простейшие зубчатые кривые (как, например, показанные на рисунке Б.19) довольно просты, результаты для события верхнего уровня могут быть достаточно сложными, но это не затрудняет применение метода.

Цель настоящего пункта заключается только в демонстрации принципа расчета с использованием логических моделей. В Б.5.2, относящемуся к марковскому подходу, приведен ряд руководящих указаний по созданию более сложных входных зубчатых кривых для элементарных компонентов.

Можно сделать вывод о том, что если отдельные компоненты являются относительно независимыми, то отсутствуют проблемы при вычислении PFD_{avg} для Э/Э/ПЭ СБЗС системы с помощью классических логических методов. С теоретической точки зрения это не так просто, и аналитик, проводящий исследование, должен иметь глубокие знания о вероятностных методах, чтобы выявить и отклонить встречающиеся некорректные значения PFD_{avg}. При условии выполнения этих мер предосторожности может быть использован любой программный пакет для расчета деревьев отказов.

Для расчетов PFH также могут быть использованы логические методы, но их теоретическое обоснование выходит за рамки настоящего приложения.

Б.5 Подходы, основанные на моделях состояний/переходов

Б.5.1 Основные положения

Логические модели в основном не зависят от времени, и введение понятия времени возможно только в особых случаях. Логические модели довольно искусственны и, чтобы избежать ошибок, требуют детального знания вероятностных методов. Поэтому в таких случаях могут быть использованы другие вероятностные модели, динамические по природе. В области надежности они основаны на следующем фундаментальном подходе, состоящем из двух этапов:

- определения всех состояний системы на этапе изучения;
- анализа переходов системы из состояния в состояние в соответствии с происходящими событиями и на протяжении их существования.

Именно поэтому они находятся в категории моделей состояний-переходов.

Основной подход состоит в построении для изучаемой системы некоторой модели поведения автомата с возникающими событиями (отказами, ремонтами, испытаниями и т. д.). Согласно настоящему стандарту Э/Э/ПЭ СБЗС системы имеют только дискретные состояния. Данные модели являются динамическими по своей природе и могут быть реализованы различными способами: графическим представлением, специальным формальным языком или универсальным языком программирования. В настоящем приложении представлены два метода, которые существенно различаются, но дополняют друг друга:

- модель Маркова, которая разработана в самом начале прошлого века, детально изучена и обрабатывается аналитически;
- сеть Петри, которая разработана в 60-х годах прошлого века, менее известна (но ее все чаще используют из-за ее гибкости), и ее применяют совместно с моделированием методом Монте-Карло.

Оба метода основаны на графическом представлении, что удобно пользователям. Другие методы базируются на моделях, лежащих в основе формальных языков, что будет кратко рассмотрено в конце раздела.

Б.5.2 Подход Маркова

Б.5.2.1 Принцип моделирования

Марковский подход является наиболее известным из всех динамических подходов в области надежности. Марковские процессы разделяются на гомогенные (или однородные процессы, в которых все интенсивности переходов — это постоянные величины) и прочие (полумарковские процессы). Так как будущее гомогенного процесса Маркова не зависит от его прошлого, то выполняемые аналитические вычисления являются относительно простыми. Для более сложного, полумарковского, процесса может быть использован метод моделирования Монте-Карло. В настоящем стандарте рассмотрены только гомогенные процессы и для упрощения термин «марковские процессы» применен именно в этом контексте [см. ГОСТ 34332.5—2021 (пункт Б.6.4)].

Основная базовая формула для марковских процессов:

$$P_i(t+\mathrm{dt}) = \sum_{k=1} P_k(i)\lambda_{ki}\mathrm{dt} + P_i(t)\left(1 - \sum_{k=1}\lambda_{ki}\mathrm{dt}\right), \qquad (Б.44)$$

где λ_{ki} — интенсивность перехода (т. е. частота отказов или ремонтов) из состояния i в состояние k.

Вероятность нахождения в состоянии i в момент времени t + dt является вероятностью перехода к состоянию i (если другим состоянием является k) или вероятностью пребывания в состоянии i (если система уже находится в этом состоянии) в интервале времени от t до t + dt.

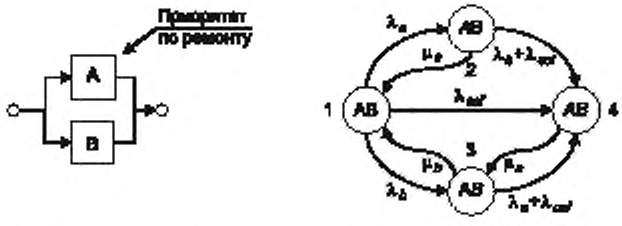


Рисунок Б.23 — Граф марковской модели, описывающей поведение системы из двух компонент

Существует тесная связь между приведенной выше формулой и графическим изображением на рисунке Б.23, которое представляет собой систему, состоящую из двух компонентов с одной командой ремонта (компонент *A* имеет больший приоритет на ремонт) и общей причиной отказа. На рисунке Б.23 компонент *A* обозначает, что компонент *A* — в рабочем состоянии, A — в состоянии отказа. Так как необходимо учитывать время обнаружения, поэтому μ_a и μ_b на рисунке Б.23 являются частотами восстановления компонентов (т.е. $\mu_a = 1/\mathrm{MTTR}_a$ и $\mu_b = 1/\mathrm{MTTR}_b$).

Например, вероятность нахождения в состоянии *4* вычисляют по следующей формуле:

$$P_4(t+\mathrm{dt}) = \left[P_1(t)\lambda_{ccf} + P_2(t)\left(\lambda_\beta + \lambda_{ccf}\right) + P_3(t)\left(\lambda_a + \lambda_{ccf}\right)\right]\mathrm{dt} + P_4(t)\left(1-\mu_a\mathrm{dt}\right), \qquad (Б.45)$$

что приводит к дифференциальному уравнению в векторной форме $d\vec{P}(t)\mathrm{dt} = P[M]\vec{P}(t)$, которое условно разрешимо:

$$\vec{P}(t)\mathrm{dt} = e^{t[M]}\vec{P}(0),$$

где $[M]$ — матрица Маркова, содержащая частоты переходов, а $\vec{P}(0)$ — вектор начальных условий (обычно вектор-столбец с 1 для начального состояния и 0 для остальных).

Даже если экспонента матрицы имеет не точно такие же свойства, как обычная экспонента, то можно записать:

$$\vec{P}(t) = e^{(t-t_1)[M]}e^{t_1[M]}\vec{P}(0) = e^{(t-t_1)[M]}\vec{P}(t_1),$$

Это показывает базовое свойство марковских процессов: знание вероятностей состояний в заданный момент времени t_1 — это сумма знаний всех предыдущих, что достаточно для вычисления поведения системы после момента времени t_1 и полезно для вычисления PFD.

Для решения указанных уравнений разработаны эффективные алгоритмы и реализованы в программных пакетах. Поэтому при использовании данного подхода аналитик может строить модели, не особенно вникая в лежащую в его основе математику, хотя в любом случае он должен, по крайней мере, понимать изложенное в настоящем приложении.

На рисунке Б.24 представлен принцип расчета PFD.

Расчеты PFD относят к Э/Э/ПЭ СБЗС системам, работающим в режиме работы с низкой интенсивностью запросов и с периодическими (контрольными) проверками. Для подобных систем ремонты начинают только после проведения проверок. Моменты выполнения проверок являются особыми точками на временной оси, но многофазный подход Маркова может быть использован для решения этой проблемы.

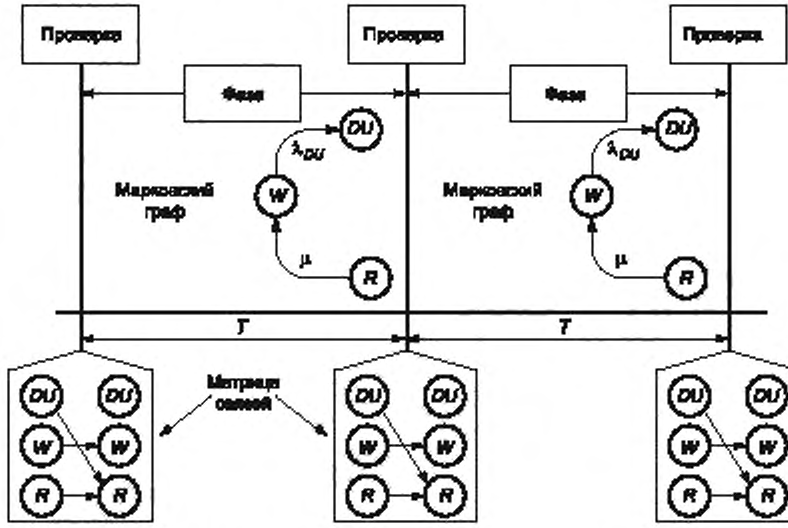


Рисунок Б.24 — Принцип марковского многофазного моделирования

Например, в простой системе производится периодическая проверка одного компонента, имеющего три состояния, как показано на рисунке Б.24: рабочее (*W*), необнаруженный опасный отказ (*DU*) и ремонт (*R*).

Его поведение между испытаниями моделируется марковским процессом, показанным в верхней части рисунка Б.24: он может отказать (*W*→ *DU*) или быть в ремонте (*R* → *W*). Так как ремонт не может начаться во время интервала проверки, то отсутствует и переход от *DU* к *R*. Поскольку диагностика отказа производится после перехода в состояние *R*, μ является частотой ремонта компонента (т.е. μ = 1/MPT) на рисунке Б.24.

Когда испытание проведено (см. матрицу связей на рисунке Б.24), начинается ремонт, если произошел отказ (*DU* → *R*), или компонент продолжает работать, если он находится в нормально функционирующем состоянии (*W* → *W*), а в гипотетической ситуации, когда ремонт, который начался после предыдущей проверки, еще не завершен и продолжается (*R* → *R*). Матрица связей [*L*] может быть использована для вычисления начальных условий в начале состояния *i* + 1 из вероятностей состояний в конце состояния проверки *i*. В результате получают следующее уравнение:

$$\begin{bmatrix} P_{DU}(0) \\ P_W(0) \\ P_R(0) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} P_{DU}(\tau) \\ P_W(\tau) \\ P_R(\tau) \end{bmatrix} = \vec{P}_{i+1}(0) = [L]\vec{P}_i(\tau). \quad (Б.46)$$

Замена $\vec{P}_i(\tau)$ его значением приводит уравнение к рекуррентному виду, что позволяет вычислить начальные условия в начале каждого проверочного интервала по выражению

$$\vec{P}_{i+1}(0) = [L]e^{t[M]}\vec{P}_i(0). \quad (Б.47)$$

Данное выражение может быть использовано для вычисления вероятностей в любой момент времени $t = i\tau + \zeta$. Например, во время тестового интервала i получают следующее выражение:

$$\vec{P}_{i+1}(0) = [L]e^{t[M]}\vec{P}_i, (i-1)\tau \le t < i\tau, \zeta = 1 \text{ по модулю 2.} \quad (Б.48)$$

Получить значение мгновенной недоступности можно путем простого суммирования вероятностей состояний, когда система недоступна. Для выражения мгновенной недоступности применяют линейный вектор q_k

$$U(t) = \sum_{k=1}^{n} q_k P_k(t), \quad (Б.49)$$

где $q_k = 1$ означает, что система недоступна в состоянии k, иначе $q_k = 0$.

Для простой модели получается выражение

$$\text{PFD}(t) = U(t) + P_{DU}(t) = P_R(t), \quad (Б.50)$$

зубчатая кривая представлена на рисунке Б.25.

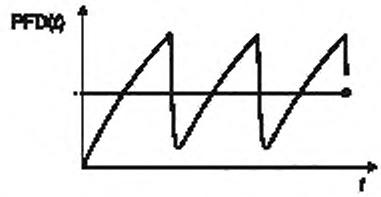


Рисунок Б.25 — Зубчатая кривая, полученная с помощью многофазного марковского подхода

PFD_{avg} вычисляют описанным ранее способом через MDT по Б.4.4, что легко получить из среднего учтенного времени (MCT — от английского «Mean Cumulated Times»), проведенного системой в этих состояниях

$$\overline{\text{MCT}}(T) = \sum_{0}^{T} \vec{P}(t)\text{dt}.$$

Как и для $\vec{P}(t)$, существуют эффективные алгоритмы для вычисления этого интеграла на отрезке [0, T] и окончательно получают

$$\text{PFD}_{avg}(T) = \frac{1}{T}\sum_{k=1}^{n} q_k \text{MDT}_k(T). \quad (Б.51)$$

Применяя формулу (Б.52) к модели, показанной на рисунке Б.24, определяют:

$$\text{PFD}_{avg}(T) = \frac{1}{T}\left[\text{MCT}_{DU}(T) + \text{MCT}_R(T)\right]. \quad (Б.52)$$

Из формулы (Б.53) можно исключить первое слагаемое, если УО выключено в момент ремонта.

Черная точка на рисунке Б.25 — это PFD_{avg} зубчатой кривой для всего периода вычислений.

Необходимо отметить, что указанные выше вычисления обычно проводят с использованием приближенной модели Маркова, показанной на рисунке Б.26, где состояния DU и R связаны и где $\tau/2$ (т. е. среднее время до обнаружения отказа) используют как эквивалент времени восстановления. Это верно, если только в целях нахождения данного равенства уравнение Маркова решено ранее другим методом. Приближение применимо, только если время ремонта незначительно. Применение данного метода может оказаться затруднительным для больших сложных систем.

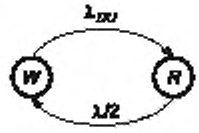


Рисунок Б.26 — Приближенная модель Маркова

Простая модель, показанная на рисунке Б.24, может быть усовершенствована для более реальных компонентов. На рисунке Б.27 показана матрица связей влияния на отказы самого запроса, моделирующая тот компонент, который может оказаться в состоянии отказа при запросе (т. е. реальный отказ при запросе) с вероятностью γ, или может оказаться, что отказ не обнаружен при проверке (из-за ошибки человека) с вероятностью σ.

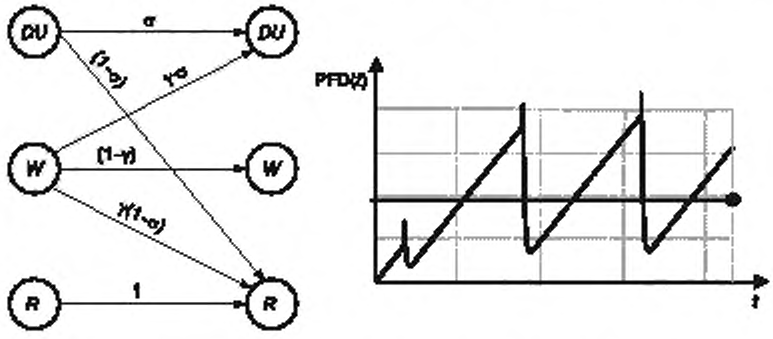


Рисунок Б.27 — Влияние на отказы самого запроса

При каждой проверке вид зубчатой кривой изменяется, и наблюдаемые скачки соответствуют вероятности отказа γ. И вновь черная точка на графике представляет собой PFD_{avg}.

Когда (резервный) компонент отключен для проверки, он становится недоступным во время всего проведения испытания, и это влияет на его PFD_{avg}. Таким образом, должна быть учтена продолжительность проверки π и введена дополнительная фаза между проверочными интервалами. Это показано на рисунке Б.28, где состояния *R* и *W* смоделированы в данной фазе только для полноты картины.

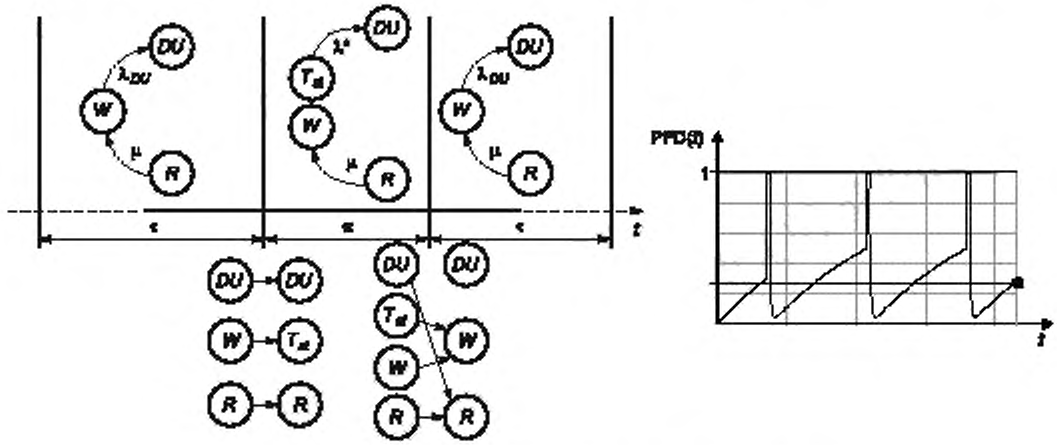


Рисунок Б.28 — Моделирование влияния продолжительности проверки

В данной марковской модели система недоступна в состояниях *R*, *DU* и T_{st}. Это несколько сложнее, чем раньше, но принцип расчетов остается точно таким же. Поведение зубчатой кривой показано на рисунке Б.28 справа — система недоступна во время проверок, и это может быть основным вкладом в PFD_{avg}.

На предыдущем марковском графе рассмотрены только опасные необнаруженные отказы, но опасные обнаруженные отказы также могут быть представлены. Отличие в том, что ремонт начинается точно в тот момент, который показан на рисунке Б.29. Таким образом, μ_{DD} — это интенсивность восстановления компонента (μ_{DD} = 1/MTTR), а μ_{DU} — интенсивность ремонта (μ_{DU} = 1/MRT).

В случае необходимости должны быть отражены и безопасные отказы, но в данном случае для простоты это не сделано.

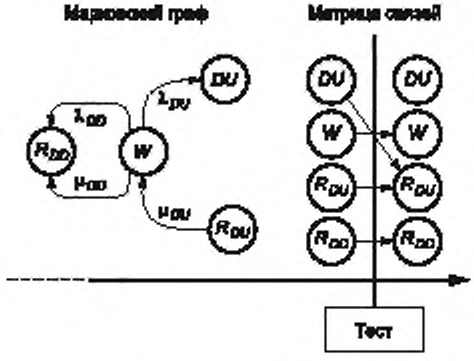


Рисунок Б.29 — Многофазная модель Маркова с отказами *DD* и *DU*

Основная проблема с марковскими графами заключается в том, что количество состояний растет экспоненциально с увеличением числа компонентов изучаемой системы. Так что построение марковских графов и проведение указанных выше расчетов вручную без достаточного приближения очень быстро становится невыполнимым.

Решить вопрос со сложностями вычислений помогает использование эффективных программных пакетов для марковских моделей. Существует внушительное количество доступных пакетов, даже если они не обязательно применимы непосредственно для вычислений PFD_{avg}: большинство пакетов предназначено для вычисления мгновенной недоступности, но только некоторые из них позволяют рассчитать среднее накопленное время нахождения системы в конкретных состояниях, и только единицы дают возможность производить многофазное моделирование. В любом случае их не так сложно адаптировать для вычисления PFD_{avg}.

Что касается непосредственно моделирования, то, если зависимости между компонентами слабые, марковский и логический подходы могут быть объединены следующим образом:

- марковская модель может быть использована для установления мгновенной недоступности для каждого из компонентов;
- деревья отказов или блок-схемы надежности используют для объединения отдельных недоступностей для вычисления мгновенной недоступности PFD(t) всей системы;
- PFD_{avg} получают путем усреднения PFD(t).

Такой подход описан в разделе Б.4, и зубчатые кривые, подобные тем, что показаны на рисунках Б.25, Б.27 и Б.28, могут быть использованы как входные данные для деревьев отказов.

Если зависимостями между компонентами не представляется возможным пренебречь, то можно воспользоваться какими-либо инструментами для автоматического построения марковского графа. Они основаны на моделях более высокого уровня, чем марковские (например, сети Петри или формальный язык). Из-за комбинаторного взрыва количества состояний их применение все равно может быть сопряжено с трудностями.

Для моделирования сложных систем крайне эффективен представленный ниже объединенный подход.

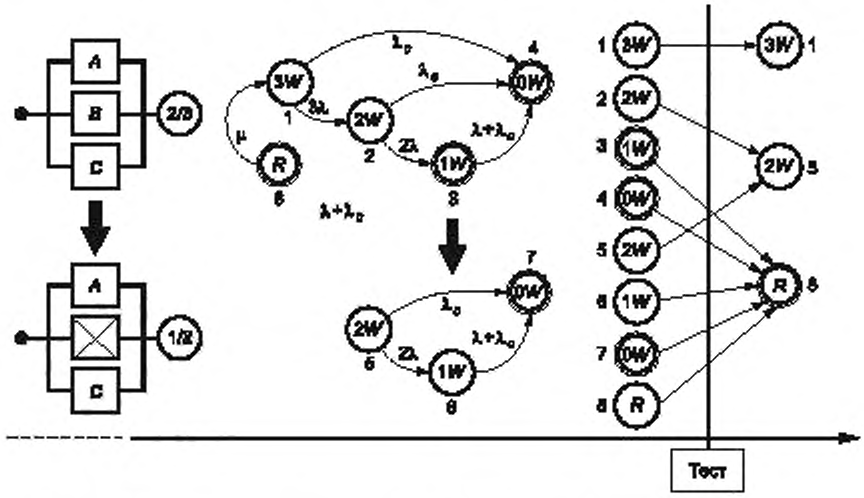


Рисунок Б.30 — Изменение логики (с 2oo3 на 1oo2) вместо ремонта первого отказа

Система, смоделированная на рисунке Б.30, состоит из трех компонентов, проверяемых в одно и то же время и работающих по схеме 2oo3. Когда отказ обнаружен, логика меняется с 2oo3 на 1oo2, т. к. логика 1oo2 лучше, чем 2oo3 с точки зрения безопасности (но хуже с точки зрения ложного отказа). И только в случае обнаружения второго отказа должен произойти ремонт, который включает в себя замену всех трех элементов на новые. Это вносит системные ограничения, поэтому невозможно построить поведение всей системы простым объединением поведения независимых компонентов.

Б.5.2.2 Принцип расчета

Аналогичный тип мультифазного марковского моделирования может быть использован для расчета PFH для *DU* отказов, обнаруженных контрольными проверками. В целях упрощения будет показан только принцип вычисления PFH для *DD* отказов, для которых нужны только обычные (однофазные) модели Маркова. Конечно, для Э/Э/ПЭ СБЗС систем, работающих в режиме с непрерывным запросом и имеющих обнаруженные периодическими контрольными проверками *DU* отказы, должен быть использован многофазный марковский подход. Это не меняет принцип, рассматриваемый ниже.

На рисунке Б.31 показаны два марковских графа с поглощающим состоянием, моделирующих одну и ту же систему, выполненную из двух дублирующих компонентов с общей причиной отказа. Компоненты *A* и *B*, показанные в левой части рисунка, могут быть отремонтированы, а в правой части рисунка — такая возможность отсутствует.

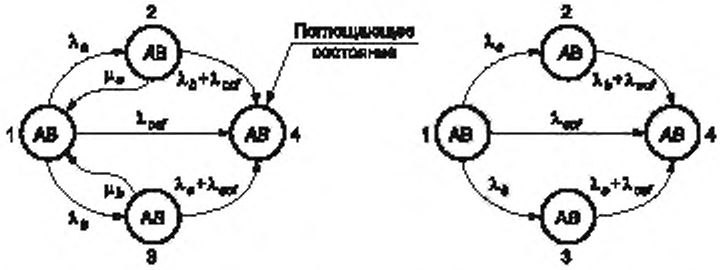


Рисунок Б.31 — Марковский граф «надежности» с поглощающим состоянием

На обоих графах состояние 4 (*AB*) является поглощающим. Система остается отказавшей после отказа всей системы, и $P(t) = P1(t) + P2(t) + P3(t)$ — это вероятность того, что не произошло отказа на промежутке [0; *t*]. Тогда $R(t) = P(t)$ является надежностью системы, а $F(t) = 1 — R(t) = P4(t)$ — это ее ненадежность. Как обсуждалось в пункте Б.2.3, возможно использование модели надежности для обработки такой ситуации, когда отказ Э/Э/ПЭ СБЗС системы незамедлительно приводит к опасной ситуации. При этом μ_a и μ_b являются интенсивностями восстановления компонентов (т. е. $\mu_a = 1/\mathrm{MTTR}_a$ и $\mu_b = 1/\mathrm{MTTR}_b$).

Такой марковский граф надежности позволяет получить PFH непосредственно, учитывая, что PFH = $F(T)/T$. Например, на основе рисунка Б.31 можно непосредственно получить PFH(T) = $P_4(T)/R$ [при условии, что $P_4(T) << 1$)].

Такой марковский граф надежности позволяет также вычислять MTTF системы по следующей формуле:

$$\text{MTTF} = \lim_{n \to \infty} \sum_{k=1}^{n} a_k \text{MCT}_k(t), \tag{Б.53}$$

где $\text{MCT}_k(t)$ — среднее накопленное время нахождения в состоянии k и $i_k = 1$, если k является нормальным рабочим состоянием, и $i_k = 0$ во всех других случаях.

Верхние границы можно получить следующим образом:

$$\text{PFH} = 1/\text{MTTF}.$$

Эффективные алгоритмы расчета известны, и почти все программные пакеты для марковских моделей могут быть использованы для расчетов $F(t)$ и MTTF.

Указанные выше ожидания для PFH верны для всех случаев, даже если интенсивность отказов всей системы непостоянна (как для графа, расположенного справа на рисунке Б.31). Единственное ограничение состоит в том, что нужно использовать марковский граф надежности с одним (или несколькими) поглощающим(ими) состоянием(ями). Это применимо и при использовании многофазных моделей.

Когда все состояния являются полностью и быстро восстановимыми, общая интенсивность отказов системы стремится к асимптотическому значению $\Lambda_{as} = 1/\text{MTTF}$. В таких графах, за исключением исходных и поглощающих состояний, все остальные состояния являются квазимгновенными (так как значения MTTR для компонентов существенно меньше их MTTF). Это позволяет непосредственно вычислять постоянные интенсивности отказов всей системы для каждого сценария, начиная от исходного и заканчивая поглощающим состоянием. Марковский граф слева на рисунке Б.31 моделирует такую полностью и быстро восстанавливаемую систему. Так что:

$1 \to 4$: $\Lambda_{14} = \lambda_{ccf}$.

$1 \to 2 \to 4$: $\Lambda_{124} = \lambda_a \left(\lambda_b + \lambda_{ccf}\right) / \left[\left(\lambda_a + \lambda_{ccf}\right) + \mu_a\right] \approx \lambda_a \left(\lambda_b + \lambda_{ccf}\right) / \mu_a$. (Б.54)

$1 \to 3 \to 4$: $\Lambda_{134} = \lambda_a \left(\lambda_{ba} + \lambda_{ccf}\right) / \left[\left(\lambda_b + \lambda_{ccf}\right) + \mu_a\right] \approx \lambda_a \left(\lambda_b + \lambda_{ccf}\right) / \mu_a$.

В формуле (Б.55) для сценария $1 \to 3 \to 4$ λ_b — вероятность перехода из исходного состояния, а $(\lambda_a + \lambda_{ccf})/\mu_b$ — вероятность перехода в состояние 4 предпочтительнее возврата в состояние 1, если система оказалась в состоянии 3.

Наконец: $\Lambda_{as} = \Lambda_{12} + \Lambda_{124} + \Lambda_{134} = 1/\text{MTTF}$.

Это можно легко обобщить для сложных марковских графов, но оно верно лишь для полностью и быстро восстановимых систем, т. е. *DD* отказов.

Марковский граф справа на рисунке Б.31 не является полностью и быстро восстановимым. Так что использование приведенных выше вычислений даст неправильный результат.

Если Э/Э/ПЭ СБЗС система, работающая в режиме с непрерывным запросом, использована вместе с другими слоями безопасности, то должна быть рассмотрена ее готовность. Это показано на обоих графах на рисунке Б.32, на котором отсутствует поглощающее состояние, и система восстанавливается после полного отказа. $P(t) = P1(t) + P2(t) + P3(t)$ — вероятность того, что система работает в момент времени t. Тогда $A(t) = P(t)$ является готовностью, а $U(t) = 1$ — $A(t) = P4(t)$ — неготовностью.

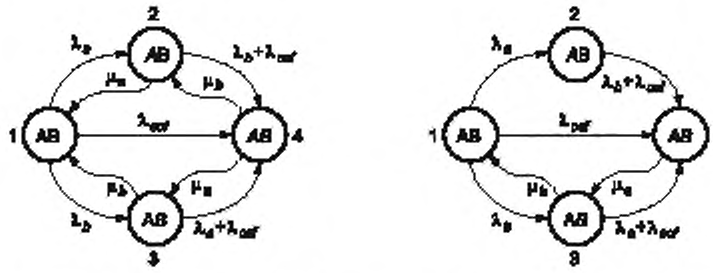


Рисунок Б.32 — Марковский граф «готовности» без поглощающих состояний

Данный случай существенно отличается от примера, приведенного на рисунке Б.31, поэтому $R(t)$ и $A(t)$ должны быть использованы корректно так же, как $U(t)$ и $F(t)$, если необходимо получить корректные результаты.

В случае *DD* отказов простейшим путем решения такой проблемы является вычисление верхней границы PFH через MDT и MUT, как показано в Б.2.3.

Примечательное свойство марковских графов готовности состоит в том, что они достигают асимптотического равновесия, когда вероятность перехода в данное состояние равна вероятности перехода из него. Отмечают:

- $P_{i,\ as} = \lim_{t\to\infty} P_i(t)$ — асимптотическое значение $P_i(t)$;
- $\lambda_i = \sum_{j\neq i}\lambda_{ij}$ — вероятность переходов из состояния i в любое другое. Каждый раз, когда система переходит в состояние i, среднее время нахождения в этом состоянии равно $\mathrm{Mst}_i = 1/\lambda_i$. Это позволяет вычислить

$$\mathrm{MUT} = \sum_i (1-q_i)P_{i,\ as}\mathrm{Mst}_i \text{ и } \mathrm{MDT} = \sum_i q_i P_{i,\ as}\mathrm{Mst}_i,$$

где $q_i = 0$, если i — рабочее состояние, и $q_i = 1$ в противном случае.

В результате получаем следующее выражение:

$$\mathrm{PFH} = 1/(\mathrm{MUT}+\mathrm{MDT}) = 1/\sum_i P_{i,\ as}\mathrm{Mst}_i = 1/\sum_i \frac{P_{i,\ as}}{\lambda_i}. \qquad (Б.55)$$

Необходимо отметить, что число отказов, произошедших в период $[0, T]$, равно

$$n = T/\sum_i \frac{P_{i,\ as}}{\lambda_i}.$$

Поскольку большинство марковских программных пакетов способно находить асимптотические вероятности, особые трудности не возникают для выполнения приведенных выше расчетов.

Если период рассмотрения чрезвычайно мал для сходимости марковского процесса, то PFH может быть получена как $w(t) = \Sigma_i \lambda_{if} P_i(t)$. В результате получают:

$$\mathrm{PFH} = \sum_{i\in f}\lambda_i \frac{\int_0^T P_i(t)\,\mathrm{dt}}{T} = \sum_{i\in f}\lambda_{if}\mathrm{MCT}_i(T)/T. \qquad (Б.56)$$

Сложность для проведения подобных вычислений в специальном программном пакете, подставив накопленное время для каждого из состояний, отсутствует.

В случае полностью и быстро восстанавливаемых систем (*DD* отказы) функция интенсивности отказов Веселя (*Vesely*) $\lambda_V(t)$ быстро сходится к асимптотическому значению Λ_{as}, которое является приемлемым приближением постоянной интенсивности отказа всей системы. Таким образом, PFH может быть получена так же, как и для безотказности.

Случай *DU* отказов является наиболее сложным ввиду многофазного моделирования. Формула (Б.57) может быть обобщена следующим образом:

$$PFH(T) = \sum_{\varphi=1}^{n}\sum_{i\neq f}\lambda_{if}MCT_i\left(T_{\varphi}\right) / \sum_{\varphi=1}^{n}T_{\varphi}, \quad (Б.57)$$

где T_{φ} — продолжительность фазы φ.

Многофазные марковские процессы, как правило, достигают равновесия, когда вероятность перехода из заданного состояния равна вероятности перехода в него. Асимптотические значения не имеют общих значений с теми, которые описаны выше, но они могут быть использованы в формуле (Б.58).

Необходимо отметить, что марковский подход предоставляет множество возможностей для вычисления PFH Э/Э/ПЭ СБЗС системы, работающей в режиме с непрерывным запросом. Однако для корректного применения марковского подхода необходимо четкое понимание лежащего в его основе математического аппарата.

Б.5.3 Сети Петри и метод моделирования Монте-Карло

Б.5.3.1 Принцип моделирования

Эффективным способом моделирования динамических систем является создание конечного автомата, поведение которого настолько близко к поведению изучаемой Э/Э/ПЭ СБЗС системы, насколько это возможно. Сети Петри [см. ГОСТ 34332.5—2021 (пункты. Б.2.3.3 и Б.2.5.6)] и ГОСТ Р 51901.5 являются эффективным средством для этой цели по следующим причинам:

- их легко обрабатывать графически;
- размер моделей растет линейно относительно числа моделируемых компонентов;
- они гибкие и позволяют моделировать большинство ограничений;
- они идеально подходят для моделирования с использованием метода Монте-Карло [см. ГОСТ 34332.5—2021 (пункт Б.6.5.8) и ГОСТ 34100.3.1].

Разработанные в 60-х годах для формального доказательства в теории автоматов, сети Петри были активно применены инженерами по надежности для решения двух задач: автоматизации построения больших марковских графов и в 80-х годах — для моделирования с использованием метода Монте-Карло.

Типичная подсеть Петри для простого периодически проверяемого компонента состоит из трех частей:

- статическая часть (т. е. рисунок):

а) позиции (круги) соответствуют возможным состояниям,

б) переходы (прямоугольники) соответствуют возможным событиям,

в) стрелки вверх (от позиций к переходам) разрешают переходы,

г) стрелки вниз (от переходов к позициям) показывают, что происходит, когда запускается переход;

- часть планирования:

а) стохастические задержки являются случайными задержками, произошедшими до события,

б) детерминированные задержки — это известные задержки, произошедшие до события;

- динамическая часть:

а) метки (маленькие черные точки), которые двигаются, когда происходит событие, для отображения того, какое из возможных состояний достигнуто,

б) предикаты (любая формула, которая может быть истинной или ложной), разрешающие переходы,

в) утверждения (любые выражения), обновляющие какие-либо переменные, когда переход запускается. Кроме того, существует ряд правил разрешения и запуска перехода.

Кроме того, существует ряд правил разрешения и запуска перехода:

- разрешение перехода (т. е. условия для соответствующего события, которое может произойти):

а) все входные позиции имеют как минимум одну метку,

б) все предикаты должны быть истинными;

- запуск перехода (т. е. что происходит, когда соответствующее событие реализуется):

а) одна метка удаляется из входной позиции,

б) одна метка добавляется в выходную позицию,

в) утверждения обновляются.

Большинство понятий, связанных с сетями Петри, введены выше, остальные — по мере необходимости.

Б.5.3.2 Принцип моделирования Монте-Карло

Моделирование Монте-Карло представляет собой анимацию моделей поведения с помощью случайных чисел для определения того, как часто система остается в состояниях, управляемых либо случайными, либо детерминированными задержками [см. также ГОСТ 34332.5—2021 (пункт Б.6.5.8)].

Это можно объяснить с помощью сети Петри, представленной на рисунке Б.33.

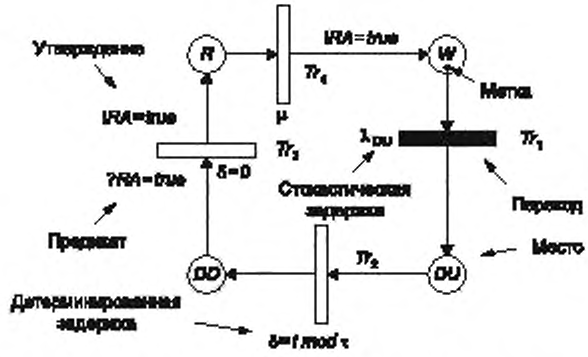


Рисунок Б.33 — Сеть Петри для моделирования одного периодически проверяемого компонента

Последовательность моделирования следующая:

- вначале метка находится в позиции *W* и компонент в нормально работающем состоянии;
- в данном состоянии может появиться только одно событие — опасный необнаруженный отказ (переход Tr_1 разрешен и закрашен черным);
- время, проведенное в данном состоянии, является случайной величиной и зависит от экспоненциального распределения параметра λ_{DU}. Метод Монте-Карло состоит в использовании случайных чисел (см. ниже) для вычисления задержки d_1 перед отказом, который должен произойти (т. е. должен быть запущен переход Tr_1);
- по завершении времени d_1 запускается переход Tr_1, и метка перемещается в позицию *DU* (точнее, одна метка удаляется из позиции *W* и одна метка добавляется в позицию *DU*);
- компонент оказывается в состоянии опасного необнаруженного отказа и переход Tr_2 становится разрешенным;
- обнаружение опасного отказа происходит после детерминированной задержки d_2 ($d_2 = t$ *modulo* T, где t — текущее время, τ — интервал проверки) (таким образом моделируется проверочный интервал);
- по истечении времени t_2, т. е. когда опасный отказ обнаружен, метка переходит на позицию *DD* (теперь компонент ожидает ремонта, и переход Tr_3 становится разрешенным);
- задержка d_3 для запуска перехода Tr_3 (начала ремонта) не зависит от самого компонента, но готовность ресурсов для ремонта представляется сообщением *RA* (это регулируется событием, происходящим из другой части всей сети Петри, не представленной на рисунке Б.33);
- ремонт начинается в тот момент, когда у ремонтной бригады появляется готовность (т. е. ?*RA* = *true* становится истинным), метка переходит в позицию *R*. Ремонтные ресурсы мгновенно становятся неготовыми для другого ремонта, и равенство !*RA* = *false* используется для обновления значения *RA* (это предотвращает проведение еще одного ремонта в это же время);
- случайный переход Tr_4 (т. е. окончание ремонта) становится разрешенным, и может быть рассчитана задержка *d*4 при помощи случайного числа, соответствующего интенсивности ремонта μ;
- по истечении d_4 запускается переход Tr_4, и компонент повторно возвращается в нормальное рабочее состояние (метка переходит в позицию *W*). Ремонтные ресурсы вновь становятся готовыми, и *RA* обновляется посредством утверждения !*RA* = *true*;
- и так далее до тех пор, пока запуск следующего разрешенного перехода попадает в заданный период [0, *T*].

Если следующий запуск не попадает в период [0, *T*], то моделирование останавливается, и в результате для компонента формируется одна история. Во время формирования такой истории могут быть зафиксированы соответствующие параметры в виде их значений для маркируемых позиций (например, отношение времени нахождения метки в конкретной позиции ко времени *T*), частоты запуска переходов, время до первого появления заданного события и т. д.

Идея метода Монте-Карло состоит в том, что формируется огромное количество таких историй и выполняется их статистическая обработка для получения адекватных параметров процесса.

В отличие от аналитических вычислений метод Монте-Карло позволяет легко объединять детерминированные и случайные задержки, для которых может быть выполнено моделирование на основе их кумулятивного распределения вероятностей $F(d)$ и случайных чисел z_i на отрезке [0, 1]. Такие случайные числа имеются почти в любом языке программирования, и разработаны мощные алгоритмы для подобного моделирования.

Затем случайная величина (*di*), распределенная в соответствии с $F(d)$, получается из случайной величины (z_i) при помощи операции: $d_i = F^{-1}(z_i)$. Это довольно просто, если существует аналитическое выражение для $F^{-1}(zi)$, как, например, для экспоненциально распределенной задержки $d_i = \frac{1}{\lambda_{DU}} \log(z_i)$.

Точность моделируемого параметра (X_i) обеспечивается статистическим анализом, который позволяет рассчитать среднее значение, дисперсию, стандартное отклонение и доверительный интервал моделируемого параметра:

- среднее значение: $\bar{X} = \sum_i \bar{x}_i / N$;

- дисперсия: $\sigma^2 = \sum_i (x_i - \bar{X})^2 / N$,

- стандартное отклонение: σ;

- 90-процентный доверительный интервал для $\bar{X}$: $Conf = 1{,}64\frac{\sigma}{\sqrt{N}}$.

Таким образом, при использовании метода Монте-Карло всегда можно предсказать точность результатов. Например, 90-процентная вероятность того, что истинный результат X принадлежит интервалу $\left[\bar{X} - 1{,}64\sigma / \sqrt{N}\right], \left[\bar{X} + 1{,}64\sigma / \sqrt{N}\right]$.

Данный интервал уменьшается, когда число историй возрастает и когда частота появления X растет.

На современных персональных компьютерах для Э/Э/ПЭ СБЗС систем несложно выполнить вычисления вплоть до УПБ 4.

Б.5.3.3 Принцип расчета

Подсеть Петри на рисунке Б.33 можно непосредственно использовать для оценки PFD_{avg} компонента, потому что значение одного из параметров маркируемой позиции W, которое равно отношению времени нахождения метки в позиции W ко времени T, в действительности является средним значением готовности компонента A. В результате получают:

$$PFD_{avg} = 1 - A. \qquad (Б.58)$$

Точность вычислений, как было показано выше, можно оценить, используя статистический анализ.

Более сложное поведение можно представить, используя специальные подсети Петри. На рисунке Б.34 показана идея, как можно выполнить моделирование периодически проверяемых компонентов, отказы по общей причине (*CCF*) и ремонтные ресурсы.

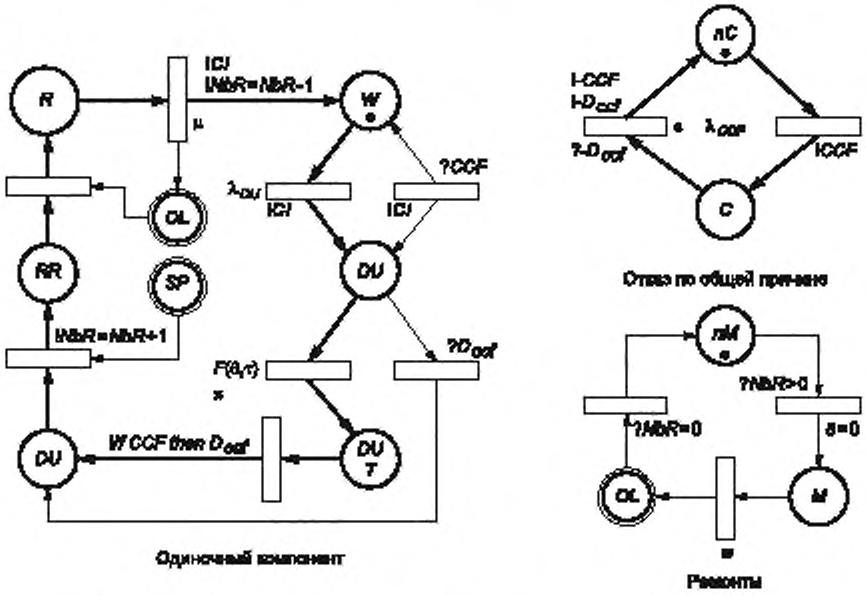


Рисунок Б.34 — Сеть Петри, моделирующая отказ по общей причине и ремонтные ресурсы

Слева представлена модель периодически проверяемого компонента, который переходит из одного состояния в другое состояние: рабочее состояние (*W*), опасный необнаруженный отказ (*DU*), проверка (*DUT*), опасный обнаруженный отказ (*DD*), готовность к ремонту (*RR*) и ремонт (*R*).

Когда происходит отказ (*DU*), формируется сообщение !-C_i (эквивалентное !C_i = *false*), указывающее, что компонент отказал. Затем компонент находится в режиме ожидания периодической проверки (*DUT*). Интервал периодической проверки равен τ и смещение равно θ. После выполнения проверки в течение времени, равного π, система переходит в состояние *DD*. Если запасные части готовы (хотя бы одна метка в *SP*), то компонент становится готовым к ремонту (*RR*), и переменная *NbR* увеличивается на 1, чтобы проинформировать ремонтные ресурсы о числе компонентов, которым необходим ремонт. После того как ремонтные ресурсы доставлены к месту ремонта (одна метка в *OL*), начинается ремонт (*R*), и метка из *OL* удаляется. Когда вновь достигается нормально работающее состояние компонента, то формируется сообщение !*Ci* (т. е. !*Ci* = *true*), *NbR* уменьшается на 1 и метка возвращается обратно в *OL*, что разрешает выполнять дальнейшие ремонты и т. д.

В подсетях Петри, моделирующих ремонт, использована переменная *NbR*. Когда ее величина становится более 0, начинается мобилизация ресурсов (*M*), и после определенной задержки они готовы выполнять работы на месте (*OL*). Метка в *OL* применена для проверки того, начался ли ремонт одного из отказавших компонентов. Таким образом, в каждый момент времени может быть осуществлен только один ремонт. После выполнения всех ремонтов (т. е. *NbR* = 0) ремонтные ресурсы демобилизуются.

На рисунке Б.34 также представлена модель отказа по общей причине (*CCF*). Когда происходит такой отказ (λ_{DCC}), сообщение !*CCF* становится истинным и используется для того, чтобы все отказавшие по общей причине компоненты были переведены в их состояние *DU*. Соответствующее сообщение C_i становится ложным, и компоненты ремонтируются независимо друг от друга. Когда проверка компонента завершена, утверждение !*FCCF then* D_{ccf} позволяет сообщить всем остальным компонентам, что *CCF* выявлен. Данное сообщение применяется для их незамедлительного перевода в состояния *DD*. Это сообщение также используется для восстановления отказавшей по общей причине подсети Петри, но это делается через некоторое время (ε), для того чтобы обеспечить перевод всех компонентов перед восстановлением в их состояние *DD*.

Подсети Петри, представленные на рисунке Б.34, используют как части более сложных моделей. Один из способов их применения показан на рисунке Б.35, где представлена несколько адаптированная блок-схема надежности, заимствованная из рисунка Б.16, в которую добавлены промежуточные выходы O_i.

Для компонентов *A*, *B*, *C*, *D*, *E*, *F* может быть выполнено моделирование с помощью набора подсетей Петри, представленных на рисунке Б.34, например *CCF* для (*A*, *B*, *C*) и (*E*, *F*) с одними и теми же ремонтными ресурсами для всех компонентов. Остается только проблема связать компоненты вместе в соответствии с логикой блок-схемы надежности и расчета интересующего значения PFD_{avg}.

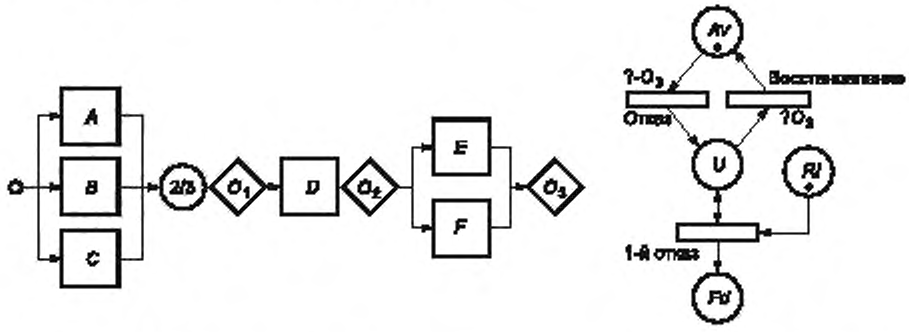


Рисунок Б.35 — Использование блок-схемы надежности для построения сети Петри и вспомогательной сети Петри для вычислений PFD и PFH

Взаимодействие компонентов можно легко выполнить при помощи сообщений C_i и построения следующих равенств:

$$\begin{aligned} C_1 &= C_a C_b + C_a C_c + C_b C_c; \\ C_2 &= O_1 C_d; \\ O_3 &= O_2 (C_b + C_f). \end{aligned} \qquad (Б.59)$$

Таким образом, когда O_3 истинно, вся Э/Э/ПЭ СБЗС система работает четко, иначе она не готова. Это сообщение использовано в подсети Петри с правой стороны для моделирования различных состояний Э/Э/ПЭ СБЗС систем: готовность (*Av*), неготовность (*U*), безотказность (*Rl*) и состояние отказа (*Fd*).

Для расчета PFD важны лишь *Av* и *U*: когда O_3 становится ложным, система отказывает и является неготовой; когда O_3 становится истинным, система восстановлена и опять готова. Выполнить расчет достаточно просто, так как значение нахождения метки в состоянии *Av* — это среднее значение готовности системы, а значение нахождения метки в состоянии *U* — среднее значение неготовности системы, т. е. PFD_{avg}.

Таким образом, в методе Монте-Карло автоматически берется интеграл от мгновенной неготовности, но его не нужно вычислять, за исключением тех случаев, для которых необходима зубчатая кривая. Это можно выполнить достаточно просто, оценив значение нахождения метки в состоянии *U* на всем периоде [0, *T*].

Описанное выше является иллюстрацией основных направлений использования сетей Петри для вычисления УПБ, но потенциальные возможности моделирования безграничны.

Б.5.3.4 Принцип расчета PFH

Для расчета PFH используют такие же принципы, как указаны выше, и для *DU* отказов могут быть использованы точно такие же подмодели. На рисунке Б.36 представлена подсеть Петри, моделирующая отказ, который выявляется и подвергается ремонту, как только будет обнаружен.

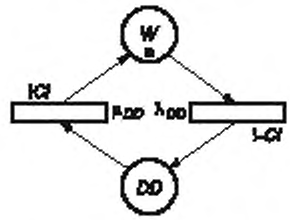


Рисунок Б.36 — Простая сеть Петри для одного компонента с выявляемыми отказами и ремонтами

Как описано выше, такие модели компонентов могут быть использованы вместе с блок-схемами надежности, представляющими всю систему, как на рисунке Б.35.

Если Э/Э/ПЭ СБЗС система работает в режиме с непрерывным запросом и является последним слоем безопасности, то инцидент происходит непосредственно после отказа, и PFH должна вычисляться через надежность системы. Это показано в нижней части подсети Петри, представленной справа на рисунке Б.35. Средняя частота первого отказа системы на отрезке [0, *T*] является ее ненадежностью *F*(*T*). Если значение *F*(*T*) достаточно мало по сравнению с 1, то в соответствии с определением PFH получают: PFH = *F*(*T*)/*T*.

Ввиду того что метка находится в *Rl*, первый отказ является одним коротким переходом. При условии, что все истории ведут к отказу (т. е. период *T* достаточно длительный), среднее время нахождение метки в позиции *Rl* является MTTF — это системы. Таким образом, PFH ≈ 1/MTTF является верхней границей для PFH.

Когда Э/Э/ПЭ СБЗС система, работающая в непрерывном режиме, не является конечным барьером безопасности, то ее выход из строя не приводит непосредственно к аварии. Систему ремонтируют после полного отказа, и ее PFH следует вычислять через неготовность системы. Эту величину получают непосредственно из запуска перехода *Nbf* , моделирующего отказ. Таким образом определяют данные относительно того, сколько раз система отказала в течение указанного периода; в результате PFH = *F*(*T*)/*T*.

Если период *T* является достаточно большим, то MUT может быть рассчитан при помощи накопленного времени MCT_{Av} в состоянии *Av*, а MDT — при помощи среднего накопленного времени MCT_U в состоянии *U*. Средние накопленные времена MCT_A и MCT_U легко вычислить во время моделирования методом Монте-Карло, просто сложив время, когда метка находится в позициях *Av* или *U*. Получают: MUT = MCT_A/*Nbf* и MUT = MCT_U/*Nbf*. Это может быть использовано для вычисления PFH = 1/(MUT + MDT) = 1/MTBF = *Nbf*/*T*.

Эти результаты получают непосредственно, так как метод Монте-Карло легко определяет средние величины. Все описанное выше является лишь иллюстрацией широты использования сетей Петри для расчета УПБ, но реальные возможности моделирования практически безграничны.

Б.5.4 Прочие подходы

Отношение между размером моделей и числом компонентов изучаемой системы существенно изменяется в зависимости от используемого подхода. Для дерева отказов и сетей Петри — это линейное отношение, но для марковских процессов оно — экспоненциальное. Таким образом, для моделирования сложных систем чаще используют деревья отказов и сети Петри, чем марковские процессы. По этой причине сети Петри иногда применяют для создания больших марковских графов.

Формальные языки для описанных выше графических представлений формируют плоские модели: каждый элемент на каждом уровне описывают отдельно. Из-за этого большие модели иногда сложно осваивать и поддер-

живать. Одним из способов решения данной проблемы является использование структурного языка, представляющего компактную иерархическую модель. В последнее время разработан ряд таких формальных языков, доступны также некоторые программные пакеты. В качестве примера можно рассмотреть язык *AltaRica Data Flow*, опубликованный в 2000 г. для свободного использования сообществом по надежности и спроектированный для точного моделирования свойств корректно и некорректно функционирующих промышленных систем.

На рисунке Б.37 показан эквивалент блок-схемы надежности, представленной на рисунке Б.1. Данная модель является иерархической, потому что модели отдельных модулей созданы один раз и затем используются повторно по мере необходимости на разных уровнях моделирования системы. Это позволяет получать предельно компактные модели.

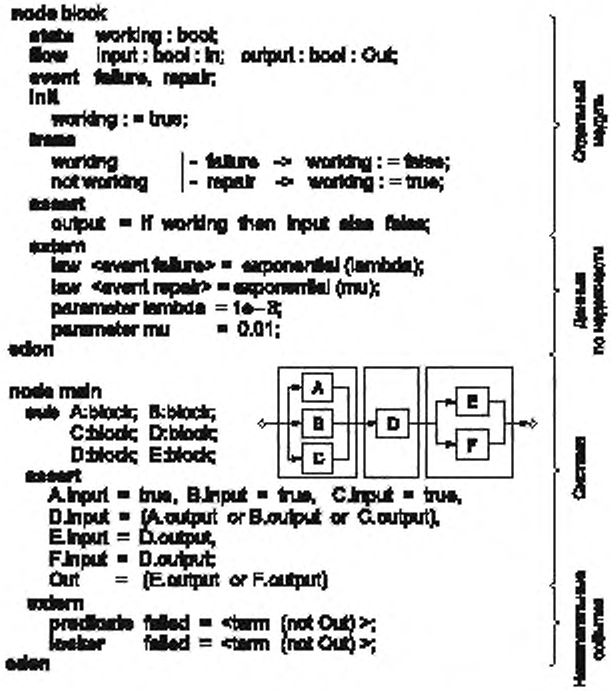


Рисунок Б.37 — Пример моделирования свойств корректно и некорректно функционирующих систем с использованием формального языка

В целях упрощения представления для компонентов отображены только два перехода: отказ и ремонт (т. е. *DD* отказы выявляются и исправляются по мере появления).

Логические операторы («*И*», «ИЛИ») используют для описания логики системы. Это сделано для прямой связи с блок-схемой надежности, и значение переменной *Out* моделирует состояние системы: если система в работоспособном состоянии, то *Out* = *true*; если система в состоянии отказа, то *Out* = *false*. Это позволяет создавать эффективные модели поведения для эффективного моделирования методом Монте-Карло, так что все описанное выше для PFD_{avg} и PFH остается верным и в данном случае. Поэтому далее эта тема не развивается.

Такой формальный язык обладает аналогичными математическими свойствами, как и сети Петри, и поэтому можно компилировать одну модель с другой без особого труда. Это также позволяет обобщать свойства языков дерева отказов и марковских процессов. Поэтому если описание ограничено свойствами марковских процессов или дерева отказов, то можно преобразовать модель в эквивалентный марковский граф или дерево отказов. Ключевые слова «*predicate*» и «*locker*» в конце модели содержат указание на выполнение генерации дерева отказов или марковской модели или на применение метода Монте-Карло.

Использование формального языка, созданного для моделирования поведения корректно и некорректно функционирующих систем, позволяет:

- выполнять моделирование методом Монте-Карло непосредственно на моделях;
- генерировать марковские графы и выполнять аналитические вычисления, как показано ранее (когда язык ограничен марковскими свойствами);

- генерировать эквивалентное дерево отказов и проводить аналитические вычисления, как показано ранее (когда язык ограничен логическими свойствами).

Такие формальные языки, описывающие поведение корректно и некорректно функционирующих систем, являются языками общего назначения. Их можно применять для конкретного анализа Э/Э/ПЭ СБЗС систем. Эти языки предоставляют эффективный способ выполнения вычислений PFD_{avg} и PFH для Э/Э/ПЭ систем, связанных с безопасностью, с несколькими слоями защиты, различными типами режимов отказа, сложными структурами контрольных проверок, зависимостью компонентов, ресурсами обслуживания и т. д., т. е. когда прочие методы не подходят из-за своих ограничений.

Б.6 Обработка неопределенностей

Основная проблема, с которой сталкиваются при вероятностных расчетах, связана с неопределенностями в параметрах надежности. Таким образом, при проведении расчетов PFD и PFH следует оценить, что и как влияет на неопределенность результатов.

К данной проблеме нужно подходить осторожно, но, как показано на рисунке Б.38, использование метода Монте-Карло позволяет ее эффективно решать.

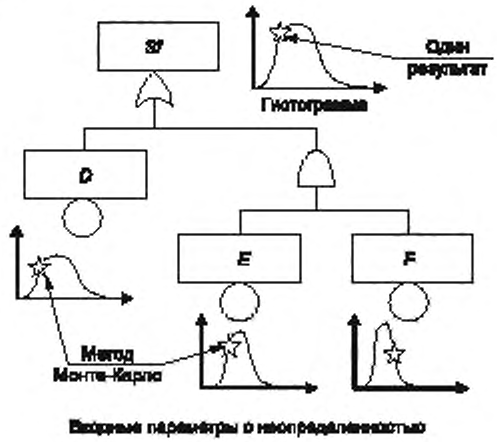


Рисунок Б.38 — Принцип распространения неопределенности

На рисунке Б.38 входные параметры надежности (например, интенсивность необнаруженных опасных отказов) более не являются определенными и поэтому заменены случайными переменными. Плотность вероятности таких случайных величин более или менее «острая» или «плоская» в зависимости от степени неопределенности: плотность вероятности *F* острее, чем *E* или *D*. Это означает, например, что неопределенность *F* менее, чем *E* или *D*.

Порядок вычислений следующий:

а) Генерируют один набор входных параметров при помощи генератора случайных чисел в соответствии с вероятностным распределением данных параметров (аналогично тому, что описано в Б.3.2).

б) Проводят одно вычисление, используя сгенерированный ранее набор входных параметров.

в) Записывают полученный результат (в него входит один результат, используемый на шаге 4).

г) Повторяют шаги с 1 по 3 до тех пор, пока не будет получено достаточное (например, 100 или 1000) число значений, необходимое для составления гистограммы (точечная линия на рисунке Б.38).

д) Выполняют статистический анализ гистограммы для получения среднего значения и стандартного отклонения конечного результата.

Среднее значение гистограммы является PFD_{avg} или PFH в зависимости от выполненных вычислений, а стандартное отклонение определяет неопределенность результатов. Чем меньше стандартное отклонение, тем более точны вычисления PFD_{avg} или PFH.

Представленный выше порядок вычисления для дерева отказов является довольно общим и может быть применен к любому из методов, приведенных в настоящем приложении: упрощенные формулы, марковские процессы и даже сети Петри или формальные языки. Если вычисления по методу Монте-Карло уже проведены, то их нужно повторить.

Распределение вероятности для заданного входного параметра надежности должно быть выбрано в соответствии с собранным знанием о нем. Это может быть:

- равномерное распределение между верхней и нижней границами;
- треугольное распределение с наиболее вероятным значением;

- логнормальное распределение с заданным значением ошибки;
- распределение χ^2 (хи-квадрат) и т. д.

Первое можно оценить технически, когда данных реальных испытаний не очень много. Если данных реальных испытаний много, то можно использовать последнее распределение, так как данные реальных испытаний обеспечивают средние значения параметров, а также доверительные интервалы для этих средних значений.

Например, если наблюдается n отказов в течение накопленного времени наблюдения T, то получают:

- $\lambda = n/T$ — максимальное вероятное ожидание интенсивности отказов;
- $\lambda_{Inf,a} = \frac{1}{2T}\chi^2_{(1-a),2n}$ — нижняя граница с вероятностью α, %, что будет ниже $\lambda_{In\,f,a}$;
- $\lambda_{Sup,a} = \frac{1}{2T}\chi^2_{a,2(n+1)}$ — верхняя граница с вероятностью α, %, что будет выше $\lambda_{Sup,a}$.

Когда α = 5 %, истинное значение λ имеет 90 шансов из 100 принадлежать интервалу $[\lambda_{In\,f,a}, \lambda_{Sup,a}]$. Чем меньше этот интервал, тем точнее значение λ. Обычно эту информацию содержат достоверные базы данных по надежности. Аналитики должны рассматривать данные по надежности, предоставляемые без доверительного интервала (или информации, позволяющей его рассчитать), предельно внимательно.

$\hat{\lambda}$, $\lambda_{In\,f,a}$, $\lambda_{Sup,a}$ могут быть использованы для построения подходящего распределения при моделировании интенсивности отказов $\hat{\lambda}$ заданного режима отказа и его неопределенностей. Это очевидно для распределения χ^2, но и для построения логнормального распределения было показано, что их использование также эффективно. Такой логнормальный закон определяют его средним $\hat{\lambda}$ или его медианой $\hat{\lambda}_{50\,\%}$ и так называемым стандартным отклонением. Это распределение имеет интересное свойство: $\lambda_{In\,f,a} = \lambda_{50\,\%}/ef_a$ и $\lambda_{Sup,a} = \lambda_{50\,\%} \cdot ef_a$.

Тогда оно определяется только двумя параметрами: $\hat{\lambda}$ и $ef_a = \sqrt{\frac{\lambda_{Sup,a}}{\lambda_{Inf,a}}}$.

Если $ef = 1$, то неопределенности отсутствуют, если $ef = 3{,}3$, то верхняя и нижняя границы доверительного интервала различаются почти в 10 раз и т. д. Эти законы могут быть использованы, в свою очередь, вместе с методом Монте-Карло для того, чтобы учесть влияние средних значений и неопределенностей PFD_{avg} и PFH. Поэтому всегда возможно получить значение неопределенности с помощью вероятностных расчетов. Некоторые программные пакеты реализуют такие вычисления непосредственно.

При анализе избыточных систем анализ должен учитывать не только неопределенность интенсивности отказов основного элемента, но также и точность интенсивности *CCF*. Даже если существует набор данных реальных испытаний для элементов, то редко имеется в наличии набор данных реальных испытаний для *CCF*, и, следовательно, это будет вносить наибольшую неопределенность.

Приложение В
(справочное)

Примеры расчета охвата диагностикой и доли безопасных отказов

Метод расчета охвата диагностикой и доли безопасных отказов приведен в ГОСТ 34332.3—2021 (приложение В). Настоящее приложение содержит краткое описание примеров использования данного метода для расчета охвата диагностикой. Предполагается, что информация, представленная в ГОСТ 34332.3, доступна и при необходимости используется при получении значений, приведенных в таблице В.1. Возможные диапазоны охвата диагностикой для некоторых подсистем или компонентов Э/Э/ПЭ систем представлены в таблице В.2. Значения, представленные в таблице В.2, опираются на инженерные оценки.

Чтобы понять все значения таблицы В.1, потребовалась бы подробная схема АС, с помощью которой можно определить влияние всех режимов отказов. Представленные в таблице В.1 значения приведены только в качестве примера (для некоторых компонентов таблицы В.1 охват диагностикой не определен, так как практически невозможно обнаружить все режимы отказов этих компонентов).

Таблица В.1 сформирована нижеприведенным образом:

Для определения влияния каждого вида отказов каждого компонента на поведение системы без диагностических испытаний проведен анализ видов и влияния отказов. Для каждого компонента приведены доли безопасных отказов (*S*) и опасных отказов (*D*) от общей интенсивности отказов, связанные с каждым видом отказов. Для простых компонентов деление на опасные и безопасные отказы может быть четко определено, в остальных случаях — основано на инженерной оценке. Для сложных компонентов, если детальный анализ каждого вида отказа невозможен, считают, что отказы делятся в соотношении: 50 % безопасных, 50 % опасных отказов. Для формирования таблицы В.1 использовались виды отказов, задаваемые именно таким распределением, хотя возможно и другое, более предпочтительное распределение по видам отказов.

Значения охвата диагностикой для каждого конкретного диагностического испытания каждого компонента помещают в столбце DC_{comp} таблицы В.1. В таблице В.1 также приведены конкретные значения охватов диагностикой для обнаружения как безопасных, так и опасных отказов. Показано, что для простых компонентов (например, резисторов, конденсаторов и транзисторов) отказы из-за отсутствия контакта или короткого замыкания обнаруживаются с охватом диагностикой 100 %, тем не менее использование таблицы В.2 ограничивает охват диагностикой значением 90 % для компонента *U*16 комплексного компонента типа *B*.

В столбцах 1 и 2 таблицы В.1 приведены интенсивности безопасных и опасных отказов для каждого компонента при отсутствии диагностических испытаний (λ_S, λ_{DD} и λ_{DU}, соответственно).

Обнаруженный опасный отказ считают фактически безопасным, что позволяет определить отношение между фактически безопасными отказами (т. е. любыми обнаруженными безопасными, необнаруженными безопасными или обнаруженными опасными отказами) и необнаруженными опасными отказами. Интенсивность фактически безопасных отказов определяют произведением значения интенсивности опасных отказов и значения охвата диагностикой для опасных отказов и сложением результата со значением интенсивности безопасных отказов (см. столбец 3 таблицы В.1). Точно так же интенсивность необнаруженных опасных отказов определяют вычитанием охвата диагностикой для опасных отказов из 1 и умножением результата на интенсивность опасных отказов (см. столбец 4 таблицы В.1).

В столбце 5 таблицы В.1 приведены значения интенсивности обнаруженных безопасных отказов, а в столбце 6 таблицы В.1 — значения интенсивности обнаруженных опасных отказов, полученные умножением значения охвата диагностикой на значения интенсивности безопасных и опасных отказов соответственно.

Использование таблицы В.1 дает следующие результаты:

а) общая интенсивность безопасных отказов, включая обнаруженные опасные отказы:

$$\sum\lambda_S + \sum\lambda_{DD} = 9{,}9 \cdot 10^{-7};$$

б) общая интенсивность необнаруженных опасных отказов:

$$\sum\lambda_{DU} = 5{,}1 \cdot 10^{-8};$$

в) общая интенсивность отказов:

$$\sum\lambda_S = \sum\lambda_{DD} + \sum\lambda_{DU} = 1{,}0 \cdot 10^{-6};$$

г) общая интенсивность необнаруженных безопасных отказов:

$$\sum\lambda_{SU} = 2{,}7 \cdot 10^{-8};$$

д) охват диагностикой для безопасных отказов:

$$\frac{\lambda_{SD}}{\lambda_S} = \frac{3,38}{3,65} = 9,3\ \%;$$

е) охват диагностикой для опасных отказов (обычно называемый «диагностический охват»):

$$\frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{6,21}{6,72} = 9,2\ \%;$$

ж) доля безопасных отказов:

$$\frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} + \frac{986}{365+672} = 95\ \%.$$

Без диагностических испытаний интенсивность отказов распределяют следующим образом: 35 % безопасных отказов и 65 % опасных отказов.

Таблица В.1 — Расчет охвата диагностикой и доли безопасных отказов

Компонент	N	Тип	Распределение на безопасные и опасные отказы для каждого вида отказов								Распределение на безопасные и опасные отказы для охвата диагностикой и рассчитанных интенсивностей отказов (10^{-9})/ч						
			Обрыв цепи		КЗ		Изменение значения		Функциональные отказы		DC_{comp}		1	2	3	4	5	6
			ОО	БО	ОО	БО	ОО	БО	ОО	БО	ОО	БО	λ_S	$\lambda_{DD} + \lambda_{DU}$	$\lambda_S + \lambda_{DD}$	λ_{DU}	λ_{SD}	λ_{DD}
Print	1	Печать	0,5	0,5	0,5	0,5	0	0	0	0	0,99	0,99	11,0	11,0	21,9	0,1	10,9	10,9
CN1	1	Con96pin	0,5	0,5	0,5	0,5					0,99	0,99	11,5	11,5	22,9	0,1	11,4	11,4
C1	1	100 нФ	1	0	1	0	0	0	0	0	1	0	3,2	0,0	3,2	0,0	3,2	0,0
C2	1	10 мкФ	0	0	1	0	0	0	0	0	1	0	0,8	0,0	0,8	0,0	0,8	0,0
R4	1	1 М	0,5	0,5	0,5	0,5					1	1	1,7	1,7	3,3	0,0	1,7	1,7
R6	1	100 К									0	0	0,0	0,0	0,0	0,0	0,0	0,0
OSC1	1	OSC24 МГц	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	1	16,0	16,0	32,0	0,0	16,0	16,0
U8	1	74HCT85	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U16	1	MC68000-12	0	1	0	1	0,5	0,5	0,5	0,5	0,90	0,90	260,4	483,6	695,6	48,4	234,4	435,2
U26	1	74HCT74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U27	1	74F74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	14,4	14,4	28,7	0,1	14,3	14,3
U28	1	PAL16L8A	0	1	0	1	0	1	0	1	0,98	0,98	0,0	88,0	86,2	1,8	0,0	86,2
T1	1	BC817	0	0	0	0,67	0	0,5	0	0	1	1	0,0	0,2	0,4	0,0	0,0	0,2
Всего													365	672	986	50,9	338	621

ОО — опасный отказ;
БО — безопасный отказ;
КЗ — короткое замыкание;
DC_{comp} — охват диагностикой для компонента.

Примечания

1 Не обнаружен ни один вид отказа для компонента *R6*, т. е. его отказ не влияет на безопасность и готовность системы.

2 В настоящей таблице интенсивности отказов приведены только для отдельных рассматриваемых компонентов в канале, а не для каждого компонента.

Таблица В.2 — Уровни и диапазоны охвата диагностикой различных подсистем (компонентов)

Компонент	Низкий охват диагностикой	Средний охват диагностикой	Высокий охват диагностикой
Процессор (см. примечание 3):	В сумме менее 70 %	В сумме менее 90 %	—
- регистр	50 % — 70 %	85 % — 90 %	99 % — 99,99 %
- внутренняя регистровая память (см. примечание 3)	50 % — 60 %	75 % — 95 %	—
- блок кодирования и выполнения, включающий регистр тегов (см. примечание 3)	50 % — 70 %	85 % — 98 %	—
- устройство вычисления адреса	50 % — 60 %	60 % — 90 %	85 % — 98 %
- счетчик команд	50 % — 70%	—	—
- указатель стека	40 % — 60 %	—	—
Шина:			
- модуль управления памятью	50 %	70 %	90 % — 99 %
- устройство управления шины	50 %	70 %	90 % — 99 %
Обработка прерываний	40 % — 60 %	60 % — 90 %	85 % — 98 %
Кварцевый тактовый генератор (см. примечание 4)	50 %	—	95 % — 99 %
Контроль выполнения программы:			
- временное (см. примечание 3)	40 % — 60 %	60 % — 80 %	—
- логическое (см. примечание 3)	40 % — 60 %	60 % — 90 %	—
- временное и логическое (см. примечание 5)	—	65 % — 90 %	90 % — 98 %
Постоянная память	50 % — 70 %	99 %	99,99 %
Непостоянная память	50 % — 70 %	85 % — 90 %	99 % — 99,99 %
Дискретное оборудование:			
- цифровой ввод/вывод	70 %	90 %	99 %
- аналоговый ввод/вывод	50 % — 60 %	70 % — 85 %	99 %
- источник питания	50 % — 60 %	70 % — 85 %	99 %
Устройство связи и запоминающее устройство большой емкости	90 %	99,9 %	99,99 %
Электромеханические устройства	90 %	99 %	99,9 %
Датчики	50 % — 70 %	70 % — 85 %	99 %
Оконечные элементы	50 % — 70 %	70 % — 85 %	99 %

Примечания

1 Настоящую таблицу применяют совместно с таблицей ГОСТ 34332.3, в которой приведены анализируемые виды отказов.

2 Если для охвата диагностикой задан конкретный диапазон, то верхние границы интервала могут быть определены только для узкого круга средств контроля или тестирования, которые реализуют чрезвычайно динамичную нагрузку для проверяемой функции.

3 В настоящее время для подсистем, схемы высокого охвата диагностикой которых отсутствуют, средства и методы высокой достоверности диагностики неизвестны.

4 В настоящее время не известны средства и методы средней эффективности для кварцевых генераторов.

5 Низкий диагностический охват для комбинации временного и логического контроля выполнения программы является средним.

Приложение Г
(справочное)

Методика и примеры количественного определения влияния отказов аппаратных средств по общей причине в Э/Э/ПЭ СБЗС системах

Г.1 Общие положения

Г.1.1 Введение

Настоящий стандарт включает в себя ряд методов, рассматривающих систематические отказы. Независимо от эффективности этих методов существует остаточная вероятность возникновения систематических отказов. Это незначительно влияет на результаты расчета безотказности для одноканальных систем. Однако возможность появления отказов, способных повлиять на несколько каналов многоканальной системы (или несколько компонентов в системе безопасности с избыточностью), т. е. отказов по общей причине, приводит к существенным ошибкам при расчетах безотказности многоканальных систем или систем с избыточностью.

В настоящем приложении приведено описание методики, позволяющей учитывать отказы по общей причине при оценке безопасности многоканальных или Э/Э/ПЭ СБЗС систем с избыточностью. Использование данной методики дает более точную оценку полноты безопасности такой системы, чем при игнорировании отказов по общей причине.

Методику применяют для расчета значения β-фактора, часто используемого при моделировании отказов по общей причине. Описываемая методика может быть использована для оценки интенсивности отказов по общей причине в случае двух или более параллельно работающих систем, если известна интенсивность случайных отказов АС для одной из этих систем (см. Г.5). Принято считать, что в общее число случайных отказов оборудования будет включено много отказов, которые вызваны систематическими отказами.

В некоторых случаях предпочтительнее применять альтернативные методики, например: если благодаря наличию данных об отказах по общей причине можно получить более точное значение β-фактора или когда число элементов, отказавших по общей причине, более 4. В качестве альтернативной методики, в частности, может быть использован метод биномиальной интенсивности отказов (также называемая «шоковая модель»).

Г.1.2 Краткий обзор

Считается, что отказы в системе возникают из двух различных источников:

- случайные отказы АС;
- систематические отказы.

Предполагается, что отказы первого вида возникают случайно по времени для любого компонента и приводят к отказу канала системы, частью которого является соответствующий компонент, тогда как отказы второго типа появляются незамедлительно и детерминированным образом, когда система достигает такого состояния, в котором существует систематическая ошибка.

Существует некоторая вероятность того, что во всех каналах многоканальной системы могут произойти независимые случайные отказы АС, вследствие чего все каналы одновременно окажутся неработоспособными. Так как предполагается, что такие отказы АС возникают во времени случайно, их вероятность, одновременно возникающая в параллельных каналах, низка по сравнению с вероятностью отказа одного канала. Эта вероятность может быть рассчитана с помощью зарекомендовавших себя методов, но результат может быть более оптимистичным, когда отказы не полностью независимы друг от друга.

Зависимые отказы, как правило, делят на следующие группы:

- отказ по общей причине (*CCF*) вызывает несколько отказов по одной общей причине. Несколько отказов могут произойти одновременно или в течение некоторого периода времени;
- отказы в общем режиме (*CMF*), которые являются частным случаем *CCF*, когда несколько единиц оборудования отказывают в одном режиме;
- каскадные отказы, когда один компонент отказывает вследствие отказа другого компонента.

Термин «*CCF*» обычно используют для обобщения всех видов зависимых отказов, как сделано в настоящем приложении. Зависимые отказы также делятся:

- на зависимые отказы, вызванные понятными детерминированными причинами;
- события возможного остаточного многократного отказа, которые явно не анализируются из-за недостаточной точности их представления, отсутствия явных детерминированных причин их возникновения или отсутствия возможности собрать данные по надежности.

Для первых видов зависимых отказов должны быть выполнены анализ, моделирование и оценка общепринятым способом, и только вторые должны быть обработаны, как показано в настоящем приложении. Тем не менее систематические отказы, которые являются полностью зависимыми отказами, не выявленными во время анализа безопасности (иначе они должны быть устранены), обрабатываются определенным способом, указанным в настоящем стандарте, но данное приложение применяется в основном для случайных зависимых отказов аппаратных средств.

Таким образом, отказы по общей причине, являющиеся следствием одной причины, могут влиять на несколько каналов или несколько компонентов. Данная причина может быть следствием систематической ошибки (например, конструктивной или ошибки технических условий) либо внешнего воздействия, ведущего к преждевременным случайным отказам АС (например, избыточной температуры, возникающей из-за случайного отказа АС, обычного вентилятора, что сокращает время жизни компонентов или нарушает заданные условия окружающей среды для их работы), или комбинации этих факторов. Так как отказы по общей причине чаще влияют на несколько каналов многоканальной системы, то вероятность такого отказа, скорее всего, будет доминирующим фактором при определении общей вероятности отказа многоканальной системы. Если не учитывать этот фактор, то будет трудно получить правильную оценку УПБ.

Г.1.3 Защита от отказов по общей причине

Хотя отказы по общей причине являются следствием одной причины, они не обязательно проявляются во всех каналах одновременно. Например, при отказе вентилятора все каналы многоканальной Э/Э/ПЭ СБЗС системы могут отказать, что ведет к отказу по общей причине. Однако необязательно все каналы нагреваются с одинаковой скоростью или имеют общую критическую температуру. Следовательно, отказы могут возникать в разных каналах в разное время.

Архитектура ПЭ систем позволяет им выполнять внутреннее диагностическое тестирование непосредственно во время работы, что может быть реализовано различными способами, например:

- один канал ПЭ системы одновременно с обеспечением работы входного и выходного устройств может непрерывно выполнять внутреннюю проверку своей работы. На этапе проектирования можно достичь значения тестового охвата, равного 99 %. Если 99 % внутренних сбоев обнаружены до того, как они приведут к отказу, вероятность сбоев одного канала, которые могут в конечном счете стать частью отказов по общей причине, значительно снижается;

- помимо внутреннего тестирования каждый канал ПЭ системы может отслеживать выходы других каналов многоканальной ПЭ системы (или каждое ПЭ устройство может отслеживать другое ПЭ устройство системы, состоящей из нескольких ПЭ устройств). Следовательно, отказ, возникший в одном канале, может быть обнаружен, и один или несколько оставшихся неотказавших каналов будут выполнять перекрестный контроль и инициировать безопасное отключение. (Следует отметить, что перекрестный контроль эффективен, если состояние системы управления постоянно меняется, например: при наличии часто используемой в циклически работающем устройстве защитной блокировки или при внесении в устройство небольших изменений, не влияющих на управляющую функцию.) Интенсивность выполняемого перекрестного контроля может быть достаточно высока, поэтому непосредственно перед неодновременными отказами по общей причине перекрестный контроль, скорее всего, обнаружит первый отказавший канал и позволит перевести систему в безопасное состояние до момента отказа второго канала.

Например, для вентилятора скорость роста температуры и восприимчивость каналов несколько различаются, поэтому второй канал, возможно, откажет спустя несколько десятков минут после первого. Это позволяет после диагностического тестирования инициировать безопасное отключение первого отказавшего канала до того, как по общей причине откажет второй канал.

Таким образом:

- ПЭ системы обладают возможностью формировать барьеры защиты от отказов по общей причине и, следовательно, в меньшей степени подвержены им по сравнению с другими технологиями;

- для ПЭ систем можно использовать β-фактор, отличающийся от β-фактора для других технологий. Следовательно, оценки β-фактора, опирающиеся на предыдущие значения оценки интенсивности отказов, скорее всего, окажутся неправильными (ни одна из известных существующих моделей оценки вероятности отказа по общей причине не учитывает эффект автоматического перекрестного контроля);

- так как разнесенные во времени отказы по общей причине могут быть обнаружены с помощью диагностического тестирования до отказа всех каналов, подобные отказы могут не восприниматься как отказы по общей причине.

Существуют три способа уменьшения вероятности потенциально опасных отказов по общей причине:

- уменьшение общего числа случайных аппаратных и систематических отказов (это уменьшает площади эллипсов, представленных на рисунке Г.1, приводя к уменьшению площади пересечения эллипсов);

- максимальное увеличение независимости каналов (это уменьшает площадь пересечения эллипсов, представленных на рисунке Г.1, не меняя площади самих эллипсов);

- обнаружение неодновременных отказов по общей причине, когда неисправным становится только один канал, до того, как станет неисправным второй, т. е. использование диагностического тестирования или смещения контрольных проверок.

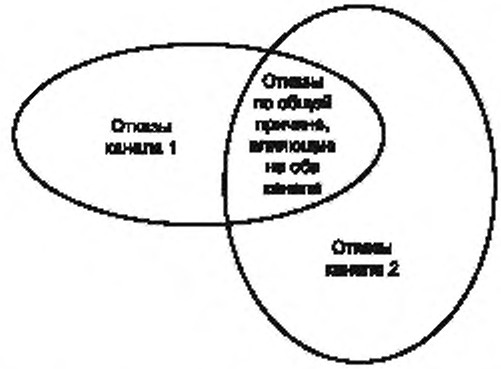


Рисунок Г.1 — Связь между отказами по общей причине и отказами отдельных каналов

В системах с более чем двумя каналами отказ по общей причине может повлиять на все каналы или только на несколько, но не на все, работающие в общем режиме каналы. Таким образом, подход, представленный в данном приложении, в соответствии с первым способом, заключается в расчете значения β для дуплексной системы голосования 1oo2, а затем в использовании повышающего коэффициента для получаемого значения β в зависимости от общего числа каналов и схемы голосования (см. таблицу Г.5).

Г.1.4 Подход, принятый в серии стандартов ГОСТ 34332

Подход ГОСТ 34332 основан на выполнении следующих трех этапов.

Этап 1. Использование методов по ГОСТ 34332.3 и ГОСТ 34332.4 для снижения вероятности систематических отказов всей системы до уровня, соизмеримого с вероятностью случайных отказов АС.

Этап 2. Количественное определение факторов, которые могут быть определены количественно, т. е. учет вероятности случайных отказов АС, как определено в ГОСТ 34332.3.

Этап 3. Определение отношения, связывающего вероятность отказа по общей причине с вероятностью случайного отказа АС с использованием практических средств, которые считаются наиболее эффективными в настоящее время. В настоящем приложении описана методика определения этого отношения.

В большинстве методик оценки вероятности отказов по общей причине формируют прогнозы на основе вероятности случайного отказа АС. Несомненно, непосредственная взаимосвязь между этими вероятностями отсутствует, тем не менее на практике некоторая корреляция между ними найдена и, возможно, является следствием эффектов второго порядка. Например, высокая вероятность случайного отказа АС системы связана:

- с большим объемом обслуживания, который требуется для системы. Вероятность систематического отказа, являющегося следствием обслуживания, зависит от числа проведенных сеансов обслуживания, что также повышает интенсивность воздействия человеческих ошибок, приводящих к отказам по общей причине. Таким образом, возникает связь между вероятностью случайного отказа АС и вероятностью отказа по общей причине. Например:

- после каждого случайного отказа АС требуются ремонт, а за ним тестирование и, возможно, повторная калибровка,

- при заданном УПБ для системы с большей вероятностью случайного отказа АС требуется чаще выполнять контрольные проверки и с большей глубиной/сложностью, что также увеличивает влияние человеческого фактора;

- со сложностью системы. Вероятность случайного отказа АС зависит от числа компонентов и, следовательно, сложности системы. Сложную систему труднее понять, поэтому у нее выше вероятность появления систематических отказов. Кроме того, сложность системы затрудняет обнаружение отказов путем анализа или тестирования и может приводить к тому, что часть логики системы будет выполняться только в редко встречающихся условиях. Это также приводит к появлению связи между вероятностью случайного отказа АС и вероятностью отказа по общей причине.

В настоящее время используют несколько подходов для обработки *CCF* (β-фактор, несколько греческих букв, α-фактор, биномиальная интенсивность отказов и др.). Далее описаны две из актуальных моделей, предлагаемые в настоящем приложении для третьего этапа трехэтапного подхода. Несмотря на ограничения считается, что в настоящее время они представляют собой наиболее приемлемый способ обработки вероятности отказа по общей причине:

- устоявшаяся модель β-фактора, которая широко используется и обычно ее можно задействовать в многоканальных системах вплоть до четырех зависимых каналов/элементов;

- биномиальная интенсивность отказов (также известная как «шоковая модель»), которая может быть использована, когда число зависимых элементов более 4.

При использовании модели β-фактора для Э/Э/ПЭ СБЗС системы возникают следующие две проблемы:

- выбор значения β-фактора. В отдельных источниках представлены диапазоны возможных значений β-фактора, но не определены их конкретные значения, оставляя выбор за пользователем. Для решения этой проблемы методика β-фактора, представленная в настоящем приложении, основывается на применяемом подходе;

- ни в модели β-фактора, ни в шоковой модели не учтены возросшие возможности диагностического тестирования современных ПЭ систем, которыми можно воспользоваться для обнаружения неодновременных отказов по общей причине до того, как отказ полностью проявит себя. Для преодоления этой проблемы существует подход для отражения диагностического тестирования при оценке возможного значения β.

Функции диагностического тестирования, выполняющиеся внутри ПЭ системы, обеспечивают непрерывное сравнение работы ПЭ системы с заранее определенными состояниями. Эти состояния предварительно устанавливают программно или аппаратно (например, с помощью контрольного таймера). Рассматриваемые таким образом функции диагностического тестирования можно считать дополнительными и частично различающимися для каналов, работающих в ПЭ системе параллельно.

Также может быть использован метод перекрестного контроля каналов. Многие годы этот метод применялся в двухканальных системах с взаимной блокировкой, построенных исключительно на реле. Однако релейная технология обычно позволяет проводить перекрестное тестирование только во время изменения состояния каналов, что делает такое тестирование неподходящим для обнаружения неодновременных отказов по общей причине, если системы остаются в одном (например, включенном) состоянии в течение длительного времени. С помощью технологии ПЭ системы перекрестный контроль может быть проведен с высокой частотой.

Г.2 Область применения методики

Область применения методики ограничена отказами по общей причине АС из-за следующих обстоятельств:

- модель β-фактора и шоковая модель связывают вероятность отказов по общей причине с вероятностью случайных аппаратных отказов. Вероятность отказов по общей причине, затрагивающих систему в целом, зависит от сложности системы (в которой главную роль, возможно, играет пользовательское ПО), а не только от сложности самих АС. Очевидно, что в любых расчетах, основанных на вероятности случайного аппаратного отказа, не может быть учтена сложность ПО;

- информирование об отказах по общей причине обычно ограничивается информацией об отказах АС, что является главной обязанностью производителей оборудования;

- моделирование систематических отказов (например, отказов ПО) считается практически неосуществимым;

- целью мероприятий, определенных в ГОСТ 34332.4, является снижение вероятности отказов по общей причине, связанных с ПО, до значения, приемлемого для необходимого УПБ.

Следовательно, оценка вероятности отказа по общей причине, выполненная по данной методике, связана только с аппаратными отказами. Эту методику не допускается использовать для получения интенсивности отказов всей системы, учитывающей вероятность отказа, связанную с ПО.

Г.3 Особенности методики

Так как на датчики, логическую подсистему и исполнительные элементы влияют, например, различные условия окружающей среды и диагностические тесты с разным уровнем возможностей, для каждой из этих подсистем настоящую методику применяют независимо. Например, логическую подсистему стоит поместить в контролируемую среду, а датчики могут быть установлены снаружи и подвергнуты внешнему воздействию.

Программируемые электронные каналы предоставляют возможность для реализации разнообразных функций диагностического тестирования и способны:

- обеспечивать высокий охват диагностикой в пределах конкретных каналов;
- контролировать дополнительные избыточные каналы;
- обеспечивать высокую частоту повторения;
- контролировать с повышенной частотой датчики и/или исполнительные элементы.

Чаще всего отказы по общей причине не возникают одновременно во всех затронутых каналах. Поэтому, если частота повторения диагностического тестирования достаточно высока, большую часть отказов по общей причине можно обнаружить и, следовательно, устранить до того, как будут затронуты остальные доступные каналы.

Не все функции многоканальной системы, обеспечивающие устойчивость к отказам по общей причине, можно проверить с помощью диагностического тестирования. Однако эффективность этих функций, связанных с диверсификацией или независимостью, постоянно повышается. Любая функция, которая, возможно, увеличивает время между отказами каналов в случае неодновременного отказа по общей причине (или уменьшает долю одновременных отказов по общей причине), увеличивает вероятность обнаружения отказа при диагностическом тестировании и перевода установки в безопасное состояние. Следовательно, функции, связанные с устойчивостью к отказам по общей причине, делятся на функции, влияние которых предположительно возрастает при использовании диагностического тестирования и не меняется (см. таблицу Г.1, столбцы *X* и *Y* соответственно).

Таблица Г.1 — Оценка мероприятий защиты программируемых электронных средств или датчиков/исполнительных элементов от возникновения отказов по общей причине

Мероприятие	Логическая подсистема		Датчики и исполнительные элементы	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Разделение/изолирование				
Все ли сигнальные кабели каналов разделены между собой?	1,5	1,5	1,0	2,0
Расположены ли логические подсистемы каналов на отдельных печатных платах?	3,0	1,0	—	—
Расположены ли логические подсистемы каналов в отдельных шкафах?	2,5	0,5	—	—
Если датчики/исполнительные элементы включают в себя собственную управляющую электронику, то расположена ли электроника для каждого канала на отдельной печатной плате?	—	—	2,5	1,5
Если датчики/исполнительные элементы включают собственную управляющую электронику, то расположена ли электроника для каждого канала в различных помещениях и различных шкафах?	—	—	2,5	0,5
Разнообразие/избыточность				
Реализованы ли в каналах различные электрические технологии, например один канал электронный или программируемый электронный, а для другого используются реле?	8,0	—	—	—
Реализованы ли в каналах различные электронные технологии, например один канал — электронный, а другой — программируемый электронный?	6,0	—	—	—
Используют ли устройства различные физические принципы для датчиков, например давления и температуры, анемометр с вертушкой и доплеровский датчик и т. д.?	—	—	9,0	—
Используют ли устройства различные электрические принципы/конструкции, например цифровые и аналоговые, с компонентами от различных производителей (но не уцененные) или с различной технологией?	—	—	6,5	—
Применяется ли низкая диверсификация, например диагностическое тестирование аппаратуры использует одинаковую технологию?	2,0	1,0	—	—
Разнообразие/избыточность				
Применяется ли среднее разнообразие, например, для диагностического тестирования аппаратуры использует различную технологию?	3,0	2,0	—	—
Были ли разработаны каналы различными конструкторами, которые не взаимодействовали между собой в процессе разработки?	1,5	1,5	—	—
Использовались ли для каждого канала различные люди и различные методы тестирования в процессе его пуска?	1,0	0,5	1,0	1,0
Обслуживается ли каждый канал в разное время разными людьми?	3,0	—	3,0	—
Сложность/конструкция/применение/завершенность/опыт				
Предотвращает ли перекрестная связь между каналами обмен любой информацией, кроме используемой для диагностического тестирования или голосования?	0,5	0,5	0,5	0,5
Превышает ли время использования в отрасли методов, применяемых для проектирования аппаратуры, 5 лет?	0,5	1,0	1,0	1,0
Превышает ли время работы с этим же оборудованием в аналогичных условиях 5 лет?	1,0	1,5	1,5	1,5

Продолжение таблицы Г.1

Мероприятие	Логическая подсистема		Датчики и исполнительные элементы	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Проста ли система, например имеет ли она не более 10 входов или выходов на канал?	—	1,0	—	—
Защищены ли входы и выходы от возможного превышения безопасных значений напряжения и тока?	1,5	0,5	1,5	0,5
С запасом ли рассчитаны все устройства/компоненты (например, с коэффициентом 2 или более)?	2,0	—	2,0	—
Оценка/анализ и обратная связь				
Изучены ли результаты анализа видов и влияния отказов или дерево неисправностей для того, чтобы установить источники отказов по общей причине, и устранены ли при проектировании предварительно известные источники отказов по общей причине?	—	3,0	—	3,0
Рассматривались ли отказы по общей причине при анализе проекта при последующем внесении изменений в проект (требуется документальное доказательство действий по анализу проекта)?	—	3,0	—	3,0
Все ли возможные отказы были полностью проанализированы и учтены в проекте (требуется документальное доказательство процедуры)?	0,5	3,5	0,5	3,5
Процедуры/интерфейс пользователя				
Существует ли зафиксированная письменно схема работы, гарантирующая обнаружение отказов (или ухудшение характеристик) всех компонентов, установление корневых причин и проверку других аналогичных вопросов для аналогичных возможных причин отказов?	—	1,5	0,5	1,5
Предусмотрены ли процедуры, обеспечивающие: разнесение обслуживания (включая настройку или калибровку) по времени любой части независимых каналов; возможность выполнения диагностического тестирования помимо ручных проверок, проводимых в ходе очередного обслуживания, между завершением обслуживания одного канала и началом обслуживания другого?	1,5	0,5	2,0	1,0
Определено ли в документированных процедурах обслуживания, что обеспечивающие избыточность компоненты систем (например, кабели и т. д.) должны быть независимы друг от друга и закреплены в устройстве?	0,5	0,5	0,5	0,5
Обеспечивает ли система низкий охват диагностикой (от 60 % до 90 %) и сообщает ли об отказах на уровне модуля, допускающего замену в процессе эксплуатации?	0,5	—	—	—
Обеспечивает ли система средний охват диагностикой (от 90 % до 99 %) и сообщает ли об отказах на уровне модуля, допускающего замену в процессе эксплуатации?	1,5	1,0	—	—
Обеспечивает ли система высокий охват диагностикой (>99 %) и сообщает ли об отказах на уровне модуля, допускающего замену в процессе эксплуатации?	2,5	1,5	—	—
Сообщает ли диагностическое тестирование системы об отказах на уровне модуля, допускающего замену в процессе эксплуатации?	—	—	1,0	1,0
Компетентность/обучение/культура безопасности				
Обучены ли конструкторы (с помощью обучающей документации) понимать причины и следствия отказов по общей причине?	2,0	3,0	2,0	3,0
Обучен ли обслуживающий персонал (с помощью обучающей документации) понимать причины и следствия отказов по общей причине?	0,5	4,5	0,5	4,5

Окончание таблицы Г.1

Мероприятие	Логическая подсистема		Датчики и исполнительные элементы	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Контроль состояния окружающей среды				
Ограничен ли доступ персонала (закрытые шкафы, недоступное размещение компонентов и т. д.)?	0,5	2,5	0,5	2,5
Возможно ли, что система всегда будет работать в заданных диапазонах температур, влажности, коррозии, пыли, вибрации и т. д., в которых ее работа была проверена, без использования внешнего контроля состояния окружающей среды?	3,0	1,0	3,0	1,0
Все ли сигнальные и силовые кабели отделены друг от друга?	2,0	1,0	2,0	1,0
Проверка влияния окружающей среды				
Было ли проверено, что система устойчива ко всем воздействиям окружающей среды (например, ЭМС, температура, вибрация, ударные нагрузки, влажность) на уровне, заданном в соответствующих международных или национальных стандартах?	10,0	10,0	10,0	10,0

Примечания

1 Ряд факторов, связанных с работой системы, сложно предсказать во время проектирования. В таких случаях конструкторы должны убедиться в том, что конечный пользователь системы уведомлен, например, о процедурах, используемых для достижения требуемого уровня полноты безопасности. Необходимая информация должна быть включена в сопроводительную документацию.

2 Значения *X* и *Y* основаны на инженерной оценке и учитывают как косвенное, так и прямое влияние мероприятий. Например, использование модулей, допускающих замену во время эксплуатации, приводит:

- к выполнению ремонтных работ производителем в соответствующих условиях вместо ремонтных работ, выполняемых на месте в менее подходящих условиях. Это вносит свой вклад в значения *Y*, так как снижается вероятность систематических отказов и, следовательно, отказов по общей причине;
- снижению необходимости вмешательства человека на месте и к возможности быстрой замены неисправных модулей, не выключая системы, повышая таким образом эффективность диагностики для идентификации отказов до того, как они станут отказами по общей причине. Это заметно влияет на значения *X*.

Хотя для трехканальной системы вероятность отказов по общей причине, влияющих на все три канала, скорее всего, значительно ниже вероятности отказов, влияющих на два канала, для упрощения методики β-фактора предполагается, что вероятность отказов не зависит от числа затрагиваемых каналов, т. е. возникающий отказ по общей причине затрагивает все каналы. Альтернативой является шоковая модель.

Данных об аппаратных отказах по общей причине, необходимых для калибровки методики, не существует, поэтому данные, приведенные в таблицах Г.1—Г.6, основаны на инженерных оценках.

В некоторых случаях процедуры диагностического тестирования не рассматриваются как необходимые для обеспечения безопасности, поэтому их уровень обеспечения качества может быть ниже, чем у процедур, обеспечивающих основные функции управления. Данная методика разработана в предположении, что УПБ для диагностического тестирования соответствует требуемому. Следовательно, любые программные процедуры диагностического тестирования должны быть разработаны с использованием методов, соответствующих требуемому уровню полноты безопасности.

Г.4 Использование β-фактора для вычисления вероятности отказа Э/Э/ПЭ СБЗС системы из-за отказов по общей причине

Влияние отказов по общей причине на многоканальную систему с диагностическим тестированием следует рассматривать в каждом из каналов системы.

Используя модель β-фактора для интенсивности опасных отказов по общей причине получают $\lambda_D\beta$, где λ_D — интенсивность опасных случайных отказов АС для каждого отдельного канала, а β — это β-фактор при отсутствии диагностического тестирования, т. е. доля отказов одного канала, влияющих на все каналы.

Если допустить, что отказы по общей причине влияют на все каналы, а промежуток времени между таким влиянием на первый и остальные каналы мал по сравнению с интервалом времени между последовательными отказами каналов по общей причине. И в каждом канале применено диагностическое тестирование, которое обнаруживает и определяет часть отказов. В таком случае отказы подразделяют на две категории: отказы, которые

находятся вне охвата диагностического тестирования (т. е. не могут быть обнаружены), и отказы в пределах охвата диагностическим тестированием (которые в конечном счете будут обнаружены диагностическим тестированием).

Поэтому общую интенсивность отказов системы, вызванных опасными отказами по общей причине, определяют как:

$$\lambda_{DU}\beta + \lambda_{DD}\beta_D,$$

где λ_{DU} — интенсивность необнаруженных отказов одного канала, т. е. интенсивность опасных отказов, находящихся за пределами охвата диагностического тестирования; очевидно, любое уменьшение β-фактора, являющееся следствием частоты проведения диагностического тестирования, не может повлиять на эту долю отказов;

β — фактор отказов по общей причине для необнаруживаемых опасных отказов, который равен общему β-фактору, применяемому при отсутствии диагностического тестирования;

λ_{DD} — интенсивность обнаруженных опасных отказов одного канала (т. е. интенсивность опасных отказов одного канала), находящихся в области охвата диагностического тестирования; если частота проведения диагностического тестирования высока, доля обнаруженных отказов ведет к уменьшению значения β, т. е. β_D;

β_D — доля опасных отказов по общей причине, обнаруживаемых диагностическими тестами. С увеличением частоты проведения диагностического тестирования значение β становится менее β_D.

Значение β определяют по таблице Г.5, в которой используют результаты Г.4, с помощью оценки $S = X + Y$ (см. Г.5).

Значение β_D определяют по таблице Г.5, в которой используют результаты Г.4, с помощью соотношения $S_D = X(Z + 1) + Y$.

Г.5 Использование таблиц для оценки β-фактора

Оценку β-фактора рассчитывают отдельно для датчиков, логической подсистемы и исполнительных элементов.

Для того чтобы свести к минимуму вероятность возникновения отказов по общей причине, следует сначала определить средства, эффективно защищающие от появления таких отказов. Реализация соответствующих средств в системе ведет к уменьшению значения β-фактора, используемого при оценке вероятности отказа системы из-за отказов по общей причине.

Мероприятия и соответствующие им значения (баллы) параметров X и Y, полученные с помощью инженерной оценки и описывающие вклад каждого из мероприятий в уменьшение числа отказов по общей причине, перечислены в таблице Г.1. Так как датчики и исполнительные элементы анализируются иначе, чем программируемая электроника, в таблице Г.1 используются столбцы X_{LS} и Y_{LS} для программируемых электронных средств и столбцы X_{SF} и Y_{SF} для датчиков или исполнительных элементов.

ПЭ системы могут использовать интенсивное диагностическое тестирование, позволяющее обнаруживать неодновременные отказы по общей причине. Для учета диагностического тестирования при оценке β-фактора общий вклад каждого из мероприятий, перечисленных в таблице Г.1, разделен с использованием инженерной оценки на наборы значений X и Y. Для каждого конкретного мероприятия отношение S/Y представляет собой меру повышения вклада этого мероприятия в борьбу с отказами по общей причине благодаря диагностическому тестированию.

Пользователь таблицы Г.1 должен определить, какие мероприятия будут использованы для рассматриваемой системы, и сложить соответствующие мероприятиям баллы, приведенные в графах X_{LS} и Y_{LS} для логической подсистемы, или в графах X_{SF} и Y_{SF} — для датчиков или исполнительных элементов, получив суммы X и Y соответственно.

Коэффициент Z определяют по таблицам Г.2 и Г.3 по частоте и охвату диагностического тестирования с учетом примечания 4, определяющего, когда следует использовать ненулевое значение Z. Затем (при необходимости) рассчитывают сумму баллов S (см. Г.5) по формуле $X + Y$ — для получения значения β_{int} (β-фактора для необнаруженных отказов) и $S_D = X(Z + 1) + Y$ — для получения значения β_{Dint} (β-фактора для обнаруженных отказов), где S или S_D — баллы, используемые в таблице Г.4 для определения соответствующего β_{int}-фактора.

β_{int} и β_{Dint} являются значениями отказа по общей причине до рассмотрения эффекта различных степеней избыточности.

Таблица Г.2 — Значение *Z* (программируемая электроника)

Охват диагностикой, %	Периодичность диагностического тестирования		
	Менее 1 мин	От 1 до 5 мин	Более 5 мин
99	2,0	1,0	0
90	1,5	0,5	0
60	1,0	0	0

Таблица Г.3 — Значение *Z* (датчики или исполнительные элементы)

Охват диагностикой, %	Периодичность диагностического тестирования			
	Менее 2 ч	От 2 ч до 2 дней	От 2 до 7 дней	Более 7 дней
99	2,0	1,5	1,0	0
90	1,5	1,0	0,5	0
60	1,0	0,5	0	0

Примечания

1 Данная методика наиболее эффективна, если при подсчете баллов равномерно учитываются все группы мероприятий, представленные в таблице Г.1. Следовательно, рекомендуется, чтобы общая сумма баллов *X* и *Y* для каждой группы была не менее общей суммы баллов *X* и *Y*, деленной на 20. Например, если общая сумма баллов *X* + *Y* равна 80, то общая сумма баллов *X* + *Y* для любой из групп (например, для группы мероприятий «Процедуры/интерфейс пользователя») должна быть не менее четырех.

2 При использовании данных таблицы Г.1 следует учитывать баллы для всех реализованных в системе мероприятий. Подсчет суммы баллов разработан для учета тех мероприятий, которые не являются взаимно исключающими. Например, для системы, логические подсистемы каналов которой расположены в отдельных стойках, подсчитывают сумму баллов мероприятий таблицы Г.1 «Расположены ли логические подсистемы каналов в отдельных шкафах» и «Расположены ли логические подсистемы каналов на отдельных печатных платах».

3 Если в датчиках или исполнительных элементах использована программируемая электроника, их рассматривают как часть логической подсистемы, если они находятся в том же здании (транспортном средстве), что и устройство, являющееся главной частью логической подсистемы, и в качестве датчиков или исполнительных элементов, если они расположены отдельно.

4 Для того чтобы использовать ненулевое значение *Z*, нужно убедиться в том, что управляемое оборудование переходит в безопасное состояние до того, как неодновременный отказ по общей причине сможет повлиять на все каналы. Время, необходимое для обеспечения этого безопасного состояния, должно быть менее заявленного интервала диагностического тестирования. Ненулевое значение *Z* допускается использовать только в том случае, если:

- система инициирует автоматическое выключение при обнаружении сбоя, или
- безопасное выключение не инициируется после первого сбоя[1)], но диагностическое тестирование:
- определяет местонахождение сбоя и может его локализовать, а также
- сохраняет способность перевода УО в безопасное состояние после обнаружения любых последующих сбоев, или
- применяется формальная система работы, гарантирующая, что причина любого обнаруженного сбоя будет полностью проанализирована в течение заявленного периода диагностического тестирования и либо установка немедленно выключается, если сбой может привести к отказу по общей причине, либо канал, в котором произошел сбой, восстанавливается в течение заявленного интервала диагностического тестирования.

5 В обрабатывающих отраслях практически невозможно выключать УО при обнаружении сбоя во время интервала диагностического тестирования в соответствии с таблицей Г.2. Настоящая методика не должна восприниматься как содержащая строгое требование выключать технологические установки непрерывного производства

[1)] Необходимо учитывать действия системы при обнаружении сбоя. Например, простая система с архитектурой голосования 2oo3 должна быть выключена (или отремонтирована) после обнаружения одиночного отказа в течение времени, приведенного в таблице Г.2 или Г.3. Если система не выключена, отказ второго канала может привести к тому, что при голосовании два отказавших канала получат перевес голосов над оставшимся (работоспособным) каналом. У системы, которая автоматически меняет архитектуру голосования на 1oo2 при отказе одного канала и автоматически выключается при возникновении второго отказа, вероятность обнаружения неисправности второго канала повышается, и, следовательно, ненулевое значение *Z* возможно.

при обнаружении подобных сбоев. Однако если выключение не производится, то и β-фактор не уменьшить с помощью использования диагностического тестирования для программируемых электронных средств. В ряде других отраслей выключение УО во время интервала диагностического тестирования возможно. В этих случаях можно использовать ненулевое значение *Z*.

6 Если диагностическое тестирование проводят модульно, то время повторения, приведенное в таблице Г.2 или Г.3, — это время между завершениями последовательного диагностического тестирования всего набора модулей. Охват диагностикой — общий охват, обеспечиваемый всеми модулями.

Таблица Г.4 — Расчет величины β_{int} или β_{Dint}

Баллы (S или S_D)	Значение β_{int} или β_{Dint}	
	для логической подсистемы	для датчиков или исполнительных элементов
120 или более	0,5 %	1 %
От 70 до 120	1 %	2 %
От 45 до 70	2 %	5 %
Менее 45	5 %	10 %

Примечания

1 Максимальные уровни β_{Dint}, ниже обычно используемых, что объясняется использованием методов, описанных в настоящем стандарте, для уменьшения вероятности систематических отказов в целом и в результате вероятности отказов по общей причине.

2 Значения β_{Dint} менее 0,5 % для логической подсистемы и 1 % — для датчиков трудно подтвердить.

Значение β_{int}, полученное на основании данных таблицы Г.4, является отказом по общей причине, сопоставленным с системой голосования 1oo2. Для других уровней избыточности (*MooN*) значение β_{int} меняется, как показано в таблице Г.5, для получения окончательного значения β.

Данные таблицы Г.5 также используют для определения конечного значения β_D, но при наличии β_{int} оно может быть уменьшено до β_{Dint}.

Таблица Г.5 — Расчет β для систем с уровнем резервирования, большим 1oo2

MooN		Значение *N*			
		2	3	4	5
Значение *M*	1	β_{int}	$0{,}5\beta_{int}$	$0{,}3\beta_{int}$	$0{,}2\beta_{int}$
	2	—	$1{,}5\beta_{int}$	$0{,}6\beta_{int}$	$0{,}4\beta_{int}$
	3	—	—	$1{,}75\beta_{int}$	$0{,}8\beta_{int}$
	4	—	—	—	$2\beta_{int}$

Г.6 Использование методологии β-фактора

Для демонстрации влияния применения методологии β-фактора в таблицу Г.6 включены значения параметров для простых примеров элементов ПЭ средств.

Таблица Г.6 — Пример значений параметров для программируемых электронных средств

Группа мероприятий		Система с разнообразием и хорошим диагностическим тестированием	Система с разнообразием и плохим диагностическим тестированием	Система с избыточностью и хорошим диагностическим тестированием	Система с избыточностью и плохим диагностическим тестированием
Разделение/выделение	*X*	3,50	3,50	3,50	3,50
	Y	1,50	1,50	1,50	1,50
Разнообразие/избыточность	*X*	14,50	14,50	2,00	2,00
	Y	3,00	3,00	1,00	1,00
Сложность/конструкция/...	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Оценка/анализ/...	*X*	0,25	0,25	0,25	0,25
	Y	4,75	4,75	4,75	4,75
Процедуры/интерфейс пользователя	*X*	3,50	3,50	3,50	3,50
	Y	3,00	3,00	3,00	3,00
Компетентность/обучение/...	*X*	1,25	1,25	1,25	1,25
	Y	3,75	3,75	3,75	3,75
Контроль состояния окружающей среды	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Проверка влияния окружающей среды	*X*	5,00	5,00	5,00	5,00
	Y	5,00	5,00	5,00	5,00
Охват диагностикой	*Z*	2,00	0,00	2,00	0,00
X (всего)		33,5	33,5	21	21
Y (всего)		25,5	25,5	23,5	23,5
Сумма баллов *S*		59	59	44,5	44,5
β		2 %	2 %	5 %	5 %
Сумма баллов S_D		126	59	86,5	44,5
β_D		0,5 %	2 %	1 %	5 %
Система 1oo2 с разнообразием (см. таблицу Г.5)		0,5 %	2 %	—	—
Система 2oo3 без разнообразия (см. таблицу Г.5)		—	—	1,5 %	7,5 %

Для систем, не относящихся к категориям «с разнообразием» или «с избыточностью», использованы типовые значения *X* и *Y*, которые получены делением максимального значения баллов для конкретной системы на 2.

Для систем с разнообразием значения *X* и *Y* для категории «с разнообразием»/«с избыточностью» выведены исходя из следующих мероприятий, рассмотренных в таблице Г.1:

- одна система электронная, другая — использует технологию реле;
- диагностическое тестирование аппаратных средств использует различные технологии;
- разные конструкторы (проектировщики) не взаимодействовали между собой в процессе проектирования;
- для пуска системы использованы различные методы тестирования и разный персонал;
- обслуживание проводилось в разное время разными людьми. Для систем с избыточностью значения *X* и *Y* для группы «с разнообразием/с избыточностью» выведены исходя из того, что диагностика аппаратных средств проводилась независимой системой, использующей такую же технологию, как и системы с избыточностью.

В системах с разнообразием и в системах с избыточностью для величины *Z* использованы максимальные и минимальные значения, поэтому в таблице Г.6 значения β и β_D представлены для четырех систем.

Г.7 Биномиальная интенсивность отказов (шоковая модель) (подход *CCF*)

Практические испытания отказов по общей причине (*CCF*) показывают, что если происходит много двойных отказов и мало тройных, возможно, один четырехкратный и ни одного большего порядка при наблюдении за одной явной причиной, которая не могла быть определена во время анализа безопасности, то, следовательно, вероятность множественных отказов уменьшается с увеличением порядка *CCF*. Поэтому если модель β-фактора является реалистичной для двойного отказа и несколько пессимистичной для тройного, то для четырехкратного отказа и дальше она становится чересчур консервативной. Рассмотрим типичный пример приборной системы безопасности, которая закрывает *n* скважин (например, *n* = 150) на нефтяном месторождении, когда забивается выход. Две, три или четыре скважины могут не закрыться из-за неявных *CCF*, но не *n*, как было смоделировано по β-фактору (иначе *CCF* будут явными, и должны анализироваться отдельные отказы). Другой типичный пример возникает при работе с несколькими слоями безопасности одновременно. Например, анализ возможных *CCF* между датчиками двух слоев безопасности может означать рассмотрение *CCF* между шестью датчиками (т. е. тремя датчиками в каждом слое).

Для того чтобы решить этот вопрос, предложено несколько моделей, большинство из которых требуют достаточно много параметров надежности (например, модель множественных греческих букв или α-модель), что становятся нереальными. Среди них биномиальная интенсивность отказов (шоковая модель). Идея в том, что, когда происходит *CCF*, это похоже на удар по связанным компонентам. Этот удар может быть летальным (т. е. оказывать такое же влияние, как и в модели β-фактора) или нелетальным, при котором имеется только определенная вероятность того, что данный компонент откажет из-за удара. Тогда вероятность того, что из-за удара будет получено *k* отказов, распределена биномиально.

В данной модели требуется, чтобы были определены только три параметра:

- ω — интенсивность летальных ударов;
- ρ — интенсивность нелетальных ударов;
- γ — условная вероятность отказа указанного компонента, получившего нелетальный удар.

На рисунке Г.2 приведен пример реализации данного метода при использовании дерева отказов.

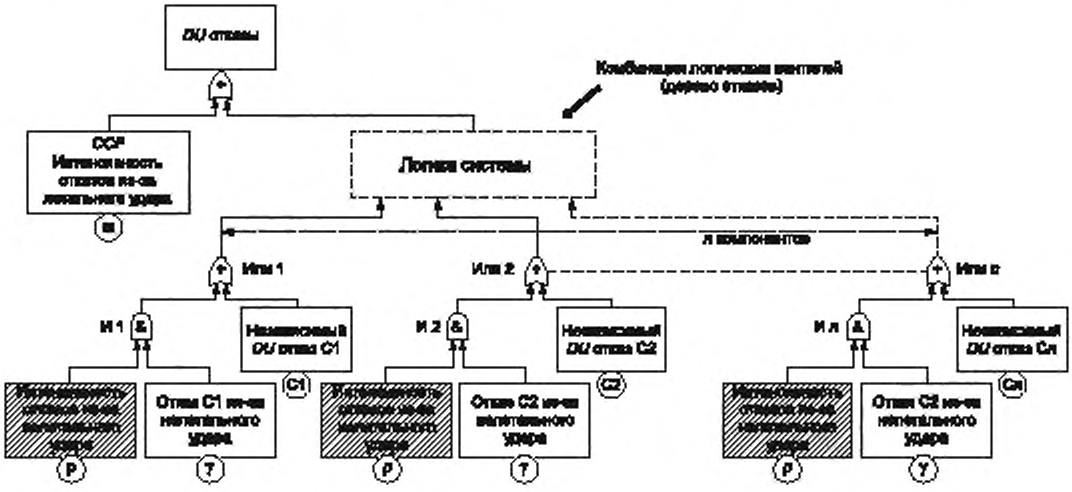


Рисунок Г.2 — Реализация шоковой модели при использовании дерева отказов

Идентичные компоненты могут быть связаны с моделью β-фактора путем разделения β на две части β_L и β_{NL}:

- $\beta = \beta_L + \beta_{NL}$;
- интенсивность отказов из-за летального удара: $\lambda_{DU} \cdot \beta_L$;
- интенсивность отказов из-за нелетального удара: $\lambda_{DU} \cdot \lambda_{NL}$;
- интенсивность независимых отказов: $\lambda_{DU} [1 — (\beta_L + \beta_{NL})]$.

В дереве отказов, представленном на рисунке Г.2, это соответствует интенсивности:

- летальных ударов: $\omega = \lambda_{DU} \cdot \beta_L$,
- нелетальных ударов: $\rho = \lambda_{DU} \cdot \beta_{NL} / \gamma$.

Обычно основной сложностью является вычисление значений трех параметров (ω, ρ, γ) или (β_L, β_{NL}, γ).

Если данные отсутствуют, то возможно использование мнения инженеров при прагматичном подходе. Например, при наличии более трех похожих элементов при использовании дерева отказов могут быть применены следующие процедуры:

- процедура 1 — следует рассматривать β так, как в методе β-фактора;
- процедура 2 — следует считать β_L незначительным (ρ_{NL} = β);
- процедура 3 — необходимо оценить γ для того, чтобы подтвердить консервативный результат. Считая, что двойные отказы реализованы по крайней мере в 10 раз чаще, чем четырехкратные (безусловно, консервативная гипотеза), можно использовать следующую формулу:

$$\gamma = \sqrt{\frac{C_N^2}{10C_N^4}}, \tag{Г.1}$$

где N — число похожих элементов;

C_N^2 — число потенциальных двойных отказов;

C_N^4 — число потенциальных четырехкратных отказов;

- процедура 4 — следует рассчитать ρ как функцию от количества N похожих элементов по формуле:

$$\rho = \frac{\beta\lambda_{DU}}{C_N^2\gamma^2 + C_N^3\gamma^3}. \tag{Г.2}$$

В данном методе основной вклад вносят двойные и тройные отказы, а результаты являются консервативными по сравнению с результатами, полученными при помощи метода β-фактора только с тремя компонентами. Двойные и тройные *CCF* рассматривают корректно, но и маловероятные множественные отказы игнорируют не полностью.

Данная модель может быть реализована при вычислениях для моделей дерева отказов, подобно тем, что показаны в приложении Г, например для дерева отказов в Б.4.3. Она позволяет анализировать системы безопасности, содержащие много похожих компонентов.

Приложение Д
(справочное)

Применение таблиц полноты безопасности программного обеспечения в соответствии с ГОСТ 34332.4

Д.1 Общие положения

Настоящее приложение содержит два примера применения таблиц полноты безопасности ПО, определенных в ГОСТ 34332.4—2021 (приложение А):

УПБ 2: программируемая электронная система, связанная с безопасностью, которая используется для управления процессом на химическом заводе;

УПБ 3: программное приложение, разработанное на языке программирования высокого уровня, которое управляет закрывающим устройством.

Данные примеры показывают, каким образом можно выбрать методики разработки ПО в определенных случаях ГОСТ 34332.4—2021 (таблицы приложений А и Б).

Следует подчеркнуть, что эти иллюстрации не являются безусловным применением стандартов в данных примерах. В ГОСТ 34332.4 четко отмечено, что с учетом огромного числа факторов, которые могут повлиять на системные возможности ПО, невозможно предоставить алгоритм для объединения методов и мер, которые необходимо применять для любого применения.

Все исходные характеристики конкретной системы, необходимые для использования упомянутых выше таблиц полноты безопасности, должны иметь документальное обоснование, подтверждающее, что все описания используемых характеристик правильны и соответствуют конкретной реализации этой системы. Предпочтительно, чтобы эти обоснования опирались на ГОСТ 34332.4—2021 (приложение В), в котором обсуждаются те свойства, с помощью которых при их достижении на соответствующей стадии ЖЦ могут убедительно доказать, что созданное ПО обладает достаточной систематической полнотой безопасности.

Д.2 Система с уровнем полноты безопасности 2

Для обеспечения безопасности объектов часто используют ПЭ СБЗС системы средней сложности с УПБ 2. Функции безопасности таких систем обычно включают в себя, как минимум, получение сигналов от различных датчиков, их обработки (обнаружение опасных ситуаций, формирование сигналов тревоги, сигналов управления УО), сопряжение с распределенной системой управления системы безопасности и передачу соответствующих сигналов потребителям. Важным фактором, определяющим эффективность систем, служит оптимальное соотношение средних вероятностей отказов от выполнения функции(ий) безопасности по запросу и ложных срабатываний. В некоторых случаях (например, в установках автоматической пожарной сигнализации и автоматического пожаротушения, особенно газового) ложное срабатывание системы может привести к более тяжелым последствиям с человеческими жертвами, чем при отказе системы.

Предприятия химической промышленности обладают большим опытом построения и применения подобных систем, который целесообразно использовать при рассмотрении ПЭ СБЗС систем.

Приведенный ниже пример представляет собой ПЭ СБ систему с УПБ 2, которую используют для управления процессом на химическом предприятии. В прикладной программе данной системы применен язык многозвенных логических схем, что служит примером прикладного программирования на языке с ограниченной изменчивостью.

Установка, работающая на химическом предприятии, состоит из нескольких реакторных баков, связанных промежуточными баками хранения, которые на определенных стадиях цикла реакции заполняются инертным газом для предотвращения воспламенения и взрывов. Функции ПЭ СБ системы помимо прочих включают в себя: получение входных данных от датчиков; включение и блокировку клапанов, насосов и исполнительных механизмов; обнаружение опасных ситуаций и включение сигнала тревоги; сопряжение с распределенной системой управления в соответствии с требованиями, предъявляемыми спецификацией безопасности. Предположения и характеристики системы:

- программируемая электроника СБЗСВ системы представляет собой программируемый логический контроллер (ПЛК);
- при анализе опасностей и рисков установлено, что необходимо использовать ПЭ СБЗС систему, и для данного приложения нужен УПБ 2 (в соответствии с ГОСТ 34332.3 и ГОСТ 34332.4);
- хотя контроллер работает в реальном времени, требуется относительно небольшая скорость реакции;
- существуют интерфейсы с оператором и распределенной системой управления;
- исходный код ПО системы и схема программируемых электронных средств ПЛК недоступны для проверки, но оценены в соответствии с ГОСТ 34332.4 как соответствующие УПБ 2;
- в качестве языка программирования приложения использован язык многозвенных логических схем; программа создавалась с помощью системы разработки, предоставляемой поставщиком ПЛК;
- код приложения должен быть исполнен только на ПЛК одного типа;
- вся разработка ПО контролировалась лицом, независимым от команды разработчиков ПО;

- лицо, независимое от команды разработчиков ПО, наблюдало за приемочными испытаниями и утвердило их результаты;

- изменения (если необходимы) санкционируются лицом, независимым от команды разработчиков ПО.

Примечание — Информация о разделении ответственности между поставщиком ПЛК и пользователями при использовании языков программирования с ограниченной изменчивостью приведена в ГОСТ 34332.4—2021 (примечания к 7.4.2—7.4.5).

Интерпретация ГОСТ 34332.4—2021 (приложение А) для данного примера представлена в таблицах Д.1—Д.11.

Таблица Д.1 — Спецификация требований к безопасности ПО [см. ГОСТ 34332.4—2021 (подраздел 7.2)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1а Полуформальные методы	Таблица Б.7	Р	Обычно используют причинно-следственные диаграммы, циклограммы и функциональные блоки, используемые для спецификации требований к программному обеспечению ПЛК
1б Формальные методы	Б.2.2, В.2.4	Р	Не используют для языков программирования с ограниченной изменчивостью
2 Прямая прослеживаемость между требованиями к системе безопасности и требованиями к ПО системы безопасности	В.2.11	Р	Проверка полноты: проверка, гарантирующая, что все требования к системе безопасности учтены в требованиях к ПО системы безопасности
3 Обратная прослеживаемость между требованиями к системе безопасности и предполагаемыми потребностями безопасности	В.2.11	Р	Минимизация сложности и функциональности: проверка, гарантирующая, что все требования к программному обеспечению системы безопасности фактически необходимы, чтобы учесть требования к системе безопасности
4 Автоматизированные средства разработки спецификаций для поддержки перечисленных выше подходящих методов/средств	Б.2.4	Р	Используют средства разработки, поставленные производителем ПЛК
Примечания 1 В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б). 2 Требования к безопасности ПО определены на естественном языке.			

Примечание — В графе «УПБ 2» таблиц Д.1—Д.10 и «УПБ 3» таблиц Д.11—Д.20 представлены рекомендации, которые обозначены следующим образом:

ОР — метод или средство, особо рекомендованный(ое) к применению;

Р — метод или средство, рекомендованный(ое) к применению, но степень обязательности рекомендации ниже, чем в случае рекомендации ОР;

«—» — для данного метода или средства отсутствует рекомендация относительно его применения;

НР — метод или средство, не рекомендованный(ое) к применению.

Таблица Д.2 — Проектирование и разработка ПО архитектура [см. ГОСТ 34332.4—2021 (п. 7.4.3)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Обнаружение и диагностика сбоев	В.3.1	Р	Проверка диапазона данных, контрольный таймер, ввод/вывод, средства связи. В случае ошибки поднимает тревогу (см. 3а)
2 Коды обнаружения и исправления ошибок	В.3.2	Р	Встраивают с пользовательскими функциями: требуется тщательный выбор
3а Программирование с проверкой ошибок	В.3.3	Р	Выделяют часть многозвенной логической схемы ПЛК для проверки некоторых важных условий безопасности (см. 1)

Продолжение таблицы Д.2

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
3б Методы контроля (при реализации процесса контроля и контролируемой функции на одном компьютере обеспечивается их независимость)	В.3.4	Р	Не предпочтительны: обеспечение гарантии независимости приводит к увеличению сложности ПО
3в Методы контроля (реализация процесса контроля и контролируемой функции на разных компьютерах)	В.3.4	Р	Проверяют разрешенные комбинации ввода/вывода на мониторе независимого компьютера, обеспечивающего безопасность
3г Многовариантное программирование, реализующее одну спецификацию требований к ПО системы безопасности	В.3.5	—	Не предпочтительно: недостаточное повышение безопасности по сравнению с 3в
3д Многовариантное (функционально) программирование, реализующее различные спецификации требований к ПО системы безопасности	В.3.5	—	Не предпочтительно, в значительной степени достигается 3в
3е Восстановление предыдущего состояния	В.3.6	Р	Встраивают с пользовательскими функциями: требуется тщательный выбор
3ж Проектирование программного обеспечения, не сохраняющего состояние (или проектирование ПО, сохраняющего ограниченное описание состояния)	В.2.12	—	Не используют. Управлению процессом необходима информация о состояниях, чтобы запоминать состояние установки
4а Механизмы повторных попыток парирования сбоя	В.3.7	Р	Используют в соответствии с требованиями прикладной задачи (см. 2 и 3б)
4б Постепенное отключение функций	В.3.8	Р	Не используют для программирования с ограниченной изменчивостью
5 Исправление ошибок методами искусственного интеллекта	В.3.9	НР	Не используют для программирования с ограниченной изменчивостью
6 Динамическая реконфигурация	В.3.10	НР	Не используют для программирования с ограниченной изменчивостью
7 Модульный подход	Таблица Б.9	ОР	—
8 Использование доверительных/проверенных элементов ПО (если таковые имеются)	В.2.10	ОР	Созданный ранее код для более ранних проектов
9 Прямая прослеживаемость между спецификацией требований к ПО системы безопасности и архитектурой ПО	В.2.11	Р	Проверка полноты: проверка, гарантирующая, что все требования к ПО системы безопасности учтены в требованиях к архитектуре ПО
10 Обратная прослеживаемость между спецификацией требований к ПО системы безопасности и архитектурой ПО	В.2.11	Р	Минимизация сложности и функциональности: проверка, гарантирующая, что все требования к архитектуре ПО системы безопасности фактически необходимы, чтобы учесть требования к ПО системы безопасности
11а Структурные методы	В.2.1	ОР	Методы потоков данных и логических таблиц данных могут быть использованы, по крайней мере, для описания проекта архитектуры
11б Полуформальные методы	Таблица В.7	Р	Могут быть использованы для интерфейса DCS
11в Формальные методы проектирования и усовершенствования	Б.2.2, В.2.4	Р	Редко используют для программирования с ограниченной изменчивостью

Окончание таблицы Д.2

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
11г Автоматическая генерация ПО	В.4.6	Р	Не используют для программирования с ограниченной изменчивостью
12 Автоматизированные средства разработки спецификаций и проектирования	Б.2.4	Р	Используют средства разработки, поставленные производителем ПЛК
13а Циклическое поведение с гарантированным максимальным временем цикла	В.3.11	ОР	Не используют. Время цикла ПЛК контролируется техническими средствами
13б Архитектура с временным распределением	В.3.11	ОР	Не используют. Время цикла ПЛК контролируется техническими средствами
13в Управление событиями с гарантированным максимальным временем реакции	В.3.11	ОР	Не используют. Время цикла ПЛК контролируется техническими средствами
14 Статическое выделение ресурсов	В.2.6.3	Р	Не используют. Вопросы о динамических ресурсах не возникают для программирования с ограниченной изменчивостью
15 Статическая синхронизация доступа к разделяемым ресурсам	В.2.6.3	—	Не используют. Вопросы о динамических ресурсах не возникают для программирования с ограниченной изменчивостью

Примечания

1 В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).

2 Требования к безопасности ПО определены на естественном языке.

Таблица Д.3 — Проектирование и разработка ПО: средства поддержки и языки программирования [см. ГОСТ 34332.4—2021 (пункт 7.4.4)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Выбор соответствующего языка программирования	В.4.5	ОР	Обычно используют многозвенные логические схемы и часто используют фирменные языки поставщика ПЛК
2 Строго типизированные языки программирования	В.4.1	ОР	Не используют. Используют ПЛК-ориентированный структурированный текст
3 Подмножество языка	В.4.2	—	Не используют и-за сложных «макроинструкций», прерываний, которые изменяют цикл сканирования ПЛК, и т. д.
4а Сертифицированные средства и сертифицированные трансляторы	В.4.3	ОР	Поставляется производителем ПЛК
4б Инструментальные средства и трансляторы: повышение уверенности на основании опыта использования	В В.4.4	ОР	Используют средства разработки, предлагаемые поставщиком ПЛК, а также собственные инструменты, разработанные в ходе работы над несколькими проектами

Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В).

Таблица Д.4 — Проектирование и разработка ПО: подробная модель [см. ГОСТ 34332.4—2021 (пункты 7.4.5 и 7.4.6)] (включает проектирование систем ПО, проектирование модулей ПО и кодирование)

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1а Структурные методы	В.2.1	ОР	Не используют для языков программирования с ограниченной изменчивостью
1б Полуформальные методы	Таблица Б.7	ОР	Используют причинно-следственные схемы, циклограммы, функциональные блоки, типичные для языков программирования с ограниченной изменчивостью
1в Формальные методы проектирования и усовершенствования	Б.2.2, В.2.4	Р	Не используют для языков программирования с ограниченной изменчивостью
2 Средства автоматизированного проектирования	Б.3.5	Р	Используют средства разработки, поставленные производителем ПЛК
3 Программирование с защитой	В.2.5	Р	Включают в системное ПО
4 Модульный подход	Таблица Б.9	ОР	Используют упорядочение и группировку программы для ПЛК на многозвенных логических схемах для максимального увеличения модульности требуемых функций
5 Стандарты по проектированию и кодированию	Б.2.6, таблица Б.1	ОР	Используют собственные соглашения для применения документации и удобства эксплуатации
6 Структурное программирование	Б.2.7	ОР	Для рассматриваемого примера аналогично модульности
7 Использование доверительных/проверенных элементов ПО (по возможности)	Б.2.10	ОР	Функциональные блоки, части программ
8 Прямая прослеживаемость между спецификацией требований к ПО системы безопасности и проектом ПО	Б.2.11	Р	Проверка полноты: проверка, гарантирующая, что все требования к ПО системы безопасности учтены в требованиях проектирования ПО
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.5 — Проектирование и разработка ПО: проверка и интеграция программных модулей [см. ГОСТ 34332.4—2021 (пункты 7.4.7 и 7.4.8)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Вероятностное тестирование	В.5.1	Р	Не используют для языков программирования с ограниченной изменчивостью
2 Динамический анализ и тестирование	Б.6.5, таблица Б.2	ОР	Используются
3 Регистрация и анализ данных	В.5.2	ОР	Запись исходных данных и результатов тестирования
4 Функциональное тестирование и тестирование методом «черного ящика»	Б.5.1, Б.5.2, таблица Б.3	ОР	Выбирают входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используют тестовые примеры, полученные с помощью причинно-следственных схем, анализ граничных значений и декомпозиция входных данных

Окончание таблицы Д.5

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
5 Тестирование рабочих характеристик	Таблица Б.6	Р	Не используют для языков программирования с ограниченной изменчивостью
6 Тестирование, основанное на модели	В.5.27	Р	Не используют для языков программирования с ограниченной изменчивостью
7 Тестирование интерфейса	В.5.3	Р	Включено в функциональное тестирование и тестирование методом «черного ящика»
8 Управление тестированием и средства автоматизации	В.4.7	ОР	Используют средства разработки, поставленные производителем ПЛК
9 Прямая прослеживаемость между спецификацией проекта ПО и спецификациями тестирования модуля и интеграции	В.2.11	Р	Проверка полноты: проверка, гарантирующая, что запланирован соответствующий тест, чтобы исследовать функциональность всех модулей и их интеграции с соответственно связанными модулями
10 Формальная верификация	В.5.12	—	Не используют для языков программирования с ограниченной изменчивостью
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.6 — Интеграция программируемых электронных средств (аппаратура и ПО) [см. ГОСТ 34332.4—2021 (подраздел 7.5)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Функциональное тестирование и тестирование методом «черного ящика»	Б.5.1, Б.5.2, таблица Б.3	ОР	Выбирают входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются тестовые примеры, полученные с помощью причинно-следственных схем, анализ граничных значений и декомпозиция входных данных
2 Моделирование производительности	Таблица Б.6	Р	Если систему ПЛК собирают для заводских приемочных испытаний
3 Прямая прослеживаемость между требованиями проекта системы и ПО к интеграции программных и аппаратных средств и спецификациями тестирования интеграции программных и аппаратных средств	В.2.11	Р	Проверка, гарантирующая, что тесты интеграции аппаратуры и ПО являются адекватными
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.7 — Подтверждение соответствия аспектов программного обеспечения системы безопасности [см. ГОСТ 34332.4—2021 (подраздел 7.7)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Вероятностное тестирование	В.5.1	Р	Не используют для языков программирования с ограниченной изменчивостью
2 Моделирование процесса	В.5.18	Р	Не используют для языков программирования с ограниченной изменчивостью, но все чаще используется при разработке систем ПЛК
3 Моделирование	Таблица Б.5	Р	Не используют для языков программирования с ограниченной изменчивостью, но все чаще используется при разработке систем ПЛК
4 Функциональное тестирование и тестирование методом «черного ящика»	Б.5.1, Б.5.2, таблица Б.3	ОР	Выбираются входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются тестовые примеры, полученные с помощью причинно-следственных схем, анализ граничных значений и декомпозиция входных данных
5 Прямая прослеживаемость между спецификацией требований к ПО системы безопасности и планом подтверждения соответствия ПО системы безопасности	В.2.11	Р	Проверка полноты: проверка, гарантирующая, что запланированное адекватное подтверждение соответствия ПО учтено в требованиях к ПО системы безопасности
6 Обратная прослеживаемость между планом подтверждения соответствия ПО системы безопасности и спецификацией требований к ПО системы безопасности	С.2.11	Р	Минимизация сложности: проверка, гарантирующая, что все проверки подтверждения соответствия необходимы
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.8 — Модификация ПО [см. ГОСТ 34332.4—2021 (подраздел 7.8)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Анализ влияния	С.5.23	ОР	Выполняют анализ последствий для изучения того, насколько влияние предлагаемых изменений ограничено модульной структурой всей системы
2 Повторная верификация измененных программных модулей	В.5.23	ОР	Повторение предыдущих тестов
3 Повторная верификация программных модулей, на которые оказывают влияние изменения в других модулях	В.5.23	ОР	Повторение предыдущих тестов
4а Повторное подтверждение соответствия системы в целом	Таблица А.7	Р	Если анализ последствий показал необходимость модификации системы, то после выполнения ее модификации обязательно проводить повторное подтверждение соответствия системы
4б Регрессионное подтверждение соответствия	В.5.25	ОР	—

Окончание таблицы Д.8

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
5 Управление конфигурацией ПО	В.5.24	OP	Поддерживает базовую конфигурацию, изменения в ней, влияние на другие системные требования
6 Регистрация и анализ данных	С.5.2	OP	Выполняется запись исходных данных и результатов тестирования
7 Прямая прослеживаемость между спецификацией требований к ПО системы безопасности и планом модификации ПО (включая повторные верификацию и подтверждение соответствия)	В.2.11	P	Соответствующие процедуры модификации, обеспечивающие достижение требований к ПО системы безопасности
8 Обратная прослеживаемость между планом модификации ПО (включая повторные верификацию и подтверждение соответствия) и спецификацией требований к ПО системы безопасности	В.2.11	P	Соответствующие процедуры модификации, обеспечивающие достижение требований к ПО системы безопасности
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.9 — Верификация ПО [см. ГОСТ 34332.4—2021 (подраздел 7.9)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Формальное доказательство	В.5.12	P	Не используют для языков программирования с ограниченной изменчивостью
2 Анимация спецификации и тестирования	В.5.26	P	—
3 Статический анализ	Б.6.4, таблица Б.8	OP	Выполняют анализ перекрестных ссылок использования переменных, условий и т. д.
4 Динамический анализ и тестирование	Б.6.5, таблица Б.2	OP	Используют автоматические средства тестирования для облегчения регрессивного тестирования
5 Прямая прослеживаемость между спецификацией проекта ПО и планом верификации (включая верификацию данных) ПО	В.2.11	P	Проверка полноты: проверка, гарантирующая соответствующий тест функциональности
6 Обратная прослеживаемость между планом верификации (включая верификацию данных) ПО и спецификацией проекта ПО	В.2.11	P	Минимизация сложности: проверка, гарантирующая, что все тесты проверки необходимы
7 Численный анализ в автономном режиме	В.2.13	P	Не используют. Числовая устойчивость вычислений в данном случае не является главной проблемой
Тестирование и интеграция программных модулей	См. таблицу Д.5		
Тестирование интеграции программируемой электроники	См. таблицу Д.6		
Тестирование программной системы (подтверждение соответствия)	См. таблицу Д.7		
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.10 — Оценка функциональной безопасности [см. ГОСТ 34332.4—2021 (раздел 8)]

Метод/средство	Ссылка	УПБ 2	Интерпретация (в настоящей таблице)
1 Таблица контрольных проверок	Б.2.5	Р	Используют
2 Таблицы решений и таблицы истинности	В.6.1	Р	Используют ограниченно
3 Анализ отказов	Таблица Б.4	Р	На системном уровне анализ отказов использует причинно-следственные схемы, но для языков программирования с ограниченной изменчивостью этот метод не используют
4 Анализ отказов по общей причине для различного ПО (если используют различное ПО)	В.6.3	Р	Не используют для языков программирования с ограниченной изменчивостью
5 Структурные схемы надежности	В.6.4	Р	Не используют для языков программирования с ограниченной изменчивостью
6 Прямая прослеживаемость между требованиями раздела 8 и планом оценки функциональной безопасности ПО	В.2.11	Р	Проверка полноты охвата оценки функциональной безопасности
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Д.3 Система с уровнем полноты безопасности 3

Второй пример представляет собой программное приложение УПБ 3, разработанное на языке программирования высокого уровня, которое управляет оконечным управляемым устройством.

Рассматриваемая программная система достаточно объемная с точки зрения системы безопасности, так как включает более 30 000 строк исходного кода. Кроме того, в ней использованы обычные встроенные функции, по крайней мере две различные операционные системы и существующий код более ранних проектов (проверенных в эксплуатации). В целом система состоит более чем из 100 000 строк исходного кода.

АС (включая датчики и исполнительные механизмы) представляют собой двухканальную систему, выходы которой подключены к исполнительным элементам по схеме логического «И» (*AND*).

Предположения и характеристики системы:

- немедленная реакция не требуется, но обеспечивается максимальное время реакции;
- интерфейсы с оператором существуют для датчиков, исполнительных механизмов и оповещателей;
- исходный код операционных систем, графических процедур и коммерческих программных продуктов недоступен;
- система, скорее всего, в дальнейшем будет модернизирована;
- специально разработанное ПО использует один из распространенных процедурных языков;
- компоненты программной системы, исходный код для которых недоступен, реализованы различными способами с помощью инструментальных средств от разных поставщиков, и их объектный код создан разными трансляторами;
- ПО работает на нескольких процессорах, доступных на рынке в соответствии с требованиями ГОСТ 34332.3;
- встроенные системы соответствуют требованиям ГОСТ 34332.3 для управления отказами АС и для их предотвращения;
- разработка ПО контролировалась независимой организацией.

Интерпретация ГОСТ 34332.4—2021 (приложение А) для данного примера представлена в таблицах Д.11—Д.20.

Таблица Д.11 — Спецификация требований к безопасности ПО [см. ГОСТ 34332.4—2021 (подраздел 7.2)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1а Полуформальные методы	Таблица Б.7	ОР	Диаграммы функциональных блоков, циклограммы, диаграммы переходов
1б Формальные методы	Б.2.2, В.2.4	Р	В исключительных случаях
2 Прямая прослеживаемость между требованиями к системе безопасности и требованиями к ПО системы безопасности	В.2.11	ОР	Проверка полноты: проверка, гарантирующая, что все требования к системе безопасности учтены в требованиях к ПО системы безопасности
3 Обратная прослеживаемость между требованиями к системе безопасности и предполагаемыми потребностями в безопасности	В.2.11	ОР	Минимизация сложности и функциональности: проверка, гарантирующая, что все требования к ПО системы безопасности фактически необходимы, чтобы учесть требования к системе безопасности
4 Автоматизированные средства разработки спецификаций для поддержки, перечисленных выше, подходящих методов/средств	В.2.4	ОР	Средства поддержки выбранных методов
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.12 — Проектирование и разработка ПО: проектирование архитектуры ПО [см. ГОСТ 34332.4—2021 (пункт 7.4.3)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Обнаружение и диагностика сбоев	В.3.1	ОР	Используют для тех отказов датчиков, исполнительных устройств и средств передачи данных, которые не охватываются средствами встроенной системы в соответствии с ГОСТ Р МЭК 61508-2
2 Коды обнаружения и исправления ошибок	В.3.2	Р	Использует только для внешней передачи данных
3а Программирование с проверкой ошибок	В.3.3	Р	Используют для проверки подтверждения соответствия результатов прикладных функций
3б Методы контроля (при реализации процесса контроля и контролируемой функции на одном компьютере обеспечивается их независимость)	В.3.4	Р	Не предпочтительны: обеспечение гарантии независимости приводит к увеличению сложности ПО
3в Методы контроля (реализация процесса контроля и контролируемой функции на разных компьютерах)	В.3.4	Р	Используют для некоторых функций, связанных с безопасностью, где 3а не применимы
3г Многовариантное программирование, реализующее одну спецификацию требований к ПО системы безопасности	В.3.5	—	Используют для некоторых функций, когда исходные коды не доступны
3д Многовариантное (функционально) программирование, реализующее различные спецификации требований к ПО системы безопасности	В.3.5	Р	Не предпочтительны, в значительной степени достигается 3е
3е Восстановление предыдущего состояния	В.3.6	—	Не используют

Окончание таблицы Д.12

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
3ж Проектирование ПО, не сохраняющего состояние (или проектирование ПО, сохраняющего ограниченное описание состояния)	В.2.12	Р	Не используют. Для управления закрытием необходима информация о состояниях, чтобы запоминать состояние установки
4а Механизмы повторных попыток парирования сбоя	В.3.7	—	Не используют
4б Постепенное отключение функций	В.3.8	ОР	Используют в соответствии с природой технического процесса
5 Исправление ошибок методами искусственного интеллекта	В.3.9	НР	Не используют
6 Динамическая реконфигурация	В.3.10	НР	Не используют
7 Модульный подход	Таблица Б.9	ОР	Необходимо использовать вследствие размера системы
8 Использование доверительных/проверенных элементов ПО (если таковые имеются)	В.2.10	ОР	Существующий ранее код из более ранних проектов
9 Прямая прослеживаемость между спецификацией требований к ПО системы безопасности и архитектурой ПО	В.2.11	ОР	Проверка полноты: проверка, гарантирующая, что все требования к ПО системы безопасности учтены в требованиях к архитектуре ПО системы безопасности
10 Обратная прослеживаемость между спецификацией требований к ПО системы безопасности и архитектурой ПО	В.2.11	ОР	Минимизация сложности и функциональности: проверка, гарантирующая, что все требования к архитектуре ПО системы безопасности фактически необходимы, чтобы учесть требования к ПО системы безопасности
11а Структурные методы	В.2.1	ОР	Необходимо использовать и размера системы
11б Полуформальные методы	Таблица Б.7	ОР	Диаграммы функциональных блоков, циклограммы, диаграммы переходов
11в Формальные методы проектирования и усовершенствования	Б.2.2, В.2.4	Р	Не используют
11г Автоматическая генерация ПО	В.4.6	Р	Не используют. Следует избегать неопределенности транслятор/генератор
12 Автоматизированные средства разработки спецификаций и проектирования	Б.2.4	ОР	Средства поддержки выбранных методов
13а Циклическое поведение с гарантированным максимальным временем цикла	В.3.11	НР	Не используют
13б Архитектура с временным распределением	В.3.11	НР	Не используют
13в Управление событиями с гарантированным максимальным временем реакции	В.3.11	НР	Не используют
14 Статическое выделение ресурсов	В.2.6.3	НР	Не используют. Выбирают язык программирования, чтобы избежать проблемы динамических ресурсов
15 Статическая синхронизация доступа к разделяемым ресурсам	В.2.6.3	Р	Не используют. Выбирают язык программирования, чтобы избежать проблемы динамических ресурсов
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.13 — Проектирование и разработка ПО: средства поддержки и языки программирования [см. ГОСТ 34332.4—2021 (пункт 7.4.4)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Выбор соответствующего языка программирования	В.4.5	ОР	Выбирают язык высокого уровня с полной изменчивостью
2 Строго типизированные языки программирования	В.4.5	ОР	Используют
3 Подмножество языка	В.4.2	ОР	Определяют подмножество выбранного языка
4а Сертифицированные средства и сертифицированные трансляторы	В.4.3	ОР	Не доступны
4б Инструментальные средства и трансляторы: повышение уверенности на основании опыта использования	В.4.4	ОР	Доступны и используют
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В).			

Таблица Д.14 — Проектирование и разработка ПО: подробная модель [см. ГОСТ 34332.4—2021 (пункты 7.4.5 и 7.4.6)] (включая проектирование систем ПО, проектирование модулей ПО и кодирование)

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1а Структурные методы	В.2.1	ОР	Широко используют, в частности SADT и JSD
1б Полуформальные методы	Таблица Б.7	ОР	Используют конечные автоматы/диаграммы перехода состояний, блок-схемы, циклограммы
1в Формальные методы проектирования и усовершенствования	Б.2.2, В.2.4	Р	Используют только в исключительных случаях для некоторых важных компонентов
2 Средства автоматизированного проектирования	Б.3.5	ОР	Используют для выбранных методов
3 Программирование с защитой	В.2.5	ОР	В прикладном ПО в явном виде используют средства, которые могут быть эффективны, кроме автоматически вставляемых компилятором
4 Модульный подход	Таблица Б.9	ОР	Используют ограниченный размер программного модуля, скрытие информации/инкапсуляция, одна входная/выходная точка в подпрограммах и функциях, полностью определенный интерфейс и т. д.
5 Стандарты по проектированию и кодированию	В.2.6, таблица Б.1	ОР	Используют стандарты (предприятия) для кодирования; ограниченно используются прерывания, указатели и рекурсии; не используются динамические объекты и переменные, безусловные переходы и т. д.
6 Структурное программирование	В.2.7	ОР	Используют
7 Использование доверительных/проверенных элементов ПО (по возможности)	В.2.10	ОР	Доступен и используют
8 Обратная прослеживаемость между спецификацией требований к ПО системы безопасности и архитектурой ПО	В.2.11	ОР	Минимизация сложности и функциональности: проверка, гарантирующая, что все требования к архитектуре ПО системы безопасности фактически необходимы, чтобы учесть требования к ПО системы безопасности
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.15 — Проектирование и разработка программного обеспечения: тестирование и интеграция программных модулей [см. ГОСТ 34332.4—2021 (пункты 7.4.7 и 7.4.8)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Вероятностное тестирование	В.5.1	Р	Используют для программных модулей, исходный код которых не доступен, а определение граничных значений и классов эквивалентности для тестовых данных затруднено
2 Динамический анализ и тестирование	Б.6.5, таблица Б.2	ОР	Используют для программных модулей, исходный код которых доступен. Выполняют: контрольные примеры, разработанные с помощью анализа граничных значений, моделирование производительности, разделение входных данных на классы эквивалентности, структурное тестирование
3 Регистрация и анализ данных	В.5.2	ОР	Используют запись входных данных и результатов тестирования
4 Функциональное тестирование и тестирование методом «черного ящика»	Б.5.1, Б.5.2, таблица Б.3	ОР	Используют для программных модулей, исходный код которых не доступен, и для проверки интеграции. Выбирают входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используют тестовые примеры, полученные с помощью причинно-следственных схем, прототипирование, анализ граничных значений, разделение данных на классы эквивалентности и декомпозицию входных данных
5 Тестирование производительности	Таблица Б.6	ОР	Используют при проверке интеграции на конкретном оборудовании
6 Тестирование, основанное на модели	В.5.27	ОР	Не используют
7 Тестирование интерфейса	В.5.3	ОР	Включено в функциональное тестирование и тестирование методом «черного ящика»
8 Управление тестированием и средства автоматизации	В.4.7	ОР	Используют в случае доступности
9 Прямая прослеживаемость между спецификацией проекта ПО и спецификациями тестирования модуля и интеграции	В.2.11	ОР	Проверка, гарантирующая, что тесты интеграции достаточны
10 Формальная верификация	В.5.12	Р	Не используют
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.16 — Интеграция программируемых электронных средств (АС и ПО) [см. ГОСТ 34332.4—2021 (подраздел 7.5)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Функциональное тестирование и тестирование методом «черного ящика»	Б.5.1, Б.5.2, таблица Б.3	ОР	Используют как дополнительные тесты при интеграции ПО (см. таблицу Д.15). Выбирают входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используют тестовые примеры, полученные с помощью причинно-следственных схем, прототипирование, анализ граничных значений, разделение данных на классы эквивалентности и декомпозицию входных данных
2 Моделирование производительности	Таблица Б.6	ОР	Широко используют
3 Прямая прослеживаемость между требованиями проекта системы и ПО к интеграции программных и аппаратных средств и спецификациями тестирования интеграции программных и аппаратных средств	В.2.11	ОР	Проверка, гарантирующая, что тесты интеграции аппаратуры и ПО являются достаточными
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.17 — Подтверждение соответствия аспектов программного обеспечения системы безопасности [(см. ГОСТ 34332.4—2021 (подраздел 7.7)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Вероятностное тестирование	В.5.1	Р	Не используют для подтверждения соответствия
2 Моделирование процесса	В.5.18	ОР	Конечные автоматы, моделирование производительности, прототипирование и анимация
3 Моделирование	Таблица Б Б.5	ОР	Не используют для подтверждения соответствия
4 Функциональное тестирование и тестирование методом «черного ящика»	Б.5.1, Б.5.2, таблица Б.3	ОР	Выбирают входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используют тестовые примеры, полученные с помощью причинно-следственных схем, анализ граничных значений и декомпозицию входных данных
5 Прямая прослеживаемость между спецификацией требований к ПО системы безопасности и планом подтверждения соответствия ПО системы безопасности	В.2.11	ОР	Проверка полноты: проверка, гарантирующая, что все требования к ПО системы безопасности учтены в плане подтверждения соответствия ПО системы безопасности
6 Обратная прослеживаемость между планом подтверждения соответствия ПО системы безопасности и спецификацией требований к ПО системы безопасности	В.2.11	ОР	Минимизация сложности: проверка, гарантирующая, что все тесты подтверждения соответствия необходимы
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.18 — Модификация ПО [см. ГОСТ 34332.4—2021 (п. 7.8)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Анализ влияния	В.5.23	ОР	Используют
2 Повторная верификация измененных программных модулей	В.5.23	ОР	Используют
3 Повторная верификация программных модулей, на которые оказывают влияние изменения в других модулях	В.5.23	ОР	Используют
4а Повторное подтверждение соответствия системы в целом	Таблица А.7	ОР	Использование зависит от результатов анализа последствий
4б Регрессионное подтверждение соответствия	В.5.25	ОР	Используют
5 Управление конфигурацией программного обеспечения	В.5.24	ОР	Используют
6 Регистрация и анализ данных	В.5.2	ОР	Используют
7 Прямая прослеживаемость между спецификацией требований к ПО системы безопасности и планом модификации ПО (включая повторные верификацию и подтверждение соответствия)	В.2.11	ОР	Проверка полноты: проверка, гарантирующая, что процедуры модификации обеспечивают достижение требований к ПО системы безопасности
8 Обратная прослеживаемость между планом модификации ПО (включая повторные верификацию и подтверждение соответствия) и спецификацией требований к ПО системы безопасности	В.2.11	ОР	Минимизация сложности: проверка, гарантирующая, что все процедуры модификации необходимы
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.19 — Верификация ПО [см. ГОСТ 34332.4—2021 (подраздел 7.9)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Формальное доказательство	В.5.12	Р	Использует только в исключительных случаях для некоторых очень важных классов
2 Анимация спецификации и тестирования	В.5.26	Р	Не используют
3 Статический анализ	Б.6.4, таблица Б.8	ОР	Для всего вновь разработанного кода используют анализ граничных значений, таблицу контрольных проверок, анализ потоков управления, анализ потоков данных, проверку разработки программ, анализ проектов
4 Динамический анализ и тестирование	Б.6.5, таблица Б.2	ОР	Для всего вновь разработанного кода
5 Прямая прослеживаемость между спецификацией проекта ПО и планом верификации (включая верификацию данных) ПО	В.2.11	ОР	Проверка полноты: проверка, гарантирующая, что процедуры модификации обеспечивают достижение требований к ПО системы безопасности
6 Обратная прослеживаемость между планом верификации (включая верификацию данных) ПО и спецификацией проекта ПО	В.2.11	ОР	Минимизация сложности: проверка, гарантирующая, что все процедуры модификации необходимы

Окончание таблицы Д.19

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
7 Численный анализ в автономном режиме	В.2.13	НР	Не используют. Числовая устойчивость вычислений в данном случае не является главной проблемой
Тестирование и интеграция программных модулей	См. таблицу Д.5		
Тестирование интеграции программируемой электроники	См. таблицу Д.6		
Тестирование программной системы (подтверждение соответствия)	См. таблицу Д.7		
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Таблица Д.20 — Оценка функциональной безопасности [см. ГОСТ МЭК 61508-3—2018 (раздел 8)]

Метод/средство	Ссылка	УПБ 3	Интерпретация (в настоящей таблице)
1 Таблица контрольных проверок	Б.2.5	Р	Используют
2 Таблицы решений и таблицы истинности	В.6.1	Р	Используют в ограниченной степени
3 Анализ отказов	Таблица Б.4	ОР	Интенсивно используют анализ диагностического дерева отказов, а причинно-следственные диаграммы используют в ограниченной степени
4 Анализ отказов по общей причине для различного ПО (если различное ПО используется)	В.6.3	ОР	Используют
5 Структурные схемы надежности	В.6.4	Р	Используют
6 Прямая прослеживаемость между требованиями раздела 8 и планом оценки функциональной безопасности ПО	В.2.11	ОР	Проверка полноты охвата оценки функциональной безопасности
Примечание — В графе «Ссылка» «Б.х.х.х», «В.х.х.х» указывают на описания методов, изложенных в ГОСТ 34332.5—2021 (приложения Б и В), а «Таблица А.х», «Таблица Б.х» — на таблицы методов, представленных в ГОСТ 34332.4—2021 (приложения А и Б).			

Библиография

[1] ТР ТС 002/2011 Технический регламент Таможенного союза О безопасности высокоскоростного железнодорожного транспорта

[2] ТР ТС 003/2011 Технический регламент Таможенного союза О безопасности инфраструктуры железнодорожного транспорта

[3] ТР ТС 014/2011 Технический регламент Таможенного союза Безопасность автомобильных дорог

УДК 621.5:814.8:006.354

ОКС 13.200;
13.220;
13.310;
13.320;
91.120.99

Ключевые слова: функциональная безопасность систем; системы, связанные с безопасностью зданий и сооружений; примеры расчетов

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *М.В. Бучная*
Компьютерная верстка *Г.Д. Мухиной*

Сдано в набор 20.10.2021 Подписано в печать 12.11.2021. Формат 60×84½. Гарнитура Ариал.
Усл. печ. л. 12,09. Уч.-изд. л. 10,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
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