МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34332.3— 2021

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Часть 3

Требования к системам

(IEC 61508-2:2010, NEQ)
(IEC 61508-4:2010, NEQ)
(ISO/IEC Guide 51:2014, NEQ)

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и общие правила проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Российский научно-технический центр информации по стандартизации, метрологии и оценке соответствия» (ФГУП «СТАНДАРТИНФОРМ») совместно с Международной ассоциацией «Системсервис» (МА «Системсервис»)

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 30 апреля 2021 г. № 139-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 28 мая 2021 г. № 476-ст межгосударственный стандарт ГОСТ 34332.3—2021 введен в действие в качестве национального стандарта Российской Федерации с 1 января 2022 г.

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

- IEC 61508-2:2010 «Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью. Часть 2. Требования к системам» («Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for systems», NEQ);
- IEC 61508-4:2010 «Функциональная безопасность электрических/электронных/ программируемых электронных систем, связанных с безопасностью. Часть 4. Термины и сокращения» («Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations», NEQ);
- ISO/IEC Guide 51:2014 «Аспекты безопасности. Руководящие указания по их включению в стандарты» («Safety aspects — Guidelines for their inclusion in standards», NEQ)

6 ВВЕДЕН ВПЕРВЫЕ

7 Настоящий стандарт подготовлен на основе применения ГОСТ Р 53195.3—2015[1)]

[1)] Приказом Федерального агентства по техническому регулированию и метрологии от 28 мая 2021 г. № 476-ст ГОСТ Р 53195.3—2015 отменен с 1 января 2022 г.

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 3
4 Обозначения и сокращения 5
5 Общие требования 6
6 Требования к документации 6
7 Требования к управлению функциональной безопасностью 6
8 Требования к жизненному циклу Э/Э/ПЭ СБЗС систем 6
8.1 Общие положения 6
8.2 Спецификация требований к проектированию Э/Э/ПЭ СБЗС систем 9
8.3 Проектирование и реализация Э/Э/ПЭ СБЗС систем 12
8.4 Интеграция Э/Э/ПЭ СБЗС системы 31
8.5 Интеграция Э/Э/ПЭ СБЗС систем в комплексную систему безопасности 32
8.6 Подтверждение соответствия Э/Э/ПЭ СБЗС систем 32
8.7 Дополнительные требования к процедурам на стадии эксплуатации 33
8.8 Верификация Э/Э/ПЭ СБЗС систем 35
8.9 Оценка функциональной безопасности 36
Приложение А (обязательное) Методы и средства управления отказами Э/Э/ПЭ СБЗС систем в период эксплуатации 37
Приложение Б (обязательное) Методы и средства по предотвращению систематических отказов на стадиях жизненного цикла Э/Э/ПЭ СБЗС систем 52
Приложение В (обязательное) Охват диагностикой и доля безопасных отказов 61
Приложение Г (обязательное) Руководство по безопасности для применяемых изделий 63
Библиография 65

Введение

Современные здания и сооружения — объекты капитального строительства — представляют собой сложные системы, в состав которых входят система 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 при выполнении своих функций 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 и поддержания данного уровня в течение периода эксплуатации или использования этих объектов. К средствам снижения риска относятся системы, связанные с безопасностью зданий и сооружений (СБЗС системы). К таким системам относятся 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 используют 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 используются программируемые электронные СБЗС системы.

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

В настоящем стандарте установлены требования к стадиям проектирования, планирования и реализации Э/Э/ПЭ СБЗС систем на объектах, требования к аппаратным средствам, к полноте безопасности, предотвращению отказов, управлению систематическими отказами, поведению системы при обнаружении отказов, передаче данных, процедурам эксплуатации, технического обслуживания, модификации, верификации, оценке функциональной безопасности. Настоящий стандарт ориентирован на обеспечение соблюдения требований безопасности и антитеррористической защищенности зданий и сооружений, в том числе объектов транспортных инфраструктур, установленных [1] — [3], и на развитие базовых требований этих технических регламентов.

Настоящий стандарт распространяется на Э/Э/ПЭ СБЗС системы и их составляющие, включая сенсоры, исполнительные устройства и интерфейс «человек — машина». Он рассчитан на любой диапазон сложности Э/Э/ПЭ СБЗС систем и ориентирован на комплексное обеспечение безопасности и антитеррористической защищенности зданий и сооружений гражданского и промышленного строительства, включая объекты инфраструктур промышленности и энергетики, транспорта и связи, гидротехнические и мелиоративные сооружения.

Настоящий стандарт входит в комплекс стандартов с общим наименованием «Безопасность функциональная систем, связанных с безопасностью зданий и сооружений» и является третьим стандартом этого комплекса — «Часть 3. Требования к системам». Другие стандарты, входящие в этот комплекс:

- часть 1. Основные положения;
- часть 2. Общие требования;
- часть 4. Требования к программному обеспечению;
- часть 5. Меры по снижению риска, методы оценки;
- часть 6. Прочие средства уменьшения риска, системы мониторинга;
- часть 7. Порядок применения ГОСТ 34332, примеры расчетов.

Структура комплекса ГОСТ 34332 приведена на рисунке 1.

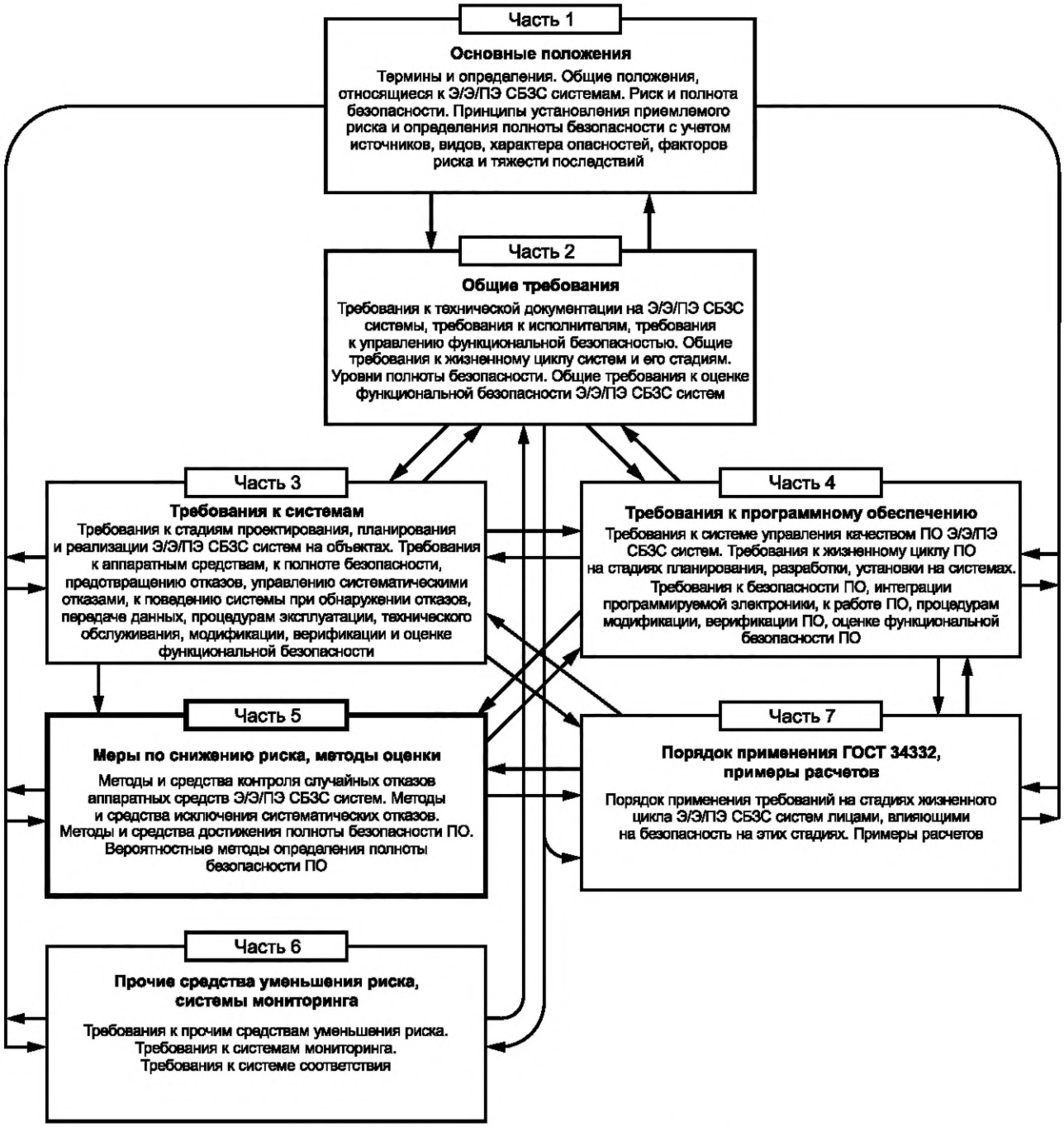


Рисунок 1 — Структура комплекса ГОСТ 34332

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

В каком месте	Напечатано	Должно быть		
Предисловие. Таблица согласования	—	Казахстан	KZ	Госстандарт Республики Казахстан

(ИУС № 4 2022 г.)

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Часть 3

Требования к системам

Functional safety of building/construction safety-related systems. Part 3. Requirements for systems

Дата введения — 2022—01—01

1 Область применения

Настоящий стандарт устанавливает:

- требования к функциональной безопасности электрических, электронных, программируемых электронных (Э/Э/ПЭ), связанных с безопасностью зданий и сооружений (СБЗС) систем (Э/Э/ПЭ СБЗС систем) и их аппаратных средств (АС) на стадиях проектирования, планирования и реализации Э/Э/ПЭ СБЗС систем.

Примечания

1 Под реализацией систем понимаются их установка на объекте, монтаж, пусконаладка, верификация, оценка и подтверждение соответствия.

2 Данные стадии являются частью базовой структуры жизненного цикла (ЖЦ) СБЗС систем, представленных совместно с ЖЦ объекта в ГОСТ 34332.2—2017 (рисунок 1). В настоящем стандарте не рассматриваются стадии ЖЦ систем, не относящиеся к Э/Э/ПЭ СБЗС системам, и часть стадий ЖЦ систем, которые относятся к периоду эксплуатации Э/Э/ПЭ СБЗС систем, а также прочие средства уменьшения риска;

- требования к действиям и процедурам, которые должны быть выполнены на этих стадиях для обеспечения функциональной безопасности Э/Э/ПЭ СБЗС систем, а также оценки и подтверждения соответствия на стадиях их ЖЦ, за исключением требований к программному обеспечению (ПО), которые установлены в ГОСТ 34332.4.

Примечание — Области применения настоящего стандарта и ГОСТ 34332.4 тесно взаимосвязаны. Эту взаимосвязь (рисунок 2) следует учитывать при применении настоящего стандарта;

- минимальный состав информации, необходимой для установки, ввода в эксплуатацию и подтверждения соответствия Э/Э/ПЭ СБЗС систем требованиям безопасности.

Настоящий стандарт распространяется на Э/Э/ПЭ СБЗС системы, включая комплексные системы безопасности (КСБ), устанавливаемые или установленные во вновь возводимых или реконструируемых зданиях и сооружениях (именуемых также в настоящем стандарте объектами) всех отраслей экономики, независимо от форм собственности и ведомственной принадлежности, включая жилые, общественные и производственные здания и сооружения, в том числе на Э/Э/ПЭ СБЗС системы объектов инфраструктуры перерабатывающей промышленности, энергетики, транспорта, включая линейные объекты, гидротехнические и мелиоративные сооружения, для обеспечения их безопасности и антитеррористической защищенности.

Настоящий стандарт применяют совместно с ГОСТ 34332.1, ГОСТ 34332.2, ГОСТ 34332.4 и ГОСТ 34332.5.

Настоящий стандарт не распространяется на Э/Э/ПЭ СБЗС систему, которая является 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 полноты безопасности (УПБ) по ГОСТ 34332.2— 2017 (пункт 7.6.12, таблицы 1 и 2).

Издание официальное

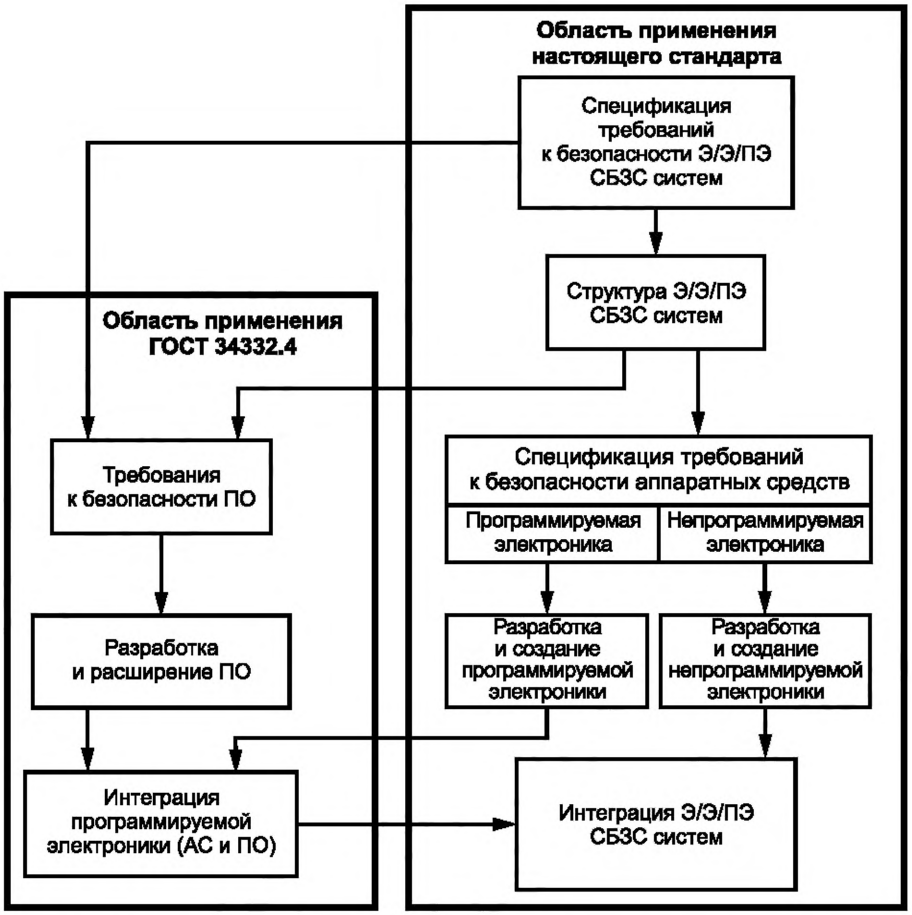


Рисунок 2 — Взаимосвязь областей применения настоящего стандарта и ГОСТ 34332.4

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 34332.1 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 34332.4—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

ГОСТ IEC/TS 61000-1-2 Электромагнитная совместимость (ЭМС). Часть 1-2. Общие положения. Методология достижения функциональной безопасности электрических и электронных систем, включая оборудование, в отношении электромагнитных помех

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации (gost.e-ecolog.ru по указателям национальных стандартов, издаваемым в государствах, указанных в предисловии, или на официальных сайтах соответствующих национальных органов по стандартизации. Если на документ дана недатированная ссылка, то следует использовать документ, действующий на текущий момент, с учетом всех внесенных в него изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то следует использовать указанную версию этого документа. Если после принятия настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение применяется без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ 34332.1 и ГОСТ 34332.2, а также следующие термины с соответствующими определениями:

3.1 **безопасный отказ** (safe failure): Отказ, который не приводит к переходу связанной с безопасностью системы в опасное состояние или в состояние невыполнения функции безопасности.

3.2 **время безопасности процесса** (process safety time): Интервал времени между опасным отказом и возникновением опасного события в случае невыполнения функции безопасности.

3.3 **время реакции функции безопасности** (safety function response time): Наихудшее время между срабатыванием датчика системы безопасности, подключенного к полевой шине, и достижением соответствующего безопасного состояния с помощью необходимого исполнительного устройства этой системы безопасности при наличии ошибок или отказов в канале функции безопасности.

3.4 избыточность (redundancy): Существование более одного средства выполнения необходимой функции или представления информации.

3.5 **интервал диагностических проверок** (diagnostic test interval): Установленный промежуток времени между отдельными проверками, предназначенными для обнаружения отказов в связанных с безопасностью системах.

3.6 **контрольная проверка** (proof test): Периодическая проверка, выполняемая для обнаружения отказов в связанных с безопасностью системах с целью последующего восстановления систем до исходного состояния в случае обнаружения отказа.

Примечание — Контрольная проверка предназначена для установления, находится ли система, связанная с безопасностью, в состоянии, гарантирующем установленную полноту безопасности.

3.7 **модуль** (module): Элемент конструкции или сформированный набор подходящих друг к другу элементов конструкций в здании или сооружении, элемент или дискретный компонент Э/Э/ПЭ СБЗС системы, или сформированный функциональный набор подходящих друг к другу дискретных компонентов аппаратных средств Э/Э/ПЭ СБЗС системы, или сформированный элемент программного обеспечения, или сформированная группа таких элементов.

3.8 **надежность** (dependability): Вероятность того, что автоматизированная система может выполнять требующуюся функцию в заданных условиях на протяжении заданного промежутка времени.

Примечания

1 Принято считать, что автоматизированная система в состоянии выполнять данную требующуюся функцию в начале заданного промежутка времени.

2 Понятие «надежность» также используют для обозначения показателя надежности, измеряемого данной вероятностью.

3 На протяжении среднего времени между отказами (MTBF) или среднего времени до отказа (MTTF) вероятность того, что автоматизированная система выполнит требующуюся функцию, уменьшается.

4 Надежность отличается от готовности.

3.9 **опасный отказ** (dangerous failure): Отказ управляемого оборудования или системы управления управляемым оборудованием с потенциальной возможностью вызова опасного события и/или невыполнения функции безопасности.

3.10 **отказ по общей причине** (common cause failure): Отказ оборудования, вызванный единичным событием в случаях, когда отказ не является следствием другого отказа.

3.11 **отказоустойчивое значение;** FV (fail-safe value, FV): Значения, которые выдаются вместо значения процесса, когда функция безопасности установлена в отказоустойчивое состояние.

Примечание — В настоящем стандарте значения отказоустойчивости (FV) должны всегда быть установлены в «0».

3.12 **отказоустойчивое состояние** (fail-safe state): Режим работы функции безопасности или оконечного элемента (исполнительного устройства), при котором посредством адекватных технических мер предотвращаются опасности детерминированно или посредством снижения риска до приемлемого значения.

3.13 **отказоустойчивость** (fault tolerance): Свойство технической системы сохранять свою работоспособность после отказа одного или нескольких составляющих компонентов.

Примечание — Отказоустойчивость определяется количеством любых последовательных единичных отказов компонентов, после которых сохраняется работоспособность системы в целом. Базовый уровень отказоустойчивости подразумевает защиту от отказа одного любого элемента — исключение единой точки отказа.

3.14 **охват диагностикой;** ОД (diagnostic coverage): Мера, принимаемая для относительного уменьшения вероятности опасных отказов зданий и сооружений, их конструкций, систем, аппаратуры, элементов, связанная с выполнением автоматических диагностических проверок.

3.15 **полевая шина** (fieldbus): Коммуникационная система, основанная на последовательной передаче данных и применяющаяся в промышленной автоматизации, автоматизации зданий и сооружений или приложениях управления процессами.

3.16 **полнота безопасности по отношению к систематическим отказам** (systematic safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью зданий и сооружений, по отношению к систематическим отказам, проявляющимся в опасном режиме.

3.17 **программный модуль** (software module): Программа или функционально завершенный фрагмент программы, предназначенный для хранения, трансляции, объединения, взаимодействия с другими программными модулями и загрузки в оперативную память.

3.18 **продукция промышленного производства** (industrial production products): Техническая продукция (изделие, система, аппаратное средство, программное обеспечение, их составная часть) разработанная и произведенная организацией-изготовителем для непосредственного применения широким кругом пользователей.

Примечания

1 Инженерные системы (включая Э/Э/ПЭ СБ системы с их АС и ПО), приобретаемые у изготовителя или поставщика, относятся к продукции промышленного производства.

2 Продукция промышленного производства может быть разработана, изготовлена, упакована, складирована, транспортирована, в том числе с пересечением таможенных границ, и применена в любом месте в соответствии с техническими условиями, предусмотренными ее изготовителем (см. рисунок 3).



Рисунок 3 — Создание и применение продукции промышленного производства

3 Продукция промышленного производства может быть проверена (оценена) на соответствие установленным для нее требованиям в любой испытательной лаборатории, аккредитованной на осуществление испытаний данной продукции на соответствие установленным для нее требованиям.

4 Продукция промышленного производства может быть использована в качестве комплектующих изделий для создания систем (включая Э/Э/ПЭ СБЗС системы, их АС и ПО), устанавливаемых в зданиях, сооружениях, линейных объектах капитального строительства в качестве их неотъемлемых частей (как продукции строительного производства).

3.19 **продукция строительного производства** (products of construction production): Результат строительной деятельности (капитального строительства).

Примечания

1 См. рисунок 4.



Рисунок 4 — Создание и использование продукции строительного производства

2 К продукции строительного производства относятся завершенные строительством здания, сооружения, линейные объекты.

3 Продукция строительного производства жестко «привязана» к местности и может быть применена, может выполнять установленные для нее функции и может быть оценена на соответствие установленным требованиям только в том месте, где здание (сооружение или линейный объект) построено и его составные части (системы, аппаратные средства и программное обеспечение) установлены.

4 При строительном производстве в качестве покупных комплектующих изделий и материалов используют продукцию промышленного производства [строительные материалы и изделия, в том числе Э/Э/ПЭ СБ системы (как продукцию промышленного производства)].

3.20 **система полевых шин** (fieldbus system): Система, использующая полевые шины с подключенными устройствами.

3.21 **систематический отказ** (systematic failure): Отказ системы, аппаратного средства или программного обеспечения, связанный с некоторой повторяющейся причиной в процессах проектирования, производства, монтажа или пусконаладки, которая может быть устранена или изменена только путем модификации этих процессов.

3.22 **случайный отказ аппаратного средства;** отказ АС (random hardware failure): Отказ аппаратного средства, возникающий в случайный момент времени в результате действия одного или нескольких возможных механизмов ухудшения его характеристик.

3.23 **спецификация** (specification): Определение и перечень специфических особенностей чего-либо.

Примечание — Примерами спецификации являются технический документ, содержащий состав или описание объекта (системы, подсистемы, изделия, АС, ПО), либо документ с перечислением состава, технических условий или требований, которым должны удовлетворять изготавливаемая(ое) или заказываемая(ое) система, подсистема, изделие, АС, ПО.

3.24 **тестовая программа** (test harness): Программный продукт, предназначенный для имитации среды, в которой должно действовать разрабатываемое программное обеспечение или аппаратное средство.

Примечание — Имитация среды осуществляется путем передачи тестовых данных в программу и регистрации ответов.

3.25 **остаточный коэффициент потери информации** (rate of residual information loss): Отношение числа необнаруженных утерянных сообщений к общему числу отправленных сообщений.

3.26 **остаточный коэффициент ошибок** (residual error rate): Отношение числа необнаруженных ошибочных сообщений к общему числу отправленных сообщений.

3.27 **уровень эффективности защиты;** УЭЗ (performance level, PL): Дискретный уровень, применяющийся для определения способности связанных с безопасностью частей системы управления выполнять функцию безопасности в прогнозируемых условиях.

3.28 **устройство ввода-вывода;** устройство В—В (IO-device): Пассивный объект коммуникаций, способный принимать сообщения и отправлять их в ответ другому объекту коммуникаций, который может быть контроллером ввода-вывода или устройством ввода-вывода.

3.29 **целевая мера отказов** (target failure measure): Величина отказов, значение которой не должно быть превышено и к которой следует стремиться для достижения и поддержания необходимого уровня полноты безопасности функции безопасности, выполняемой Э/Э/ПЭ СБЗС системой.

Примечание — При низкой частоте запросов к функции безопасности Э/Э/ПЭ СБЗС системы величина отказов выражается как средняя вероятность отказов (PFD_{avg}), а при высокой частоте запросов или непрерывном запросе — как средняя частота (интенсивность) отказов в соответствии с ГОСТ 34332.2—2017 (пункт 7.6.12).

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения и обозначения:

АОП — анализ общих причин;

ДБО — доля безопасных отказов;

ИОП — источник(и) общей причины;

ИС — интегральная схема;

НПЭ — непрограммируемая электроника;

НУ — непрограммируемое устройство;

ОЗУ — оперативное запоминающее устройство;

ПЗУ — программируемое запоминающее устройство;

ПЭ — программируемая электроника;

СБ — связанная(ое, ый) с безопасностью (система, подсистема, аппаратное средство, программное обеспечение или их элемент);

СИС — специализированная интегральная схема (микросхема);

ССО — стойкость к систематическим отказам;

УО — управляемое оборудование;

BIM — обозначение технологии информационного моделирования в строительстве.

5 Общие требования

Соответствие Э/Э/ПЭ СБЗС систем требованиям настоящего стандарта — по ГОСТ 34332.2—2017 (подраздел 5.1).

Требования к конкретным Э/Э/ПЭ СБЗС системам должны быть установлены с учетом: природных факторов, характера опасностей, необходимого снижения риска и последствий, требуемого УПБ, сложности системы, физической среды применения, новизны разработки.

6 Требования к документации

Требования к документации Э/Э/ПЭ СБЗС систем — по ГОСТ 34332.2—2017 (подраздел 5.2).

7 Требования к управлению функциональной безопасностью

Требования к управлению функциональной безопасностью Э/Э/ПЭ СБЗС систем — по ГОСТ 34332.2—2017 (раздел 6).

8 Требования к жизненному циклу Э/Э/ПЭ СБЗС систем

8.1 Общие положения

8.1.1 Цели и требования, основные положения

8.1.1.1 Настоящий пункт устанавливает цели и требования для ЖЦ Э/Э/ПЭ СБЗС систем.

Примечания

1 Цели и требования к полному ЖЦ Э/Э/ПЭ СБЗС систем установлены в ГОСТ 34332.2—2017, раздел 7.

2 Требования к каждой конкретной Э/Э/ПЭ СБЗС системе в виде спецификации требований к проектированию Э/Э/ПЭ СБЗС системы формируют после распределения функций безопасности по всем Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска.

3 Распределению всех необходимых функций безопасности (и антитеррористической защищенности) по Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска предшествуют разработка концепции безопасности, определение назначения и области применения всех СБЗС систем (включая КСБ) и средств уменьшения риска, анализ опасностей и рисков, подлежащих компенсации этими системами и средствами, и определение требований ко всем функциям безопасности (см. ГОСТ 34332.2—2017, подразделы 7.2—7.5 и рисунок 1, блоки 1—4).

4 В случае применения КСБ изначально предусматривают необходимые условия объединения Э/Э/ПЭ СБЗС в КСБ и условия, обеспечивающие возможность такого объединения (сложность систем КСБ, взаимосвязь Э/Э/ПЭ СБЗС систем между собой, совместимость протоколов и стыков, синхронизация, учет времен откликов систем на запросы и др.).

8.1.1.2 Для каждой стадии ЖЦ Э/Э/ПЭ СБЗС систем должны быть указаны:

- цели, которые должны быть достигнуты;
- область применения конкретной стадии;
- ссылка на пункт, содержащий требования;
- входы стадии;
- выходы стадии.

8.1.2 Цели

8.1.2.1 Первая цель настоящего раздела состоит в структурировании на систематической основе рассматриваемых стадий ЖЦ Э/Э/ПЭ СБЗС систем для обеспечения достижения требуемой функциональной безопасности Э/Э/ПЭ СБЗС систем.

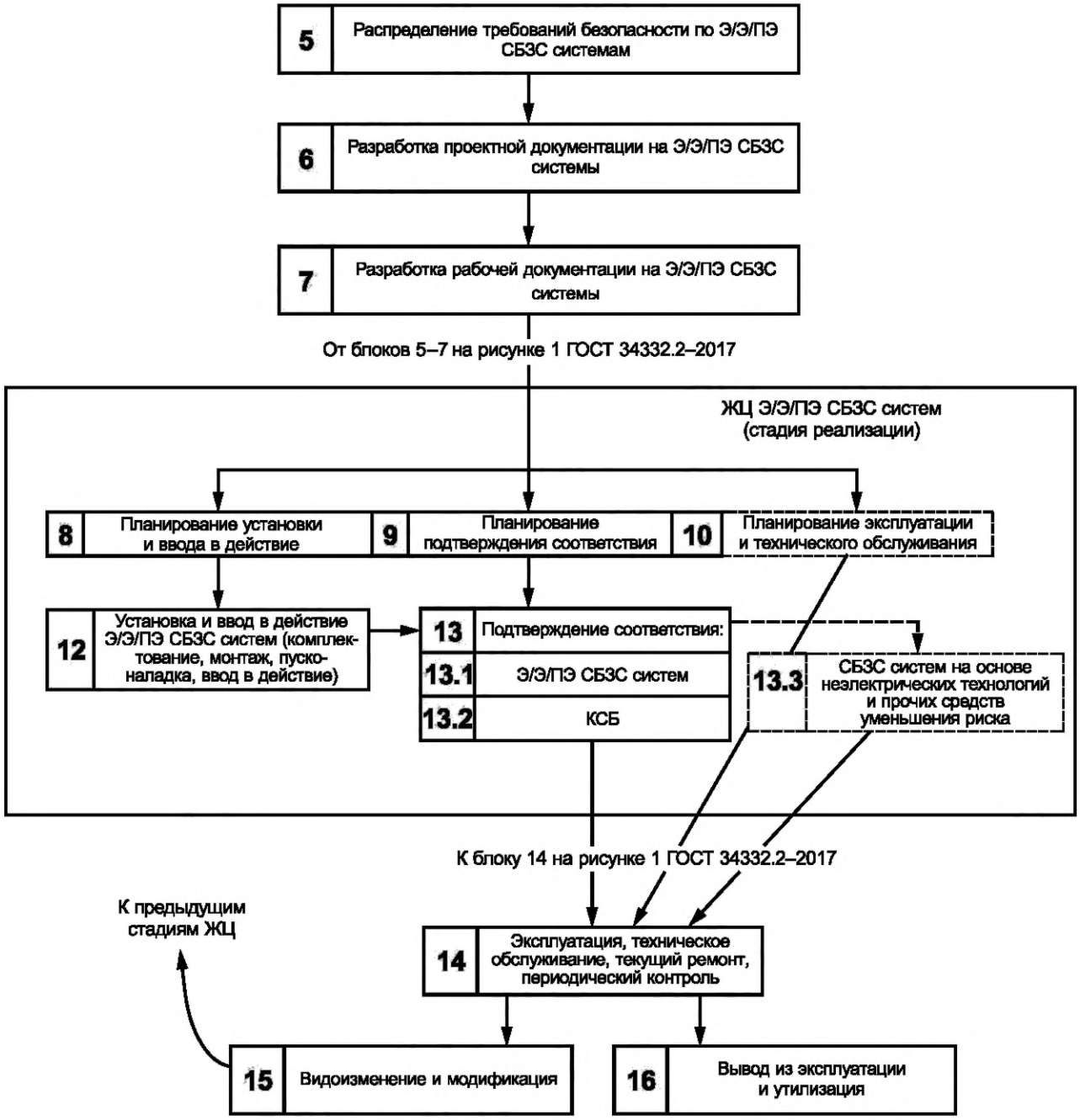
Примечание — Цели и требования для полного ЖЦ Э/Э/ПЭ СБЗС систем, включая КСБ, с учетом положений, отраженных во введении, установлены в ГОСТ 34332.2—2017 (раздел 7).

8.1.2.2 Вторая цель заключается в обеспечении документирования всей информации, относящейся к функциональной безопасности Э/Э/ПЭ СБЗС систем на протяжении всего их ЖЦ.

Примечание — Требования к документации, представляемой на всех стадиях ЖЦ полной системы обеспечения безопасности, установлены в ГОСТ 34332.2—2017 (подраздел 5.2).

8.1.3 Требования

8.1.3.1 Структура ЖЦ Э/Э/ПЭ СБЗС системы, используемого в качестве требования соответствия настоящему стандарту, представлена на рисунке 5. Для каждой стадии ЖЦ могут быть установлены необходимые промежуточные стадии с указанием для каждой из них области применения, целей, которые должны быть достигнуты, входов и выходов стадий. На каждой из промежуточных стадий должны быть достигнуты все цели и выполнены требования подразделов настоящего стандарта.



Примечание — В рамке показаны только те промежуточные стадии ЖЦ Э/Э/ПЭ СБЗС системы, которые составляют стадию реализации ЖЦ всей системы. Полный ЖЦ Э/Э/ПЭ СБЗС систем также включает в себя блоки, определенные для последующих стадий ЖЦ полной системы [см. ГОСТ 34332.2—2017 (рисунок 1, блоки 15 и 16)].

Рисунок 5 — Структура ЖЦ Э/Э/ПЭ СБЗС системы (стадии проектирования и реализации)

8.1.3.2 В случае использования другого ЖЦ Э/Э/ПЭ СБЗС систем он должен быть определен как часть управления деятельностью по функциональной безопасности Э/Э/ПЭ систем по ГОСТ 34332.2—2017 (раздел 6), а также должны быть достигнуты цели и требования, приведенные в настоящем стандарте.

8.1.3.3 Для рассмотрения ЖЦ сложных систем комплексного обеспечения безопасности и антитеррористической защищенности объекта, включая КСБ с их АС и ПО, на стадиях проектирования и реализации может быть применена подробная V-образная модель (рисунок 6).

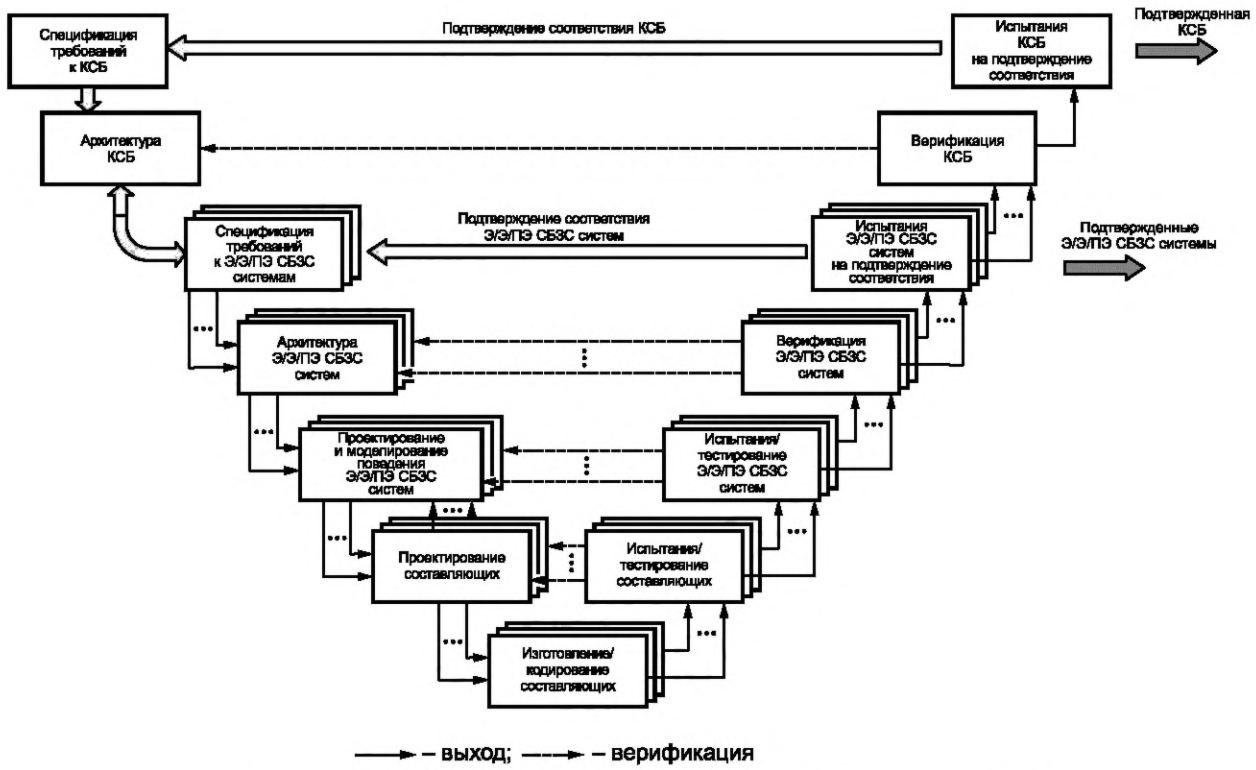


Рисунок 6 — V-образная модель стадий проектирования и реализации КСБ

Примечания

1 При этом используют системный комплексный процессный риск-ориентированный подход. Вначале формируют спецификацию требований к проектированию КСБ, затем проектируют ее архитектуру с учетом взаимосвязей, входящих в нее Э/Э/ПЭ СБЗС систем. Аналогичные шаги последовательно применяют к Э/Э/ПЭ СБЗС системам, подсистемам и их составляющим, вплоть до модулей АС и ПО (нисходящая ветвь завершается реализацией модулей АС и программных кодов ПО). Выходы каждого шага левой части V-образной модели становятся входной информацией для следующего шага (при необходимости может быть осуществлен возврат к предыдущему или более раннему шагу). Модули, подсистемы и системы подвергаются верификации в обратном порядке по восходящей ветви, т. е. моделируются результаты верификации и тестирования модулей АС и ПО, последовательно объединенных в Э/Э/ПЭ СБЗС подсистемы, системы и, наконец, в полную КСБ (результаты любого шага могут вызвать необходимость изменений проекта на любом из предыдущих шагов). На последнем шаге, после того как составляющие интегрированы в полную систему, выполняется подтверждение соответствия.

2 После разработки концепции безопасности объекта, определения области применения СБЗС систем, анализа опасностей и рисков, определения требований к функциям безопасности систем [см. ГОСТ 34332.2—2017 (подразделы 7.2—7.5)] формируют спецификацию требований к проектированию КСБ, проектируют ее архитектуру, распределяя функции безопасности по входящим в нее Э/Э/ПЭ СБЗС системам, с учетом взаимосвязей и взаимовлияния систем, а также прочим средствам уменьшения риска. Аналогичные шаги последовательно применяют к отдельным Э/Э/ПЭ СБЗС системам, подсистемам и их составляющим, вплоть до модулей АС и ПО. Нисходящая ветвь завершается реализацией модулей АС и программных кодов ПО. Выходы каждого шага нисходящей ветви V-образной модели становятся входной информацией для следующего шага (при необходимости может быть осуществлен возврат к предыдущему или более раннему шагу). Установленные и смонтированные на объекте модули, подсистемы, системы и КСБ подвергают верификации в обратном порядке по восходящей ветви V-образной модели. Вначале осуществляют тестирование и верификацию модулей АС и ПО, затем подсистем, систем и, наконец, КСБ по мере их реализации. На последнем шаге, после того как составляющие интегрированы в КСБ, осуществляют подтверждение соответствия.

3 Недостижение целей и требований любой промежуточной стадии на нисходящей ветви V-образной модели, обнаруженное в результате проведения соответствующих процедур тестирования и верификации на восходящей ветви, — недостижение целей и требований к проектированию из-за ошибки проектировщика или неверного выбора им покупного модуля (АС и ПО), подсистемы, системы (как продукции промышленного производства) — приводит к необходимости возврата к началу соответствующей или более ранней стадии на нисходящей ветви V-образной модели. В этом случае потребуются дополнительные затраты времени и ресурсов, чем они больше, тем выше точка обнаружения несоответствия на восходящей ветви.

4 Временные и ресурсные затраты по примечанию 3 могут быть существенно снижены в случае осуществления полного моделирования поведения Э/Э/ПЭ СБЗС систем и всех их составляющих с использованием методов и средств информационного моделирования в строительстве (BIM-технологии).

8.1.3.4 Процедуры управления функциональной безопасностью по ГОСТ 34332.2—2017 (раздел 6) следует выполнять параллельно рассматриваемым стадиям ЖЦ Э/Э/ПЭ СБЗС систем.

8.1.3.5 Входы каждой стадии ЖЦ Э/Э/ПЭ СБЗС систем должны соответствовать определенным для этих стадий целям и требованиям (см. 8.1—8.9). Результаты каждой стадии должны быть документированы лицами, ответственными за обеспечение функциональной безопасности на соответствующей стадии ЖЦ систем.

8.1.3.6 Каждую стадию ЖЦ Э/Э/ПЭ СБЗС системы подразделяют на элементарные действия с определением для каждого из них области применения, входов и выходов (см. таблицу 1).

Примечание — Требования к прочим средствам уменьшения риска устанавливают в соответствующем стандарте.

8.1.3.7 Выходы каждой стадии ЖЦ Э/Э/ПЭ СБЗС системы должны быть документально оформлены (см. ГОСТ 34332.2—2017 (подраздел 5.2)], если не будет обосновано, что они являются результатом деятельности по управлению функциональной безопасностью [см. ГОСТ 34332.2—2017 (раздел 6)].

8.1.3.8 Результаты (выходы) каждой стадии ЖЦ Э/Э/ПЭ СБЗС системы должны быть приведены в соответствие с определенными для этой стадии целями и требованиями (см. 8.1.1).

8.2 Спецификация требований к проектированию Э/Э/ПЭ СБЗС систем

8.2.1 Цель спецификации требований к проектированию состоит в задании требований к проектированию для каждой Э/ Э/ ПЭ СБЗС системы в терминах составляющих, из которых состоит система (подсистем, модулей и других составляющих).

Примечание — Как правило, спецификацию требований к проектированию Э/Э/ПЭ СБЗС системы формируют из спецификации требований к полной системе обеспечения безопасности и антитеррористической защищенности объекта (включая КСБ) с помощью декомпозиции функций безопасности и распределения частей функции безопасности между Э/Э/ПЭ СБЗС системами, подсистемами, их составляющими (например, группами датчиков, логическими решателями либо исполнительными устройствами) и прочими средствами уменьшения риска. Требования для подсистем могут быть включены в спецификацию требований к проектированию Э/Э/ПЭ СБЗС системы или представлены в виде отдельного документа либо в виде ссылки на них в спецификации требований проектирования Э/Э/ПЭ СБЗС системы. Далее подсистемы могут быть декомпозированы на модули, элементы и их совокупности, с тем чтобы соответствовать требованиям проектирования и разработки по 8.3, 8.4. Требования для этих составляющих могут быть включены в требования к декомпозируемым подсистемам или могут быть представлены в виде отдельного документа или ссылки на них в требованиях к подсистеме.

Таблица 1 — Стадии проектирования, планирования и реализации Э/Э/ПЭ СБЗС систем

Стадия ЖЦ Э/Э/ПЭ СБЗС системы	Цели	Область применения	Структурный элемент	Входы	Выходы
Стадия 5. Распределение требований безопасности по Э/Э/ПЭ СБЗС системам (блок 5 на рисунке 5)	Получение обоснованных исходных данных для проектирования Э/Э/ПЭ СБЗС систем	Э/Э/ПЭ СБЗС системы	8.2	Результаты анализа опасностей и угроз для распределения требований безопасности по Э/Э/ПЭ СБЗС системам	Спецификация требований к проектированию Э/Э/ПЭ СБЗС систем

Продолжение таблицы 1

Стадия ЖЦ Э/Э/ПЭ СБЗС системы	Цели	Область применения	Структурный элемент	Входы	Выходы
Стадия 6. Разработка проектной документации на Э/Э/ПЭ СБЗС системы (блок 6 на рисунке 5)	Создание проектной документации на Э/Э/ПЭ СБЗС системы, со спецификацией требований к системам, средствам, их составляющим, к взаимодействию между собой и окружением, отвечающей установленным требованиям	Э/Э/ПЭ СБЗС системы	8.3	Спецификация требований к проектированию Э/Э/ПЭ СБЗС систем	Проектная документация на Э/Э/ПЭ СБЗС системы
Подстадия 6.1. Создание КСБ с применением V-образной модели (блок 6 на рисунке 5)	Создание сложных КСБ, удовлетворяющих требованиям настоящего стандарта	Э/Э/ПЭ СБЗС системы	8.1.3.3, 8.5.3	Исходные данные на проектирование и реализацию КСБ на защищаемом объекте (см. примечание)	КСБ, установленная и введенная в действие на объекте защиты
Стадия 7. Разработка рабочей документации на Э/Э/ПЭ СБЗС системы (блок 7 на рисунке 5)	Обеспечение должного выполнения действий на последующих стадиях ЖЦ Э/Э/ПЭ СБЗС систем	Э/Э/ПЭ СБЗС системы	8.3.10	Комплект проектной документации на Э/Э/ПЭ СБЗС системы	Рабочая документация на Э/Э/ПЭ СБЗС системы (см. примечание)
Стадия 8. Планирование установки и ввода в действие СБЗС систем (блок 8 на рисунке 5)	Разработка плана установки и ввода в действие Э/Э/ПЭ СБЗС систем	Э/Э/ПЭ СБЗС системы	8.3.11	Комплект проектной и рабочей документации, план установки и ввода в действие Э/Э/ПЭ СБЗС систем	План установки и ввода в действие Э/Э/ПЭ СБЗС систем
Стадия 9. Планирование подтверждения соответствия Э/Э/ПЭ СБЗС систем (блок 9 на рисунке 5)	Разработка плана осуществления подтверждения соответствия СБЗС систем	Э/Э/ПЭ СБЗС системы	8.3.12	Комплект проектной и рабочей документации, план осуществления подтверждения соответствия	План подтверждения соответствия Э/Э/ПЭ СБЗС систем
Стадия 12. Установка и ввод в действие Э/Э/ПЭ СБЗС систем (блок 12 на рисунке 5)	Должное выполнение действий по установке и вводу в действие Э/Э/ПЭ СБЗС систем и КСБ на объекте	Э/Э/ПЭ СБЗС системы	8.3.13	Комплект проектной и рабочей документации, план установки и ввода в действие Э/Э/ПЭ СБЗС систем	Э/Э/ПЭ СБЗС системы, установленные и введенные в действие на объекте
Стадия 13. Подтверждение соответствия Э/Э/ПЭ СБЗС систем (блок 13 на рисунке 5)	Подтверждение соответствия Э/Э/ПЭ СБЗС систем требованиям настоящего стандарта	Э/Э/ПЭ СБЗС системы	8.6, 8.13	Э/Э/ПЭ СБЗС системы, установленные и введенные в действие на объекте	Документ, подтверждающий соответствие Э/Э/ПЭ СБЗС систем требованиям настоящего стандарта
Стадия 14. Эксплуатация и техническое обслуживание Э/Э/ПЭ СБЗС систем (блок 14 на рисунке 5)	Обеспечение устойчивой эксплуатации Э/Э/ПЭ СБЗС систем в соответствии с требованиями ГОСТ 34332	Э/Э/ПЭ СБЗС системы	8.7.1	Комплект эксплуатационной документации и документации на техническое обслуживание Э/Э/ПЭ СБЗС систем (см. примечание)	Устойчивая эксплуатация Э/Э/ПЭ СБЗС систем, отвечающая требованиям настоящего стандарта

Окончание таблицы 1

Стадия ЖЦ Э/Э/ПЭ СБЗС системы	Цели	Область применения	Структурный элемент	Входы	Выходы
Стадия 15. Видоизменение и модификация Э/Э/ПЭ СБЗС систем (блок 15 на рисунке 5)	Обеспечение возможности совершенствования Э/Э/ПЭ СБЗС систем при долговременной эксплуатации объектов защиты (зданий и сооружений)	Э/Э/ПЭ СБЗС системы	8.7.1	Проекты модифицированных Э/Э/ПЭ СБЗС систем для установки на защищаемом объекте	Модифицированные Э/Э/ПЭ СБЗС системы, установленные и введенные в действие на объекте, отвечающие требованиям соответствия настоящему стандарту
Примечание — Разработку эксплуатационной документации, а также документации на техническое обслуживание и текущий ремонт осуществляют на стадии подготовки рабочей документации. Стадия эксплуатации Э/Э/ПЭ СБЗС систем в настоящем стандарте не рассматривается (см. раздел 1).					

8.2.2 Общие требования

8.2.2.1 Спецификацию требований к проектированию конкретной Э/Э/ПЭ СБЗС системы формируют исходя из полных требований к системам комплексного обеспечения безопасности и антитеррористической защищенности объекта (включая КСБ) после распределения функций безопасности по отдельным Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска в соответствии с ГОСТ 34332.2—2017 (подраздел 7.6).

Примечание — Не рекомендуется, чтобы одна и та же Э/Э/ПЭ СБЗС система выполняла функции безопасности и функции, не относящиеся к безопасности. Хотя это соответствует требованиям настоящего стандарта, такое объединение приводит к большим сложностям при выполнении работ в процессе ЖЦ Э/Э/ПЭ системы (например, при проектировании, подтверждении соответствия, оценке функциональной безопасности и техническом обслуживании).

8.2.2.2 Требования к проектированию Э/Э/ПЭ СБЗС систем должны быть выражены и структурированы таким образом, чтобы они были:

- ясными, точными, недвусмысленными, поддающимися проверке, пригодными для тестирования, поддерживаемыми и реализуемыми;
- оформлены в письменном виде для обеспечения возможности их применения и правильного понимания на любой из стадий ЖЦ Э/Э/ПЭ СБЗС системы;
- выводимыми из спецификации требований к полной системе обеспечения безопасности и антитеррористической защищенности объекта.

8.2.3 Спецификация требований к проектированию Э/Э/ПЭ СБЗС системы

8.2.3.1 В спецификацию требований к проектированию Э/Э/ПЭ СБЗС системы включают требования, относящиеся к функциям безопасности (см. 8.2.3.2), и требования, относящиеся к полноте безопасности (см. 8.2.3.4).

8.2.3.2 В спецификацию требований к проектированию Э/Э/ПЭ СБЗС системы включают сведения обо всех АС и ПО, необходимых для осуществления требуемых функций безопасности. В спецификацию требований для каждой функции безопасности следует включать:

- требования к подсистемам, модулям и составляющим АС и ПО (по мере необходимости);
- требования к интеграции подсистем, модулей и составляющих АС и ПО, соответствующие спецификации требований к функциям безопасности Э/Э/ПЭ СБЗС системы;
- сведения об интерфейсе между оператором и Э/Э/ПЭ СБЗС системой;
- сведения об интерфейсах между Э/Э/ПЭ СБЗС системой и внешними системами (подсистемами), а также УО;
- описание поведения Э/Э/ПЭ СБЗС системы, в том числе ее поведение при отказе и необходимой реакции на отказ (например, выдача аварийного сигнала, автоматический останов и т. п.);
- описание взаимодействий между АС и ПО, а также (при необходимости) требуемых ограничений для АС и ПО.

Примечание — Если данные взаимодействия не известны до завершения проектирования, то устанавливают только общие ограничения;

- описание предельных и ограничивающих условий для Э/Э/ПЭ СБЗС системы и связанных с ней подсистем и модулей, например ограничения синхронизации либо ограничения, связанные с возможностью отказов по общей причине;

- специфические требования, относящиеся к процедурам запуска и повторного запуска Э/Э/ПЭ СБЗС системы.

8.2.3.3 В спецификацию требований к проектированию Э/Э/ПЭ СБЗС системы включают подробную информацию обо всех АС и ПО, необходимых для выполнения требуемых функций безопасности. В спецификацию следует включать для каждой функции безопасности:

- описание архитектуры каждой подсистемы, необходимое для удовлетворения архитектурных ограничений полноты безопасности АС (см. 8.3.4);

- соответствующие параметры для расчета надежности, необходимые для достижения целевого показателя отказа, такие как требуемая частота проверочных испытаний всех модулей АС.

Примечание — Информация о конкретном применении не должна быть ограничена. Данная информация важна для технического обслуживания, при котором интервал между контрольными испытаниями должен быть не менее предсказуемого интервала для конкретного применения;

- описание действий, которые должны быть выполнены в случае обнаружения опасного отказа, выявленного диагностикой;

- требования, ограничения, функции и возможности, позволяющие проводить проверочные испытания АС систем;

- описание требований к используемому оборудованию и экстремальным условиям окружающей среды (например, температуры, влажности, механических, электрических условий), которые указаны в требованиях к ЖЦ Э/Э/ПЭ СБЗС системы, включая производство, хранение, транспортирование, испытания, установку, ввод в эксплуатацию, эксплуатацию и техническое обслуживание;

- значение уровня электромагнитной устойчивости.

8.2.3.4 В спецификацию требований к проектированию Э/Э/ПЭ СБЗС систем следует также включать:

- сведения о том, как в проекте достигаются необходимый УПБ и требуемая целевая мера отказов для функции безопасности, которые определены в спецификации требований к полноте безопасности Э/Э/ПЭ СБЗС системы [см. ГОСТ 34233.2—2017 (пункты 7.5.6—7.5.11)], в частности:

процедуры испытаний и критерии, применяемые для подтверждения соответствия заданному в спецификации значению уровня электромагнитной устойчивости.

Примечание — Руководство по спецификации испытаний пределов электромагнитной устойчивости для составляющих СБ-систем (подсистем) представлено в ГОСТ IEC/TS 61000-1-2;

описание стратегии по устранению подтвержденного отказа;

требования к обеспечению качества — описание мер по управлению качеством, необходимых для управления безопасностью (см. ГОСТ 34332.2—2017, пункт 6.2.2).

8.2.3.5 Спецификацию требований к проектированию Э/Э/ПЭ СБЗС системы следует постоянно уточнять по ходу разработки проекта и по мере необходимости следует обновлять при его модификации.

8.2.3.6 Во избежание ошибок во время составления спецификации требований к проектированию Э/Э/ПЭ СБЗС системы необходимо использовать группу методов и средств в соответствии с таблицей А.1 приложения А и таблицей Б.1 приложения Б.

8.2.3.7 Должны быть рассмотрены последствия накладываемых на архитектуру требований к проектированию Э/Э/ПЭ СБЗС системы.

Примечание — Такое рассмотрение, как правило, включает в себя анализ простоты реализации для достижения требуемого УПБ (включая анализ архитектуры и пропорциональное распределение функциональности, реализуемой за счет конфигурирования или применения встроенной системы).

8.3 Проектирование и реализация Э/Э/ПЭ СБЗС систем

8.3.1 Цель требований настоящего подраздела (см. блоки 5—13 на рисунке 5) состоит в обеспечении соответствия проектной и рабочей документации на Э/Э/ПЭ СБЗС системы спецификации требований к ее проектированию (см. 8.2.3) в части требований к функции(ям) безопасности и требований к полноте безопасности.

8.3.2 Общие требования

8.3.2.1 Проектирование Э/Э/ПЭ СБЗС системы должно быть проведено в соответствии со спецификацией требований к ее проектированию (см. 8.2.3) с учетом всех требований 8.2.3.

8.3.2.2 Если Э/Э/ПЭ СБЗС система входит в состав КСБ, в спецификацию требований к ее проектированию включают требования, обеспечивающие устойчивое взаимодействие системы с другими Э/Э/ПЭ СБЗС системами (совместимость протоколов и стыков, синхронизируемость, учет времен откликов на запросы):

а) к полноте безопасности АС, включая:

1) требования к архитектурным ограничениям на полноту безопасности АС (см. 8.3.4);

2) требования к выполнению количественной оценки случайных отказов (см. 8.3.6);

3) требования к предотвращению систематических отказов (см. 8.3.7);

б) к специальной архитектуре СИС с избыточностью схем на кристалле в соответствующих случаях, если не может быть приведено обоснование того, что тот же самый уровень независимости между различными каналами достигается с помощью применения другого набора средств (см. [4]).

8.3.2.3 Если Э/Э/ПЭ СБЗС система предназначена для выполнения функции безопасности и функции, не относящейся к безопасности, то все АС и ПО следует рассматривать как связанные с безопасностью до тех пор, пока не будет установлено, что эти функции реализуются достаточно независимо (т. е. отказ какой-либо функции, не относящейся к безопасности, не станет причиной отказа функций, связанных с безопасностью).

Примечания

1 Достаточную независимость данных функций устанавливают демонстрацией того, что вероятность зависимого отказа между компонентами, не связанными с безопасностью, и компонентами, связанными с безопасностью, достаточно низка по сравнению с самым высоким УПБ, относящимся к используемым функциям безопасности.

2 Следует по возможности избегать совмещения функций, связанных с безопасностью, и функций, не связанных с безопасностью, в одной и той же Э/Э/ПЭ СБЗС системе. Такое совмещение, допускаемое настоящим стандартом, может усложнить систему и привести к трудностям при выполнении работ в процессе ЖЦ системы (например, при проектировании, подтверждении соответствия, оценке функциональной безопасности и техническом обслуживании).

8.3.2.4 Требования к АС и ПО следует определять УПБ функций безопасности, имеющих самый высокий УПБ, если не будет показано, что выполнение функций безопасности различных УПБ достаточно независимо.

Примечания

1 Достаточную независимость выполнения функций безопасности устанавливают демонстрацией вероятности зависимого отказа между компонентами, выполняющими функции безопасности различных УПБ, достаточно низкой по сравнению с самым высоким УПБ, относящимся к рассматриваемым функциям безопасности.

2 Если Э/Э/ПЭ СБЗС системой выполняется несколько функций безопасности, то необходимо рассмотреть возможность возникновения отказа в выполнении нескольких функций безопасности из-за единственной ошибки. В такой ситуации требования к АС и ПО допускается задавать на основе УПБ более высокого, чем для любой из функций безопасности, в зависимости от риска возникновения такого отказа.

8.3.2.5 Если требуется независимость функций безопасности (см. 8.3.2.3), то в процессе проектирования должны быть документально оформлены:

- метод достижения независимости;
- обоснование метода.

Пример — Для анализа предсказуемых видов отказа, которые могут нарушить независимость функций безопасности, и для определения интенсивности таких отказов используют метод анализа вида, последствий и критичности отказов или метод анализа зависимых отказов.

8.3.2.6 Следует обеспечивать доступность требований к связанному с безопасностью ПО (см. ГОСТ 34332.4) разработчику Э/Э/ПЭ СБЗС системы.

8.3.2.7 Разработчик Э/Э/ПЭ СБЗС системы должен провести анализ требований к связанному с безопасностью ПО и связанным с безопасностью АС с тем, чтобы убедиться, что они корректно специфицированы. В частности, разработчик Э/Э/ПЭ СБЗС системы должен рассмотреть:

- функции безопасности;
- интерфейсы между оборудованием и обслуживающим персоналом.

8.3.2.8 В проектной документации на Э/Э/ПЭ СБЗС систему должны быть определены методы и средства, необходимые для достижения и поддержания требуемого УПБ в течение стадий ЖЦ этой системы.

8.3.2.9 В проектной документации на Э/Э/ПЭ СБЗС систему должно быть приведено обоснование выбранных для интеграции методов и средств, которые обеспечивают требуемый УПБ.

Примечание — Принятие общего подхода, предусматривающего независимое принятие вида Э/Э/ПЭ СБЗС системы (включающей в себя датчики, исполнительные устройства и т. д.), ее АС и ПО, диагностических тестов и инструментов программирования и используемых (где это возможно) подходящих языков программирования, позволяет снизить сложность разработки системных приложений Э/Э/ПЭ СБЗС системы.

8.3.2.10 В процессе проектирования все существенные (в соответствующих случаях) взаимодействия АС и ПО должны быть идентифицированы, оценены и документально оформлены.

8.3.2.11 В состав проекта на сложные Э/Э/ПЭ СБЗС системы и КСБ должны быть включены также индивидуальные проекты (части проектной документации) на более простые составляющие системы (подсистемы). Для каждого(ой) из них должен быть предусмотрен набор тестов для интеграции (см. 8.3.12.4).

Примечания

1 Конкретная подсистема может состоять из одной составляющей или группы составляющих. Полная Э/Э/ПЭ СБЗС система может состоять из множества отдельных подсистем, которые при их объединении обеспечивают выполнение предусмотренной функции безопасности. Подсистема может иметь несколько каналов.

2 При необходимости должны быть использованы существующие проверенные на практике подсистемы. Данное положение является в общем случае верным, только если существует почти стопроцентное совпадение функциональных возможностей, пропускной способности и быстродействия существующей подсистемы с новыми требованиями или верифицированная (проверенная) подсистема структурирована так, чтобы пользователь мог выбрать лишь требуемые функции, пропускную способность и производительность для требуемого конкретного применения. Избыточные функциональные возможности, пропускная способность или быстродействие могут повредить безопасность системы, если существующие подсистемы чрезмерно усложнены или имеют неиспользуемые возможности и не обеспечена защита от непредусмотренных функций. Следует избегать избыточных функциональных возможностей, пропускной способности или быстродействия подсистем, если не может быть обеспечена защита от выполнения ими непредусмотренных функций.

8.3.2.12 При завершении предварительного проектирования Э/Э/ПЭ СБЗС системы необходимо провести анализ для определения, может ли какой-либо разумно предсказуемый отказ системы вызвать опасную ситуацию или сформировать запрос к какому-либо средству управления риском. При обнаружении возможности возникновения любого из таких отказов первым по приоритету действием должно быть изменение проекта Э/Э/ПЭ СБЗС системы во избежание таких видов отказов. Если это выполнить не удается, то должны быть приняты меры по снижению вероятности таких видов отказов до уровня, соизмеримого с целевой мерой отказа. Данные меры должны соответствовать требованиям настоящего стандарта.

Примечание — Цель настоящего подпункта состоит в выявлении видов отказов из-за формирования запроса(ов) к какому-либо средству управления риском. Возможны ситуации, когда интенсивность отказов для выявленных видов отказов не может быть снижена. В данном случае требуется сформировать новую функцию безопасности, либо УПБ других функций безопасности должны быть пересмотрены с учетом интенсивности отказов.

8.3.2.13 Для всех компонентов АС должно быть учтено снижение параметров относительно предельных значений. Обоснование работы любых компонентов АС при предельных значениях их параметров должно быть документально оформлено (см. ГОСТ 34332.2—2017, раздел 5).

Примечание — При назначении снижения параметров коэффициент снижения, как правило, устанавливают приблизительно равным двум третям.

8.3.2.14 Если в проекте на Э/Э/ПЭ СБЗС систему для реализации функции безопасности предусмотрено применение одной или более подсистем или СИС, то должен быть применен подход с использованием V-образной модели для этапов ЖЦ проектирования и реализации (см. 8.1.3.3).

8.3.3 Составляющие систем для обеспечения требуемой стойкости к систематическим отказам

8.3.3.1 Для удовлетворения требований стойкости к систематическим отказам создаваемая Э/Э/ПЭ СБЗС система при условиях, описанных в настоящем пункте, может быть разделена на элементы, обладающие различной стойкостью к таким отказам.

Примечания

1 Стойкость к систематическим отказам элемента определяется способностью функции безопасности противостоять отказу при отказе этого элемента. Концепция стойкости к систематическим отказам элемента применима к элементам как АС, так и ПО.

2 В ГОСТ 34332.2—2017 (пункт 7.6.10) указаны условия независимости СБЗС систем и прочих средств уменьшения риска. Эти условия могут быть применены при более детальном проектировании, и некоторая структура элементов, реализующая функцию безопасности, возможно, позволит достичь лучшей стойкости к систематическим отказам, чем ее отдельные элементы.

8.3.3.2 Если систематический сбой элемента со стойкостью к систематическим отказам ССО *N* (*N* = 1,2,3) не вызывает отказ указанной функции безопасности, но вызывает ее отказ только в сочетании со вторым систематическим отказом другого элемента со стойкостью к систематическим отказам ССО *N,* то результирующая стойкость к систематическим отказам комбинации этих двух элементов может рассматриваться как ССО (*N* + 1) при условии, что эти два элемента достаточно независимы (см. 8.3.3.4).

Примечание — Независимость элементов может быть оценена, только если известны конкретные применения этих элементов для оговоренных функций безопасности.

8.3.3.3 Стойкость к систематическим отказам, которая может быть предъявлена к комбинации элементов со стойкостью к систематическим отказам каждого из них, равной ССО *N,* в лучшем случае может быть равна ССО (*N* + 1). Элемент со стойкостью к систематическим отказам, равной ССО *N,* может быть использован таким способом только один раз. Для получения ССО (*N* + 2) и выше не допускается строить последовательные комбинации из элементов с ССО *N.*

8.3.3.4 Для обоснования достаточной независимости между элементами при проектировании и между элементами в их конкретном применении следует применять анализ отказов по общей причине, чтобы показать, что вероятность возникновения взаимных помех между самими элементами и между элементами и окружением является незначительной по сравнению с УПБ рассматриваемой функции безопасности.

Примечания

1 При определении стойкости к систематическим отказам в процессе проектирования, реализации, эксплуатации и технического обслуживания АС возможно использование следующих подходов для достижения достаточной независимости:

- функциональное разнообразие — использование различных подходов для достижения тех же результатов;
- разнообразие технологий — использование различных типов оборудования для достижения одних и тех же результатов;
- общие компоненты/процедуры обслуживания — обеспечение отсутствия общих компонентов или процедур обслуживания либо систем поддержки (например, электропитания), отказ которых может привести к опасному виду отказа всех систем;
- общие процедуры — обеспечение отсутствия общих процедур при эксплуатации, техническом обслуживании или тестировании.

2 Независимость применения означает, что элементы не повлияют друг на друга настолько неблагоприятно, чтобы это могло привести к опасному отказу.

8.3.4 Архитектурные ограничения полноты безопасности АС

Примечание — Выражение, связывающее ограничения полноты безопасности АС, определено в приложении В, а сами ограничения полноты безопасности представлены в таблицах 2 и 3.

8.3.4.1 Наиболее высокий УПБ АС, который может потребоваться для функции безопасности, ограничен предельными значениями полноты безопасности АС, которые могут быть достигнуты одним из двух возможных способов (реализуемых на уровне системы или подсистемы):

- способ 1_{AC} основан на концепции отказоустойчивости АС и концепции составляющей безопасных отказов;
- способ 2_{AC} основан на полученных данных о безотказности компонентов, об их использовании конечными пользователями, повышающих уровни доверия и отказоустойчивость АС для указанных УПБ.

Стандарты для прикладных областей[1)] могут содержать указание на предпочтительный способ (т. е. способ 1_{AC} или способ 2_{AC}).

[1)] Стандарты, основанные на [4].

Примечание — Индекс «$_{AC}$» в вышеупомянутых способах означает полноту безопасности АС в отличие от способов 1_C, 2_C и 3_C для систематической полноты безопасности.

8.3.4.2 При формировании требований к обеспечению отказоустойчивости АС следует учитывать, что:

а) отказоустойчивость АС *N* означает, что *N* + 1 является минимальным числом отказов, которые могут привести к потере функции безопасности (дополнительные разъяснения приведены в примечании 1 и таблицах 2 и 3). В определении отказоустойчивости не должны учитываться средства, которые могли бы контролировать последствия ошибок, например диагностика;

б) если одна ошибка непосредственно приводит к одной или более последующим ошибкам, их рассматривают как одиночную ошибку;

в) при определении отказоустойчивости некоторые ошибки могут быть исключены при условии, что вероятность их возникновения очень мала по сравнению с требованиями полноты безопасности подсистемы. Любые исключения ошибок должны быть обоснованы и документально оформлены (см. примечание 3).

Примечания

1 Для получения достаточно отказоустойчивой архитектуры с учетом уровня сложности элемента и подсистемы используют ограничения на полноту безопасности АС (см. 8.3.4.1 и 8.3.4.2). Самым высоким допустимым УПБ для функции безопасности, реализуемой Э/Э/ПЭ СБЗС системой, полученным в результате применения требований, указанных в настоящем подпункте, является максимальный уровень из заявленных для функции безопасности, однако в некоторых случаях расчеты надежности показывают, что может быть достигнут более высокий УПБ. Следует также отметить, что если отказоустойчивость АС достигнута для всех подсистем, необходимо выполнить расчет надежности, чтобы продемонстрировать, что заданная целевая мера отказов достигнута, так как для выполнения требований проекта может потребоваться, чтобы отказоустойчивость АС была увеличена.

2 Требования отказоустойчивости АС применяют к архитектуре подсистемы, используемой при нормальных условиях эксплуатации. Требования отказоустойчивости к АС могут быть снижены, если Э/Э/ПЭ СБЗС система восстанавливается автономно. Однако ключевые параметры, связанные с любым снижением требований, должны быть предварительно оценены (например, оценка среднего времени восстановления по отношению к вероятности запроса).

3 Некоторые ошибки могут быть исключены, так как если некоторый элемент системы имеет очень низкую вероятность отказа благодаря соответствующим ему свойствам и конструкции (например, механический соединитель привода), то нет необходимости рассматривать ограничение (связанное с отказоустойчивостью АС) полноты безопасности любой функции безопасности, для реализации которой используется этот элемент.

4 Выбор дальнейших шагов зависит от области применения, и для выбора способа необходимо учитывать:

- что безопасный отказ одной функции может создать новую опасность или стать дополнительной причиной для существующей опасности;
- резервирование не может быть реализовано для всех функций;
- ремонт не всегда возможен или быстро осуществим (например, не представляется возможным его провести за период времени, который существенно меньше интервала времени между тестовыми испытаниями);

5 Специальные требования к архитектуре СИС с избыточностью схем на кристалле приведены в [4].

6 При проектировании Э/Э/ПЭ СБЗС систем СИС не проектируют и не создают, их приобретают в качестве покупных изделий (как продукцию промышленного производства, см. 3.18). Однако для выбора СИС или модулей, содержащих СИС, пригодных для применения в конкретной СБЗС системе, проектировщик должен знать о свойствах приобретаемых СИС или модулей с СИС. Разработчики и производители СИС или модулей, содержащих СИС, должны быть ознакомлены с требованиями к тем СИС, которые могут быть использованы при создании СБЗС систем. Для удовлетворения потребностей в информации пользователей стандартов комплекса ГОСТ 34332 информация о требованиях к СИС для Э/Э/ПЭ СБЗС систем включена в настоящий стандарт и другие стандарты комплекса ГОСТ 34332.

8.3.4.3 Элемент может быть отнесен к типу А, если для его компонентов, необходимых для реализации функции безопасности, одновременно выполняются следующие условия:

- виды отказов всех составляющих компонентов определены;
- поведение элемента в условиях отказа может быть полностью определено;
- данные о претензиях по поводу интенсивности отказов для обнаруженных и необнаруженных опасных отказов недостаточно надежны (см. 8.3.13.3—8.3.13.5).

Элемент может быть отнесен к типу Б, если для его компонентов, необходимых для реализации функции безопасности, выполняется хотя бы одно из следующих условий:

- вид отказа по крайней мере одного составляющего компонента не определен;
- поведение подсистемы в условиях отказа не может быть полностью определено;

- данные о претензиях по поводу интенсивности отказов для обнаруженных и необнаруженных опасных отказов недостаточно надежны (см. 8.3.13.3—8.3.13.5).

Примечание — Если по крайней мере один из компонентов конкретного элемента соответствует условиям для типа Б, то такой элемент должен быть отнесен к типу Б, а не к типу А.

8.3.4.4 При оценке доли безопасных отказов элемента, предназначенного для использования в подсистеме с отказоустойчивостью АС, равной нулю, которая выполняет функцию безопасности или часть функции безопасности, действующей в режиме высокой частоты запросов или с непрерывными запросами, предпочтение должно быть отдано только диагностике, если:

- суммарное время диагностического испытательного интервала и времени выполнения определенного действия для достижения или поддержания безопасного состояния было меньше времени безопасности процесса;

- при работе в режиме с высокой частотой запросов отношение частоты диагностических испытаний к частоте запросов равно или превышает 100.

8.3.4.5 При оценке доли безопасных отказов элемента, который имеет отказоустойчивость АС более нуля и который выполняет функцию безопасности или часть функции безопасности, действуя в режиме с высокой частотой запросов или с непрерывным запросом, или выполняет функцию безопасности или часть функции безопасности, работая в режиме с низкой частотой запросов, предпочтение должно быть отдано только диагностике, если:

- суммарное время диагностического испытательного интервала и время выполнения ремонта обнаруженного отказа будет менее среднего времени восстановления, используемого в вычислениях при определении достигаемой полноты безопасности для этой функции безопасности;

- при работе в режиме с высокой частотой запросов отношение частоты диагностических испытаний к частоте запросов равно или превышает 100.

8.3.4.6 При оценке доли безопасных отказов элемента, который имеет отказоустойчивость АС более нуля и который выполняет функцию безопасности или часть функции безопасности, действуя в режиме с высокой частотой запросов или с непрерывным запросом, или выполняет функцию безопасности или часть функции безопасности, работая в режиме с низкой частотой запросов, доверие (предпочтение) должно быть отдано только диагностике, если суммарное время диагностического испытательного интервала и время выполнения ремонта обнаруженного отказа будет менее среднего времени восстановления, используемого в вычислениях при определении достигаемой полноты безопасности для этой функции безопасности.

8.3.5 Способы определения максимального УПБ АС

8.3.5.1 Для определения максимального УПБ АС, который может быть предъявлен к функции безопасности по способу $1_{АС}$, необходимо выполнить следующие процедуры:

а) определить подсистемы, из которых состоит Э/Э/ПЭ СБЗС система;

б) для всех элементов каждой подсистемы отдельно определить долю безопасных отказов (индивидуально для каждого элемента, имеющего отказоустойчивость АС, равную нулю). Для конфигураций элементов с резервированием доля безопасных отказов может быть вычислена с учетом дополнительной диагностики, которая может быть доступна (например, сравнением резервированных элементов);

в) для каждого элемента, используя полученное значение доли безопасных отказов и значение отказоустойчивости АС, равное нулю, определяют максимальный УПБ из второй колонки таблицы 2 (для элементов типа А) и второй колонки таблицы 3 (для элементов типа Б);

г) используя метод, представленный в 8.3.5.3 и 8.3.5.4, определить максимальный УПБ, который может быть предъявлен к подсистеме;

д) максимальный УПБ, который может быть предъявлен к Э/Э/ПЭ СБЗС системе, определить как УПБ подсистемы с самым низким УПБ.

8.3.5.2 Для подсистем, включающих в себя элементы, отвечающие представленным ниже требованиям, в качестве альтернативы применению требований, указанных в перечислениях б) — г) 8.3.5.1 для случаев, когда подсистема состоит из более чем одного элемента и элементы являются однотипными, все элементы имеют значения доли безопасных отказов, находящиеся в одном диапазоне (см. примечание), определенном в таблицах 2 или 3, применяют следующие процедуры определения максимального УПБ:

а) определяют долю безопасных отказов для всех отдельных элементов. В случае конфигураций элементов с резервированием доля безопасных отказов может быть вычислена с учетом доступной дополнительной диагностики (например, сравнение резервированных элементов);

б) определяют отказоустойчивость АС подсистемы;

в) определяют по таблице 2 максимальный УПБ, на который может претендовать подсистема, если ее элементы типа А;

г) определяют по таблице 3 максимальный УПБ, на который может претендовать подсистема, если ее элементы типа Б.

Примечание — В таблицах 2 и 3 значения доли безопасных отказов разделены на четыре диапазона (менее 60 %; от 60 % до 90 %; от 90 % до 99 % и более 99 %). Все значения доли безопасных отказов должны быть в одном диапазоне (например, все в диапазоне от 90 % до 99 %).

Примеры

1 Для определения максимального допустимого УПБ, который для указанной функции безопасности может быть достигнут подсистемой, имеющей отказоустойчивость АС, равную 1, для которой функция безопасности элемента реализована с помощью параллельных элементов, может быть принят следующий подход при условии, что подсистема соответствует требованиям, приведенным в 8.3.5.2. В этом примере все элементы относятся к типу Б, а значения доли безопасных отказов элементов находятся в диапазоне от 90 % до 99 %.

Из таблицы 3 следует, что для отказоустойчивости АС, равной 1, и для значений доли безопасных отказов элементов, находящихся в диапазоне от 90 % до 99 %, максимальный допустимый УПБ для указанной функции безопасности УПБ 3.

2 Для определения необходимой отказоустойчивости АС подсистемы для указанной функции безопасности, в которой функция безопасности элемента реализована с помощью параллельных элементов, может быть принят следующий подход, при условии, что подсистема соответствует требованиям, указанным в 8.3.5.2. В настоящем примере все элементы имеют тип А, а значения доли безопасных отказов элементов находятся в диапазоне от 60 % до 90 %. Уровень полноты безопасности функции безопасности УБП 3.

Из таблицы 2 следует, что требованию УПБ 3 соответствует необходимая отказоустойчивость АС, равная 1. Это означает, что необходимы два параллельных элемента.

Таблица 2 — Зависимость полноты безопасности АС Э/Э/ПЭ СБЗС подсистем типа А от устойчивости АС к отказам и доли безопасных отказов

Доля безопасных отказов, %	УПБ в зависимости от устойчивости АС к отказам (см. примечание 1)		
	$N = 0$	$N = 1$	$N = 2$
До 60	УПБ 1	УПБ 2	УПБ 3
От 60 до 90	УПБ 2	УПБ 3	УПБ 4
От 90 до 99	УПБ 3	УПБ 4	УПБ 4
Более 99	УПБ 3	УПБ 4	УПБ 4

Примечания

1 Требования, приведенные в настоящей таблице, совместно с требованиями, приведенными в 8.3.5.1 и 8.3.5.2, применяют для определения максимального значения УПБ, который может быть предъявлен к подсистеме: задают отказоустойчивость подсистемы и долю безопасных отказов используемых элементов:

- для общего применения к любой подсистеме представлены в 8.3.5.1;
- для применения к подсистемам, включающим в себя элементы, отвечающие требованиям, указанным в 8.3.5.2. Для того, чтобы утверждать, что подсистема соответствует указанному УПБ непосредственно по данной таблице, необходимо, чтобы для нее были выполнены все требования, указанные в 8.3.5.2.

2 Требования, приведенные в настоящей таблице, совместно с требованиями, приведенными в 8.3.5.1 и 8.3.5.2, применяют для определения:

- требований отказоустойчивости АС подсистемы, задавая необходимый УПБ функции безопасности и долю безопасных отказов используемых элементов;
- требований к значению доли безопасных отказов элементов, задавая необходимый УПБ функции безопасности и отказоустойчивость АС подсистемы.

3 Требования, указанные в 8.3.5.3 и 8.3.5.4, основаны на данных, определенных в настоящей таблице и таблице 4.

4 Расчет доли безопасных отказов представлен в приложении В.

Таблица 3 — Зависимость полноты безопасности АС СБЗС подсистем типа Б от устойчивости АС к отказам и доли безопасных отказов

Доля безопасных отказов, %	Уровень полноты безопасности в зависимости от устойчивости АС к отказам (см. примечание 1)		
	$N = 0$	$N = 1$	$N = 2$
Менее 60	Не оговаривается	УПБ 1	УПБ 2
От 60 до 90	УПБ 1	УПБ 2	УПБ 3
От 90 до 99	УПБ 2	УПБ 3	УПБ 4
Более 99	УПБ 2	УПБ 4	УПБ 4

Примечания

1 Требования, приведенные в настоящей таблице, совместно с требованиями, приведенными в 8.3.5.1 и 8.3.5.2, применяют для определения максимального значения УПБ, который может быть предъявлен к подсистеме: задаются отказоустойчивость подсистемы и доля безопасных отказов используемых элементов:

- для общего применения к любой подсистеме представлены в 8.3.5.1;
- для применения к подсистемам, включающим в себя элементы, отвечающие требованиям 8.3.5.2. Для того чтобы утверждать, что подсистема соответствует указанному УПБ непосредственно из данной таблицы, необходимо, чтобы для нее были выполнены все требования, указанные в 8.3.5.2.

2 Требования, приведенные в настоящей таблице, совместно с требованиями, приведенными в 8.3.5.1 и 8.3.5.2, применяют для определения:

- требований отказоустойчивости АС подсистемы, задавая необходимый УПБ функции безопасности и долю безопасных отказов используемых элементов;
- требований к значению доли безопасных отказов элементов, задавая необходимый УПБ функции безопасности и отказоустойчивость АС подсистемы.

3 Требования, указанные в 8.3.5.3 и 8.3.5.4, основаны на данных, определенных в настоящей таблице и таблице 3.

4 Расчет доли безопасных отказов см. в приложении В.

5 Если используют требования, указанные в 8.3.5.1, для комбинации элементов типа Б, с отказоустойчивостью АС, равной 1, в которой у обоих элементов доля безопасных отказов менее 60 %, то максимальным допустимым УПБ для функции безопасности, выполняемой этой комбинацией, является УБП 1.

8.3.5.3 В Э/Э/ПЭ СБЗС подсистеме, в которой некоторое число элементов функций безопасности реализуется с помощью последовательности элементов (как показано на рисунке 7), максимальный УПБ, который может быть предъявлен к функции безопасности, должен определяться элементом, который имеет самый низкий УПБ для достигнутой им доли безопасных отказов и отказоустойчивости АС, равной 0. Иллюстрация данного метода для архитектуры, представленной на рисунке 6, приведена на примере ниже.

Пример — Пусть архитектура (рисунок 7), где некоторое число элементов функций безопасности реализуется подсистемой, выполненной по одноканальной архитектуре, состоящей из элементов 1, 2 и 3, которые соответствуют требованиям таблиц 2 и 3 следующим образом:

- для элемента 1 УПБ, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 1;

- для элемента 2 УПБ, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 2;

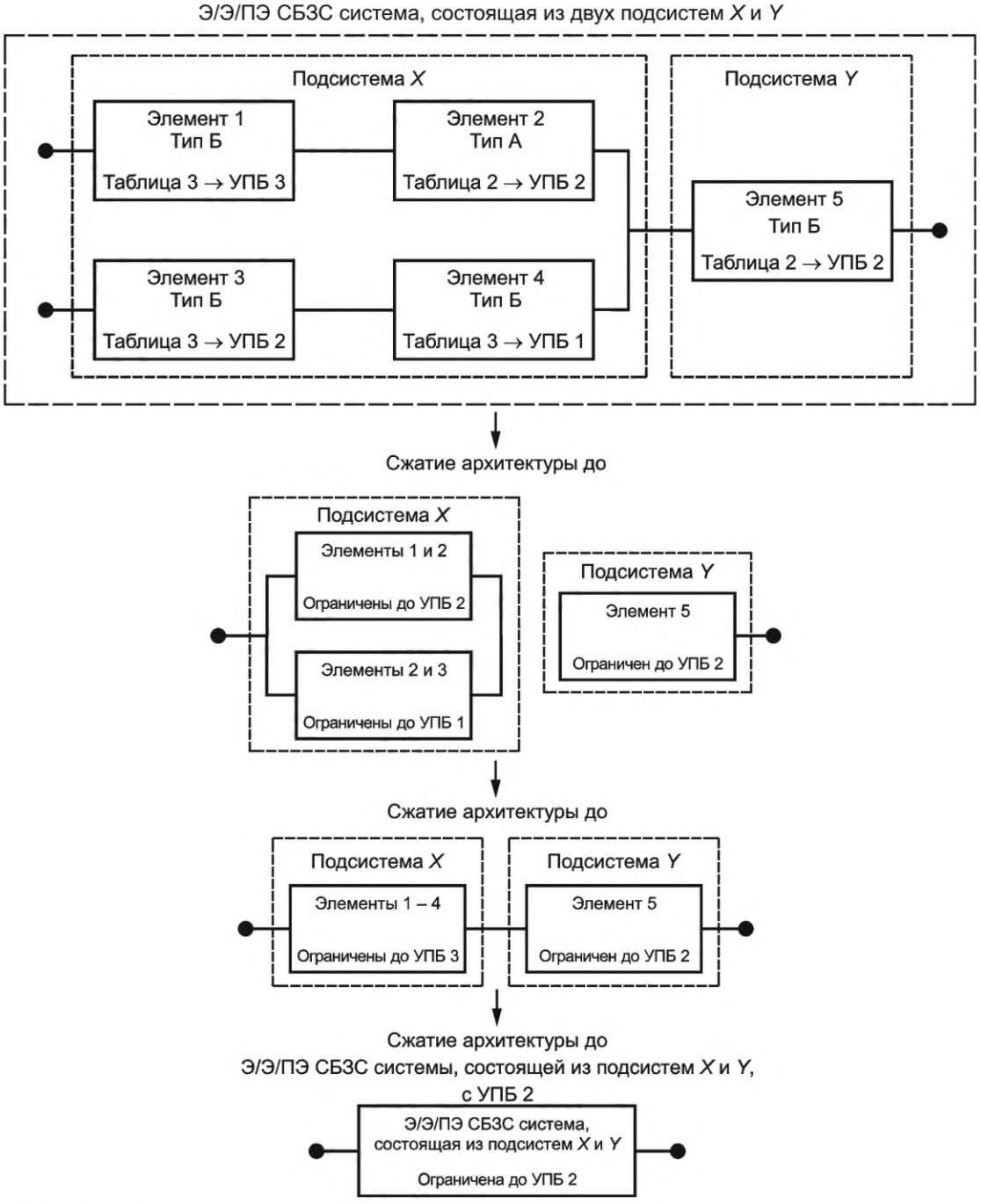
- для элемента 3 УПБ, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 1.



Рисунок 7 — Порядок определения максимального значения УПБ для заданной архитектуры (Э/Э/ПЭ СБЗС подсистема, состоящая из последовательности элементов, см. 8.3.5.3)

Элементы 1 и 3 ограничивают максимальный УПБ, который может потребоваться для соответствия отказоустойчивости АС доле безопасных отказов, до УПБ 1.

8.3.5.4 В Э/Э/ПЭ СБЗС подсистеме, в которой функция безопасности реализуется в многоканальной архитектуре с параллельным соединением элементов (рисунок 8) с отказоустойчивостью АС, равной *N,* максимальный УПБ, который может быть достигнут для рассматриваемой функции безопасности, должен быть определен:



Примечания

1 Элементы 1 и 2 реализуют требуемую часть функции безопасности подсистемы *X* независимо от элементов 3 и 4 и наоборот.

2 Подсистемы, выполняющие функцию безопасности, считают полной Э/Э/ПЭ системой, включая все элементы от сенсоров до исполнительных устройств

Рисунок 8 — Порядок определения максимального УПБ для заданной архитектуры [Э/Э/ПЭ СБЗС система, состоящая из двух подсистем *X* и *Y* (см. 8.3.5.4)]

- группированием последовательно соединенных элементов для каждого канала и затем определением максимального УПБ, который может быть достигнут для рассматриваемой функции безопасности для каждого канала (см. 8.3.5.3);

- выбором цепи с самым высоким УПБ, который может быть достигнут для рассматриваемой функции безопасности, и затем сложением УПБ *N* для определения максимальной полноты безопасности для полной подсистемы.

Примечания

1 *N* — отказоустойчивость АС комбинации параллельных элементов (см. 8.3.5.1).

2 В примере рассматривается применение настоящего подпункта.

Пример реализации метода для архитектуры, приведенной на рисунке 8, представлен ниже.

Пример

Группирование и анализ этих комбинаций могут быть проведены разными методами. Для иллюстрации одного из возможных методов принимают архитектуру, в которой конкретная функция безопасности реализована двумя подсистемами X и У, где подсистема X состоит из элементов 1—4, а подсистема У из одного элемента 5, как показано на рисунке 8. Использование параллельных каналов в подсистеме X гарантирует, что элементы 1 и 2 реализуют требуемую часть функции безопасности подсистемы X независимо от элементов 3 и 4 и наоборот. Функцию безопасности считают выполненной:

- при событии отказа в элементе 1 или 2 (поскольку комбинация элементов 3 и 4 позволяет реализовать требуемую часть функции безопасности);

- при событии отказа в элементе 3 или 4 (поскольку комбинация подсистем 1и 2 позволяет реализовать требуемую часть функции безопасности).

Далее подробно рассматривают процедуру определения максимального УПБ, который может потребоваться для рассматриваемой функции безопасности.

В подсистеме X при заданной функции безопасности каждый элемент соответствует требованиям, указанным в таблицах 2 и 3, следующим образом:

- для элемента 1 УПБ, соответствующий требованиям отказоустойчивости АС, равной 0, и доле безопасных отказов, равен УПБ 3;

- для элемента 2 УПБ, соответствующий требованиям отказоустойчивости АС, равной 0, и доле безопасных отказов, равен УПБ 2;

- для элемента 3 УПБ, соответствующий требованиям отказоустойчивости АС, равной 0, и доле безопасных отказов, равен УПБ 2;

- для элемента 4 УПБ, соответствующий требованиям отказоустойчивости АС, равной 0, и доле безопасных отказов, равен УПБ 1.

Для того чтобы получить максимальный УПБ АС для рассматриваемой функции безопасности, элементы подсистемы X объединяют следующим образом:

- объединение элементов 1 и 2. Отказоустойчивость АС и доля безопасных отказов, обеспеченная комбинацией элементов 1 и 2 (каждая в отдельности соответствует требованиям для УПБ 3 и УПБ 2 соответственно), соответствует требованиям УПБ 2 (определенным элементом 2, см. 8.3.5.3);

- объединение элементов 3 и 4. Отказоустойчивость АС и доля безопасных отказов, обеспеченная комбинацией элементов 3 и 4 (каждая в отдельности соответствует требованиям для УПБ 2 и УПБ 1 соответственно), соответствует требованиям УПБ 1(определенным элементом 5, см. 8.3.5.3);

- дальнейшее объединение комбинации элементов 1 и 2 с комбинацией элементов 3 и 4. Максимальный УПБ АС, который может быть достигнут для рассматриваемой функции безопасности, определяется выбором канала с самым высоким УПБ, который был достигнут, и затем сложением УПБ N для определения максимального УПБ для всей комбинации элементов. В данном случае подсистема включает в себя два параллельных канала с отказоустойчивостью АС, равной 1. Каналом с самым высоким УПБ для рассматриваемой функции безопасности является канал, включающий в себя элементы 1 и 2 и соответствующий требованиям для УПБ 2. Поэтому максимальный УПБ для подсистемы при отказоустойчивости АС, равной 1, будет УПБ 2 + 1 = УПБ 3 (см. 8.3.5.4).

В подсистеме У для элемента 5 УПБ, соответствующий требованиям отказоустойчивости АС, равной 0, и доле безопасных отказов, равен УПБ 2.

Для полной Э/Э/ПЭ СБЗС системы (включающей в себя две подсистемы X и У, которые достигли требований для рассматриваемой функции безопасности УПБ 3 и УПБ 2 соответственно) максимальный УПБ, который может быть достигнут для Э/Э/ПЭ СБЗС системы, определен подсистемой, которая достигла самого низкого УПБ [см. перечисление а) 8.3.5.1]. Поэтому для настоящего примера максимальным УПБ, который может быть достигнут для Э/Э/ПЭ СБЗС системы, для рассматриваемой функции безопасности является УПБ 2.

8.3.5.5 Минимальное значение отказоустойчивости АС для каждой подсистемы Э/Э/ПЭ СБЗС системы, выполняющей функцию безопасности с заданным УПБ, в случае применения способа 2_{AC} определяют следующим образом:

- значение отказоустойчивости АС равно 2 для заданной функции безопасности с УПБ 4, если не применяются условия по 8.3.5.6;
- значение отказоустойчивости АС равно 1 для заданной функции безопасности с УПБ 3, если не применяются условия по 8.3.5.6;
- значение отказоустойчивости АС равно 1 для заданной функции безопасности с УПБ 2, если не применяются условия по 8.3.5.6;
- значение отказоустойчивости АС равно 0 для заданной функции безопасности с УПБ 2, работающей в режиме с низкой частотой запросов;
- значение отказоустойчивости АС равно 0 для заданной функции безопасности с УПБ 1.

Примечание — Для перечислений, приведенных в настоящем подразделе, если не указано иное, считается, что функция безопасности может выполняться либо в режиме с низкой частотой запросов, либо в режиме с высокой частотой запросов или с непрерывным запросом.

8.3.5.6 Если установлено, только для элементов типа А, что, следуя требованиям отказоустойчивости АС, указанным в 8.3.5.5, для конкретной ситуации требуется значение отказоустойчивости АС более 0 и это приводит к дополнительным отказам и уменьшению полной безопасности УО, то может быть реализована более безопасная альтернативная архитектура с уменьшенным значением отказоустойчивости АС. В таком случае решение должно быть обосновано и документально оформлено. Обоснование должно представить свидетельства о том, что:

- соответствие с требованиями отказоустойчивости АС, определенными в 8.3.5.5, приведет к дополнительным отказам, уменьшению полной безопасности УО;
- если значение отказоустойчивости АС уменьшено до нуля, то режимы отказа, идентифицированные в элементе, выполняющем функцию безопасности, могут не учитываться, потому что интенсивность(и) опасных отказов идентифицированного(ых) режима(ов) отказа очень низка(и) по сравнению с целевой мерой отказов для рассматриваемой функции безопасности [см. перечисление в) 8.3.4.2]. То есть сумма интенсивностей опасных отказов всех последовательно соединенных элементов, для которых требуется исключение ошибки, не должна превышать 1 % целевой меры отказа. Более того, такое использование исключений ошибки должно быть обосновано с учетом возможности систематических ошибок.

Примечание — Отказоустойчивость — наиболее оптимальный путь для достижения робастной архитектуры. Если применяют требования настоящего подпункта, то цель обоснования состоит в том, чтобы продемонстрировать, что предложенная альтернативная архитектура обеспечивает эквивалентное или лучшее решение. Реализация такого решения может зависеть от технической сферы и/или применения. Например, применяют: механизмы резервирования (аналитическая избыточность, замена выхода неисправного датчика, выполненная физическим вычислением выходных результатов других датчиков); использование более надежных положений той же самой технологии (при их наличии); изменения для увеличения надежности технологии; сокращение влияния отказов по общей причине при использовании разных технологий; расширение области проектирования; ограничение условий окружающей среды (например, для электронных компонентов); снижение неопределенности данных о надежности, накапливая данные в процессе эксплуатации или оценки экспертов.

8.3.5.7 Если выбран способ 2_{AC} и данные о надежности, используемые для определения количественного значения случайных отказов АС (см. 8.3.6), то для оценки среднего уровня неопределенности [например, 90 % доверительного интервала или распределения вероятности (см. примечание)] каждого параметра надежности (например, частоты отказов), используемого в расчетах, должны быть:

а) основаны на данных об эксплуатации элементов в аналогичном применении и в подобных условиях окружающей среды;

б) основаны на данных, собранных в соответствии со стандартами по сбору данных на основе полевых испытаний и/или на основе данных при техническом обслуживании систем;

в) оценены в соответствии с количеством данных об эксплуатации и с результатами экспертной оценки, и, при необходимости, с результатами проведенных специальных тестов.

Примечание — Девяностопроцентный доверительный интервал интенсивности отказов λ — это интервал (λ_5 %, λ_{95} %), в котором ее фактические значения должны принадлежать с вероятностью 90 %. λ принимает значения с вероятностью λ_5 % лучше, чем λ_5 %, и хуже, чем λ_{95} %. Чисто статистически среднее значение интенсивности отказов может быть оценено при использовании «оценки максимальной вероятности», а доверительные

границы λ_5 % и λ_{95} % могут быть выражены с помощью функции χ^2. Точность зависит от общего времени наблюдения и числа наблюдаемых отказов. Для обработки статистических наблюдений, экспертных оценок и конкретных результатов испытаний может быть использован Байесовский подход. Эти данные могут быть использованы для формирования соответствующих функций распределения вероятностей для дальнейшего использования в методе моделирования Монте-Карло.

Если выбран способ 2_{AC}, то необходимо учесть неопределенность данных о надежности при вычислении целевой меры отказов (то есть средняя вероятность отказов по запросам или частота отказов в час), и систему следует дорабатывать до тех пор, пока не будет достигнута на 90 % целевая мера отказов.

8.3.5.8 Если выбран способ 2_{AC}, то все элементы типа Б должны быть, как минимум, охвачены диагностикой не менее 60 %.

8.3.6 Требования к количественной оценке случайных отказов АС

8.3.6.1 Для каждой функции безопасности полнота безопасности, достигнутая Э/Э/ПЭ СБЗС системой из-за случайных отказов АС (включая ошибки программ), и в коммуникационных процессах должна быть оценена по 8.3.6.2 и 8.3.15 и должна быть равна или быть менее целевой меры отказов, определенной в спецификации требований к безопасности этой системы (см. ГОСТ Р 34332.2—2017, подраздел 7.10).

Примечание — Чтобы продемонстрировать, что это было достигнуто, необходимо выполнить прогноз надежности для соответствующей функции безопасности с использованием соответствующей методики (см. 8.3.6.2) и сравнить результат с целевым показателем отказа соответствующей функции безопасности (см. ГОСТ 34332.2).

8.3.6.2 При оценке достигнутой меры отказов каждой функции безопасности в соответствии с требованиями, указанными в 8.3.6.1, следует учитывать:

- архитектуру Э/Э/ПЭ СБЗС системы в терминах ее подсистем, поскольку это касается каждой рассматриваемой функции безопасности.

Примечание — Необходимо определить, какие виды отказов элементов подсистем находятся в последовательной связи (любой отказ вызывает отказ соответствующей функции безопасности, которая должна выполняться), а какие виды отказов находятся в параллельной связи (для сбоя соответствующей функции безопасности необходимы совпадающие отказы);

- архитектуру каждой Э/Э/ПЭ СБЗС подсистемы в терминах ее элементов, поскольку это касается каждой рассматриваемой функции безопасности;

- оцененную интенсивность отказов каждой подсистемы и ее элементов в любых режимах, которые могли бы вызвать опасный отказ (см. 8.3.13.3 и 8.3.13.4). Должно быть приведено обоснование интенсивности отказов с учетом источника данных и его точности или допустимого отклонения. Обоснование может включать в себя рассмотрение и сравнение данных из многих источников, а также объяснение выбора интенсивностей отказов систем, наиболее близко напоминающих рассматриваемую систему. Интенсивность отказов, используемая для количественной оценки случайных отказов АС и вычисления доли безопасных отказов или охвата диагностикой, должна учитывать указанные условия эксплуатации.

Примечание — Для выбора интенсивности отказов из баз данных, как правило, бывает необходимо учесть условия эксплуатации, связанные, например, с нагрузкой или температурой;

- восприимчивость Э/Э/ПЭ СБЗС системы и ее подсистем к отказам по общей причине (см. примечания 1 и 2). Сделанные предположения должны быть обоснованы.

Примечания

1 Отказы из-за влияния общей причины могут быть результатом других влияний, отличных от реальных отказов компонентов АС (например, электромагнитные помехи, ошибки декодирования и т. п.). Однако такие отказы рассматриваются в настоящем стандарте как оцениваемые количественно случайные отказы АС. Тестирование в шахматном порядке приводит к уменьшению отказов по общей причине.

2 Если отказы по общей причине, идентифицируемые между Э/Э/ПЭ СБЗС системами, формируют запрос к ним или к другим уровням защиты, то должно быть подтверждение того, что отказы по общей причине были учтены при определении требований к УПБ и целевой мере отказов;

- охват диагностическими тестами (по приложению В) и связанные с ним диагностический испытательный интервал и интенсивность не обнаруженных диагностикой опасных отказов для случайных отказов АС каждой подсистемы. В соответствующих случаях необходимо рассматривать только те диа-

гностические тесты, которые соответствуют требованиям, указанным в 8.3.6.3. В модели надежности необходимо учесть и среднюю вероятность отказов по запросам, и частоту отказов в час.

Примечание — При установлении времени диагностического испытательного интервала должны быть рассмотрены интервалы между всеми испытаниями, которые вносят вклад в охват диагностикой;

- интервалы времени, на которых реализуются контрольные проверки для обнаружения опасных ошибок;
- является ли контрольная проверка эффективной на 100 %.

Примечание — В результате выполнения несовершенной контрольной проверки функция безопасности может не восстановиться до состояния «как новая», и поэтому вероятность отказа увеличится. Для сделанных предположений должно быть дано обоснование; в частности, должны быть включены периоды возобновления работоспособности для элементов или некоторое снижение риска дальнейшего выполнения функции безопасности. Необходимо рассмотреть продолжительность испытания, если элемент будет проверяться автономно;

- время ремонта для обнаруженных отказов.

Примечание — Среднее время ремонта составляет часть среднего времени восстановления, включающего в себя также время обнаружения отказа и период времени, в течение которого ремонт невозможен. Можно полагать, что ремонт происходит мгновенно только тогда, когда УО выключено или находится в безопасном состоянии во время ремонта. Для ситуаций, когда ремонт может быть выполнен в течение конкретного периода времени, например в то время, когда управляемое оборудование отключено или находится в надежном (закрытом) состоянии, важно, чтобы при полном расчете был учтен период времени, когда ремонт не может быть произведен, особенно когда этот период является относительно большим. Все соответствующие факторы, связанные с ремонтом, должны быть учтены;

- влияние случайной ошибки человека, если человек обязан принимать меры для выполнения функции безопасности.

Примечание — Природу случайной ошибки человека необходимо рассмотреть в условиях, когда человек готов к опасному событию и обязан принимать данные меры, тогда вероятность ошибки человека должна быть включена в вычисление полной вероятности;

- тот факт, что доступны многие методы моделирования и что самый подходящий метод выбирает аналитик, и этот выбор зависит от ряда обстоятельств. Доступные методы включают в себя: анализ видов и последствий отказов [см. ГОСТ 34332.5—2021 (Б.6.6.1 приложения Б)], анализ дерева ошибок [см. ГОСТ 34332.5—2021 (Б.6.6.5 приложения Б)], модели Маркова [см. ГОСТ 34332.5—2021 (Б.6.6.6 приложения Б)], структурные схемы надежности [см. ГОСТ 34332.5—2021 (Б.6.6.7 приложения Б)] и сети Петри [см. ГОСТ 34332.5—2021 (Б.6.6.10 приложения Б)].

Примечание — Необходимо отдельно для каждой функции безопасности количественно определять надежность Э/Э/ПЭ СБЗС систем (подсистем), поскольку на нее будут оказывать влияние как разнообразие видов отказов компонентов, так и изменения архитектуры (при использовании избыточности) самих Э/Э/ПЭ СБЗС систем (подсистем);

8.3.6.3 При количественной оценке случайных отказов АС подсистемы со значением отказоустойчивости АС, равным нулю, которая осуществляет функцию безопасности или часть функции безопасности, действующей в режиме высокой частоты запросов или с непрерывными запросами, доверие (предпочтение) должно быть отдано только диагностике, если:

- суммарное время диагностического испытательного интервала и время выполнения определенного действия для достижения или поддержания безопасного состояния меньше времени безопасности процесса;
- при работе в режиме высокой частоты запросов отношение частоты диагностических испытаний к частоте запросов равно или более 100.

8.3.6.4 Диагностический испытательный интервал любой подсистемы, которая:

- имеет значение отказоустойчивости АС более нуля и которая осуществляет функцию безопасности или часть функции безопасности, действуя в режиме высокой частоты запросов или с непрерывными запросами;
- осуществляет функцию безопасности или часть функции безопасности, работая в режиме с низкой частотой запросов, должен быть таким, чтобы суммарное время диагностического испытательного интервала и время выполнения ремонта обнаруженного отказа были менее среднего времени восста-

новления, используемого в вычислении при определении достигаемой полноты безопасности для этой функции безопасности.

8.3.6.5 Если для конкретного проекта требование к полноте безопасности для выполняемой функции безопасности не достигается, то следует:

- определить элементы, подсистемы и/или параметры, вносящие наибольший вклад в формулу расчета интенсивности отказов;
- оценить влияние возможных мер усовершенствования на выявленные критические компоненты, подсистемы или параметры (например, более надежные компоненты, дополнительные меры защиты от отказов по общей причине, расширенный охват диагностикой, расширенная избыточность, уменьшение интервала контрольных испытаний, смещение проверок и т. п.);
- выбрать и осуществить подходящие меры усовершенствования;
- повторить необходимые шаги для вычисления нового значения вероятности случайных отказов АС.

8.3.7 Требования по предотвращению систематических отказов

8.3.7.1 Для предотвращения внесения ошибок во время разработки и создания АС и ПО Э/Э/ПЭ СБЗС системы следует использовать соответствующую группу методов для создания АС и ПО (см. ГОСТ 34332.4—2021, таблица Б.8).

Примечание — Настоящий стандарт не содержит конкретных требований, касающихся предотвращения систематических ошибок во время проектирования серийно выпускаемых ИС, таких как стандартные микропроцессоры, так как вероятность ошибок в таких устройствах минимизирована строгими процедурами разработки, строгим тестированием и обширным опытом использования со значительной информацией от пользователей. Применение ИС, таких как новые устройства или СИС, не может быть таким образом обосновано. Поэтому к СИС, если они должны использоваться в Э/Э/ПЭ СБЗС системе, следует применять требования, представленные в 8.3.7.7 и [4].

8.3.7.2 В соответствии с требуемым УПБ метод проектирования выбирают таким, который обладает возможностями, способствующими:

а) прозрачности, модульности и другим характеристикам, которые управляют сложностью проекта;

б) ясности и точности представления:

1) функциональных возможностей;
2) интерфейсов между подсистемами и элементами;
3) информации, устанавливающей последовательность и время;
4) параллелизма и синхронизации;

в) ясности и точности документирования и передачи информации;

г) проверке и подтверждению соответствия.

8.3.7.3 Требования к техническому обслуживанию для гарантированного поддержания на необходимом уровне требуемой полноты безопасности Э/Э/ПЭ СБЗС систем должны быть формализованы на стадии проектирования.

8.3.7.4 Требования к техническому обслуживанию для гарантированного поддержания на необходимом уровне требуемой полноты безопасности Э/Э/ПЭ СБЗС систем должны быть формализованы на стадии проектирования.

8.3.7.5 В период проектирования должны быть запланированы испытания интеграции Э/Э/ПЭ СБЗС систем. В документацию по планированию испытаний включают:

- типы проводимых испытаний и сопровождающие их процедуры;
- условия окружающей среды при испытаниях, средства испытаний, схему испытаний и программы испытаний;
- критерии оценки «прошла испытание»/«не прошла испытание».

8.3.7.6 В период проектирования действия, выполняемые на рабочем месте проектировщика, должны отличаться от действий, которые должны быть доступными на рабочем месте пользователя.

8.3.7.7 В период проектирования и разработки СИС следует использовать соответствующую группу методов и средств, предназначенных для предотвращения внесения ошибок [4].

8.3.8 Требования по управлению систематическими отказами

8.3.8.1 Для управления систематическими отказами проектирование Э/Э/ПЭ СБЗС системы следует осуществлять таким образом, чтобы обеспечивалась устойчивость Э/Э/ПЭ СБЗС системы:

- к любым остаточным ошибкам проектирования АС, если вероятность ошибок проектирования АС не может быть исключена (см. таблицу А.15 приложения А);

- к внешним влияниям, включая электромагнитные воздействия (см. таблицу А.16 приложения А);
- к ошибкам оператора УО (см. таблицу А.17 приложения А);
- к любым остаточным ошибкам в ПО (см. ГОСТ 34332.4—2021, пункт 7.4.3);
- к любым ошибкам и сбоям, возникающим в результате выполнения любого процесса передачи данных (см. 8.3.9).

8.3.8.2 Для облегчения реализации свойств ремонтопригодности и тестируемости в установленных на объекте Э/Э/ПЭ СБЗС системах эти свойства должны быть учтены в процессе их проектирования и реализации.

8.3.8.3 При проектировании Э/Э/ПЭ СБЗС систем должны быть учтены способности и возможности человека с тем, чтобы реализованные на объекте системы были удобны для работы эксплуатирующего персонала и персонала по техническому обслуживанию систем. При разработке всех интерфейсов следует использовать «положительный опыт» с учетом человеческого фактора и возможного уровня подготовки или осведомленности операторов (например, при использовании Э/Э/ПЭ СБЗС систем массового производства оператором может быть человек, не имеющий специальной подготовки).

Примечания

1 Цель проектирования должна состоять в том, чтобы предсказуемые критические ошибки, допускаемые операторами или персоналом по техническому обслуживанию, предотвращались или устранялись проектными решениями везде, где возможно, либо действия для их выполнения требовали повторного подтверждения.

2 Некоторые ошибки, допускаемые операторами или персоналом по техническому обслуживанию, могут оказаться не восстанавливаемыми Э/Э/ПЭ СБЗС системами, например, если они являются необнаруживаемыми или реально восстанавливаемыми исключительно при непосредственном доступе к системе, например некоторые механические отказы в УО.

8.3.9 Требования к поведению системы при обнаружении отказов[1)]

8.3.9.1 Система должна быть спроектирована таким образом, чтобы при обнаружении опасного отказа (с помощью диагностических тестов, контрольных испытаний или иным методом) в любой подсистеме с отказоустойчивостью АС более нуля действие системы завершалось:

- конкретным действием для достижения или поддержания безопасного состояния (см. примечание);
- изоляцией дефектной части подсистемы для обеспечения возможности продолжения выполнения безопасного действия управляемым оборудованием, пока дефектная часть не будет отремонтирована. Если ремонт не завершен в пределах средней продолжительности ремонта, принятого при вычислении вероятности случайных отказов АС (см. 8.3.6.2), то для достижения и поддержания их безопасного состояния должно быть выполнено конкретное действие (см. примечание).

Примечание — Для достижения и поддержания безопасного состояния, которое должно быть определено в требованиях безопасности Э/Э/ПЭ СБЗС системы, необходимо выполнить конкретное действие (реакцию на отказ). Данное действие может состоять, например, в безопасном отключении УО или той его части, функциональная безопасность которой должна быть реализована дефектной подсистемой.

8.3.9.2 Обнаружение опасного отказа (с помощью диагностических тестов, контрольных испытаний или иным способом) в любой подсистеме с отказоустойчивостью АС, равной нулю, в случае, если такая подсистема используется только для реализации функции(ий) безопасности с низкой частотой запросов, должно завершаться:

- конкретным действием для достижения и поддержания безопасного состояния;
- восстановлением дефектной подсистемы за период времени средней продолжительности ремонта, полученный при расчете вероятности случайных отказов АС (см. 8.3.6.2). В течение этого времени безопасность УО должна обеспечиваться дополнительными мерами и ограничениями. Полнота безопасности, обеспеченная данными мерами и ограничениями, должна, по крайней мере, равняться полноте безопасности, обеспеченной Э/Э/ПЭ СБЗС системой в отсутствие любых отказов. В процедурах эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС системы должны быть определены дополнительные меры и ограничения (см. 8.7).

Примечание — Для достижения и поддержания безопасного состояния, которое должно быть определено в спецификации требований безопасности Э/Э/ПЭ системы, необходимо выполнить конкретное действие

[1)] Требования настоящего пункта относятся к заданным функциям безопасности, выполняемым одиночной Э/Э/ПЭ СБЗС системой, для которой полная функция безопасности не была распределена между ней и прочими средствами уменьшения риска.

(реакцию на отказ). Это действие может состоять, например, в безопасном отключении УО или той его части, функциональная безопасность которой должна быть реализована дефектной подсистемой.

8.3.9.3 Обнаружение опасного отказа (путем диагностического тестирования, контрольных испытаний или иным способом) в любой подсистеме с отказоустойчивостью, равной нулю, в случае подсистемы, выполняющей любую(ые) функцию(и) безопасности, действующей(их) в режиме с высокой частотой запросов или непрерывными запросами для достижения и поддержания безопасного состояния, должно завершаться конкретными действиями (см. примечание).

Примечание — Для достижения и поддержания безопасного состояния, которое должно быть определено в требованиях к безопасности Э/Э/ПЭ СБЗС системы, необходимо выполнить конкретное действие (реакцию на отказ). Это действие может состоять, например, в безопасном отключении УО или той его части, функциональная безопасность которой должна быть реализована дефектной подсистемой.

8.3.10 Разработка рабочей документации

8.3.10.1 Целью разработки рабочей документации является обеспечение должного выполнения действий для реализации последующих стадий ЖЦ Э/Э/ПЭ СБЗС систем и КСБ, а также ЖЦ объекта (см. ГОСТ 34332.2—2017, пункт 7.8.1).

8.3.10.2 При разработке рабочей документации на Э/Э/ПЭ СБЗС системы и КСБ должны быть учтены архитектурные, функционально-технологические, объемно-планировочные, конструктивные и инженерные решения утвержденного в установленном порядке проекта на объект защиты (см. ГОСТ 34332.2—2017, пункт 7.8.2).

8.3.10.3 До реализации (установки, монтажа, пусконаладки) на объекте, интеграции, ввода в действие, подтверждения соответствия Э/Э/ПЭ СБЗС систем (включая КСБ) требованиям настоящего стандарта должны быть разработаны планы проведения этих работ (см. ГОСТ 34332.2—2017, пункт 7.8.3).

8.3.11 Планирование реализации, интеграции и ввода в действие Э/Э/ПЭ СБЗС систем

8.3.11.1 Целью требований настоящего пункта является разработка планов выполнения работ по реализации, интеграции, вводу в действие Э/Э/ПЭ СБЗС систем и КСБ на объекте.

8.3.11.2 Планы по 8.3.11.1 разрабатываются лицами, ответственными за выполнение работ на данных стадиях (с привлечением, в случае возможности, представителей эксплуатирующей организации) и согласовываются с проектной организацией (см. ГОСТ 34332.2—2017, подраздел 7.9).

Примечания

1 Требования, предъявляемые к содержанию плана установки (монтажа) Э/Э/ПЭ СБЗС систем на объекте, установлены в ГОСТ 34332.2—2017 (пункт 7.9.2).

2 Требования к содержанию плана ввода в действие Э/Э/ПЭ СБЗС систем установлены в ГОСТ 34332.2—2017 (пункт 7.9.3).

8.3.12 Планирование подтверждения соответствия Э/Э/ПЭ СБЗС систем

8.3.12.1 Целью требований настоящего пункта являются планирование оценки и подтверждения соответствия Э/Э/ПЭ СБЗС систем.

Примечание — Стадия планирования подтверждения соответствия Э/Э/ПЭ СБЗС систем представлена на рисунке 5 (блок 9).

8.3.12.2 Подтверждению соответствия подлежат АС и ПО промышленного производства, входящие, используемые в качестве комплектующих изделий и средств для реализации Э/Э/ПЭ СБЗС систем. Подтверждение их соответствия осуществляет поставщик этих изделий и средств в форме сертификата соответствия.

8.3.12.3 Подтверждению соответствия подлежат отдельные Э/Э/ПЭ СБЗС системы, а также КСБ, установленные и смонтированные на объекте. Подтверждение их соответствия должен осуществлять застройщик в форме деклараций о соответствии на основании протоколов приемочных испытаний, проводимых приемными комиссиями по приемке систем и объекта.

8.3.12.4 При планировании подтверждения соответствия Э/Э/ПЭ СБЗС системы должны быть использованы:

- требования, определенные в спецификации требований к Э/Э/ПЭ СБЗС системе и в спецификации требований к проектированию Э/Э/ПЭ СБЗС системы;
- набор тестов для интеграции каждой Э/Э/ПЭ СБЗС системы и интеграции Э/Э/ПЭ СБЗС систем в КСБ;
- процедуры, применяемые для подтверждения соответствия полноте безопасности каждой функции безопасности по критериям «прошла испытания»/«не прошла испытания»;

- требуемые условия окружающей среды, при которых проводят испытания, включая необходимые инструменты и оборудование (в том числе план, в соответствии с которым эти инструменты и оборудование должны быть калиброваны);

- процедуры испытаний и критерии, применяемые для подтверждения соответствия заданным в спецификации пределам электромагнитной устойчивости;

- стратегии по устранению подтвержденного отказа.

8.3.12.5 Для КСБ особо опасных, технически сложных и уникальных объектов, а также объектов повышенного уровня ответственности, имеющих важное экономическое, социальное и оборонное значение, в программу испытаний должны быть включены сюжеты (не менее трех), имитирующие неблагоприятное сочетание наиболее опасных событий в их развитии; при этом не менее двух сюжетов должны имитировать действия, осуществляемые при управлении эвакуацией людей из объекта (см. ГОСТ 34332.2—2017, пункт 7.10.2).

8.3.13 Требования к реализации Э/Э/ПЭ СБЗС системы

8.3.13.1 Э/Э/ПЭ СБЗС системы должны быть изготовлены, установлены и смонтированы на объекте в соответствии со спецификацией требований к Э/Э/ПЭ СБЗС системе (см. 8.2.3).

8.3.13.2 Подсистемы и их элементы, используемые для одной или более функций безопасности, должны быть идентифицированы и документально оформлены как подсистемы и элементы, связанные с безопасностью.

Примечание — Поставщик (производитель) подсистемы или элемента промышленного производства, от которых требуется соответствие требованиям настоящего стандарта, должен предоставить эту информацию разработчику Э/Э/ПЭ СБЗС системы (либо другой подсистемы или элемента) в виде соответствующего руководства по безопасности (см. приложение Г).

8.3.13.3 Для каждой Э/Э/ПЭ СБЗС подсистемы должна быть представлена следующая информация (см. также 8.3.13.4):

- функциональная спецификация подсистемы и ее элементов (по мере необходимости);

- все инструкции или ограничения, касающиеся применения подсистемы и ее элементов, которые должны быть соблюдены для предотвращения систематических отказов подсистемы;

- стойкость к систематическим отказам каждого элемента [см. перечисление в) 8.3.5.2];

- определение конфигурации элемента АС и/или ПО, позволяющее управлять конфигурацией Э/Э/ПЭ СБЗС системы в соответствии с ГОСТ 34332.2—2017 (пункт 6.2);

- документально оформленное доказательство того, что подсистема и ее элементы прошли проверку указанных для них функциональных требований и стойкости к систематическим отказам в соответствии со спецификацией требований к проектированию Э/Э/ПЭ СБЗС системы (см. 8.2).

8.3.13.4 Для каждого элемента, связанного с безопасностью, в котором возможны случайные отказы АС, должна быть представлена следующая информация (см. также 8.3.13.3 и 8.3.13.5):

а) виды отказа элемента (в виде описания поведения его выходов) из-за случайных отказов АС, которые приводят к отказу функции безопасности и не выявляются внутренними для элемента диагностическими тестами или не обнаруживаются диагностикой, внешней к элементу (см. 8.3.13.5), — для каждого вида отказов оцененная интенсивность отказов для указанных условий эксплуатации;

б) виды отказов элемента (в виде описания поведения его выходов) из-за случайных отказов АС, которые приводят к отказу функции безопасности и выявляются внутренними для элемента диагностическими тестами или обнаруживаются диагностикой, внешней к элементу (см. 8.3.13.5), — для каждого вида отказов оцененная интенсивность отказов для указанных условий эксплуатации;

в) все ограничения на окружающую среду элемента, которые должны быть соблюдены для обеспечения легитимности оценочных частот отказов из-за случайных отказов АС;

г) любое ограничение срока жизни элемента, который не должен быть превышен для обеспечения легитимности оценочных частот отказов из-за случайных отказов АС;

д) требования к любым контрольным испытаниям и/или техническому обслуживанию;

е) для каждого вида отказов [см. перечисление б)], выявленного внутренними для элемента диагностическими тестами, охват диагностикой, полученный в соответствии с приложением В [см. примечание к перечислению ж)];

ж) для каждого вида отказов [см. перечисление б)], выявленного внутренними для элемента диагностическими тестами, междиагностический интервал (см. примечание).

Примечание — Охват диагностикой и междиагностический интервал необходимы, если требуется доверие к действиям по проведению диагностических тестов, выполняемых для элемента при моделировании полноты безопасности АС Э/Э/ПЭ СБЗС системы (см. 8.3.6.2—8.3.6.4);

и) интенсивность отказов диагностики из-за случайных отказов АС;

к) любая дополнительная информация (например, время ремонта), необходимая для обеспечения возможности получения среднего значения времени ремонта после обнаружения отказа с помощью диагностики;

л) вся информация, необходимая для обеспечения определения доли безопасных отказов элемента, как принято в Э/Э/ПЭ СБЗС системе, определенной в соответствии с приложением В, включая классификацию элементов на типы А и В, в соответствии с 8.3.4;

м) отказоустойчивость элемента АС.

8.3.13.5 Оценочные частоты отказов элемента из-за случайных отказов АС [см. перечисления а) и б) 8.3.13.4] могут быть определены:

- методом анализа видов и последствий отказов элемента с использованием данных по отказам элементов из признанного промышленного источника;
- из предыдущего опыта использования элемента в похожих условиях окружающей среды (см. 8.3.14).

Примечания

1 Уровень доверия любых используемых данных о частоте отказов должен быть равен по крайней мере 70 %.

2 Предпочтительно, чтобы место размещения данных об отказах было доступным. Если доступ к таким данным невозможен, то может потребоваться использование общих данных.

3 Хотя понятие «постоянная частота отказов» подсистемы принято большинством вероятностных оценочных методов, оно применимо лишь при условии, что не превышен срок жизни компонентов подсистемы. Вне их полезного срока жизни (так как вероятность отказов значительно увеличивается со временем) результаты большинства вероятностных расчетных методов бесполезны. Таким образом, любая вероятностная оценка должна включать в себя спецификацию полезного срока жизни компонентов. Полезный срок жизни компонентов подсистем зависит от самого компонента и от условий его эксплуатации, особенно температуры окружающей среды компонента (например, электролитические конденсаторы могут быть очень чувствительны к температуре). Опыт показывает, что полезный срок жизни компонентов часто находится в пределах 8 — 12 лет. Однако эти сроки могут быть значительно меньшими, если компоненты работают в условиях значений параметров эксплуатации, близких к предельным.

8.3.13.6 Для каждого применяемого изделия, для которого требуется соответствие стандартам по функциональной безопасности, поставщики должны обеспечить руководство по безопасности в соответствии с приложением Г.

8.3.13.7 Поставщик должен документально обосновать всю информацию, которая представлена в каждом руководстве по безопасности для применяемых изделий.

Примечания

1 Важно, чтобы требуемое безопасное исполнение конкретного элемента было обеспечено достаточными доказательствами. Требования, не обеспеченные достаточными доказательствами, не позволяют установить корректность и полноту функции безопасности, в реализации которой участвует данный элемент.

2 Могут существовать коммерческие или юридические ограничения на доступность доказательств. Эти ограничения в настоящем стандарте не рассматриваются. Если такие ограничения не обеспечивают необходимого доступа к доказательствам оценки функциональной безопасности, то такой элемент в Э/Э/ПЭ СБЗС системах не используется.

8.3.14 Требования к проверенным в эксплуатации элементам

8.3.14.1 Элемент рассматривают как «проверенный в эксплуатации», только если он имеет явно ограниченные и определенные функциональные возможности и при наличии соответствующего документально оформленного свидетельства, демонстрирующего, что вероятность любых опасных систематических сбоев существенно меньше требуемых уровней полноты безопасности функций безопасности систем, в которых используют этот элемент. Доказательства должны быть основанными на анализе опыта работы конкретной конфигурации элемента, проведенном вместе с анализом пригодности и тестированием.

Примечание — При рассмотрении пригодности и тестируемости следует сосредотачиваться на демонстрации работы элемента в конкретном применении. Должны быть учтены результаты уже проведенного анализа и тестирования. Они включают в себя функциональное поведение, точность, поведение в случае сбоя, время отклика, реакцию на перегрузку, удобство и простоту использования (например, предотвращение ошибки человека) и ремонтопригодность.

8.3.14.2 Документально оформленное свидетельство в соответствии с 8.3.14.1 должно продемонстрировать, что:

- предыдущие условия эксплуатации (см. примечание) конкретного элемента являются такими же или достаточно близкими к тем, в которых будет эксплуатироваться элемент в Э/Э/ПЭ СБЗС системе.

Примечание — При рассмотрении пригодности и тестируемости следует сосредотачиваться на демонстрации работы элемента в конкретном применении. Должны быть учтены результаты уже проведенного анализа и тестирования. Они включают в себя функциональное поведение, точность, поведение в случае сбоя, время отклика, реакцию на перегрузку, удобство и простоту использования (например, предотвращение ошибки человека) и ремонтопригодность;

- интенсивность опасных отказов не выше, чем в предыдущем использовании.

Примечания

1 Руководство по использованию вероятностного подхода для определения полноты безопасности предварительно разработанного программного обеспечения, основанного на его эксплуатации, см. в ГОСТ 34332.5—2021 (приложение Е).

2 Для сбора доказательств для элементов, проверенных в эксплуатации, требуется эффективная система, сообщающая об отказах.

8.3.14.3 Если имеются различия между предыдущими условиями эксплуатации подсистемы и условиями, в которых будет эксплуатироваться Э/Э/ПЭ СБЗС система, то такие различия должны быть идентифицированы и с помощью комбинации соответствующих аналитических методов и испытаний должно быть явно показано, что вероятность любой опасной систематической ошибки настолько низка, что требуемый(е) УБП для функции(й) безопасности элемента достигается(ются).

8.3.14.4 Обоснование безопасности проверенного в эксплуатации элемента должно быть документально оформлено, используя информацию, доступную в 8.3.14.2, о том, что элемент поддерживает требуемую функцию безопасности с необходимой систематической полнотой безопасности. Обоснование безопасности проверенного в эксплуатации элемента должно включать в себя:

- анализ пригодности и тестирование элемента для предназначенного применения;
- демонстрацию эквивалентности между намеченной эксплуатацией и предыдущим опытом эксплуатации, включая анализ влияния различий;
- статистические данные.

8.3.14.5 При проверке выполнения или невыполнения требований 8.3.14.1—8.3.14.4 с учетом охвата и степени детализации имеющейся информации должны быть приняты во внимание следующие факторы:

- сложность элемента;
- стойкость к систематическим отказам, требуемая для элемента;
- новизна проекта.

8.3.14.6 Должно быть доказано, что существующие функции элемента, для которых не было продемонстрировано, что они проверены в эксплуатации, не могут оказать негативного влияния на полноту безопасности выполняемых элементом функций.

Примечание — Данное требование может быть обеспечено путем гарантирования того, что функции физически или электрически отключены, или что ПО, реализующее эти функции, исключено из эксплуатационной конфигурации, или другими видами аргументов и доказательств.

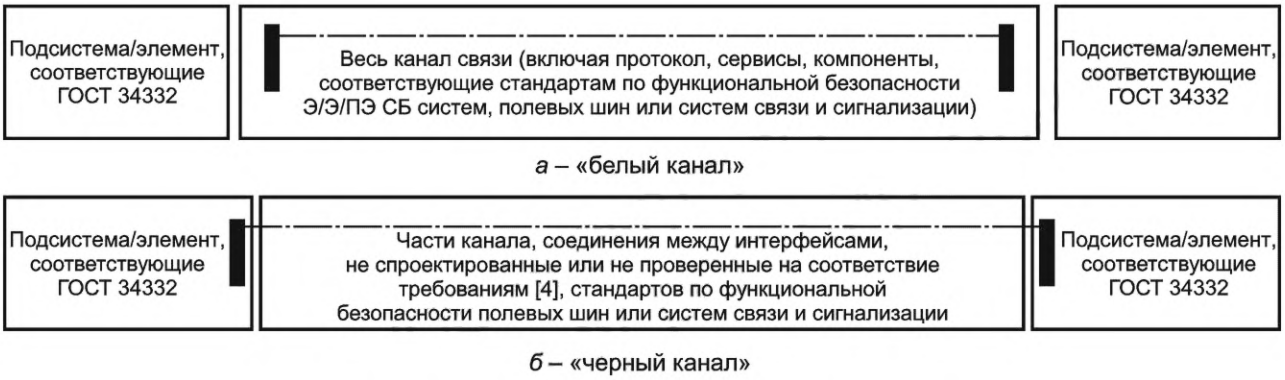
8.3.14.7 Любая будущая модификация проверенного в эксплуатации элемента должна соответствовать требованиям ГОСТ 34332.4—2021 (пункт 7.8).

8.3.15 Дополнительные требования к передаче данных

8.3.15.1 Если при реализации функции безопасности используют средства передачи данных, то должна быть оценена мера отказов (такая, как коэффициент необнаруженных ошибок) коммуникационного процесса с учетом ошибок передачи, повторения, исключения, вставки, повторного упорядочивания, искажения и актами незаконного вмешательства. Эта мера отказов должна быть учтена при оценке отказов функции безопасности из-за случайных отказов (см. 8.3.6).

8.3.15.2 Методы и средства, гарантирующие необходимую меру отказов (такую, как коэффициент необнаруженных ошибок) коммуникационного процесса (см. 8.3.15.1), должны быть реализованы в соответствии с требованиями настоящего стандарта и ГОСТ 34332.4. Допускается два возможных подхода:

- канал связи должен быть полностью разработан, реализован, и для него проведена процедура подтверждения соответствия требованиям стандартов по функциональной безопасности полевых шин, в том числе каналов связи и сигнализации. Это так называемый «белый канал» (см. рисунок 9*а*);



а – «белый канал»

б – «черный канал»

Рисунок 9 — Архитектуры каналов для передачи данных

- части канала связи не разработаны, или для них не проведена процедура подтверждения соответствия требованиям, представленным в [4]. Это так называемый «черный канал» (см. рисунок 9*б*). В этом случае для того, чтобы гарантировать обработку отказа, коммуникационный процесс должен быть осуществлен с помощью Э/Э/ПЭ СБЗС подсистем или элементов, которые взаимодействуют с каналом связи в соответствии с требованиями стандартов по функциональной безопасности, в том числе каналов связи и сигнализации (по мере необходимости).

8.4 Интеграция Э/Э/ПЭ СБЗС системы

8.4.1 Э/Э/ПЭ СБЗС система должна быть интегрирована в соответствии с конкретным проектом системы и испытана в соответствии с конкретными тестами интеграции для нее (см. 8.3.15.2).

8.4.2 В соответствии с 8.3 на стадии интеграции всех модулей в Э/Э/ПЭ СБЗС систему должно быть проведено ее испытание. Такие испытания должны показать, что все модули взаимодействуют правильно, выполняют предназначенные для них функции и не выполняют не предназначенные для них функции.

Примечания

1 Испытание для всех входных комбинаций не проводят. Считается достаточным испытание для всех классов эквивалентности [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.5.2)]. Применение статического анализа [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.6.4)], динамического анализа [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.6.5)] или анализа отказов [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.6.6)] позволяет сократить число испытаний до приемлемого уровня. Если разработку проводить с использованием метода структурного проектирования [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.3.2)] или полуформальными методами [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.2.3)], то эти требования выполнить легче.

2 Если при разработке применять формальные методы [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.2.2)] либо формальные доказательства или программирование с проверкой условий [см. ГОСТ 34332.5—2021 (приложение В, пункты В.5.12 и В.3.3)], то объем таких испытаний может быть существенно сокращен.

3 Также могут быть использованы методы статистического тестирования [см. ГОСТ 34332.5—2021 (приложение Б, пункт Б.5.3)].

8.4.3 Интеграцию СБ ПО в Э/Э/ПЭ систему следует осуществлять в соответствии с требованиями ГОСТ 34332.4—2021 (подраздел 7.5).

8.4.4 Для испытания интегрированных Э/Э/ПЭ СБЗС систем должна быть разработана соответствующая документация, устанавливающая результаты испытаний и определяющая, достигнуты ли цели и критерии, определенные на этапах проектирования и реализации систем. В случае отказа причины и способы его устранения должны быть документально оформлены.

8.4.5 В период интеграции и испытаний любые модификации или изменения Э/Э/ПЭ СБЗС системы должны стать предметом анализа, при котором следует идентифицировать все подсистемы и элементы, на которые влияют данные модификации или изменения, и все необходимые действия по повторному подтверждению выполнения требований.

8.4.6 При испытаниях интегрированной Э/Э/ПЭ СБЗС системы должны быть документально оформлены:

- используемая версия спецификации испытаний;
- критерии принятия испытаний интеграции;

- версия испытуемой Э/Э/ПЭ СБЗС системы;
- используемые средства испытаний и оборудование с датой поверки, набор тестов для интеграции системы;
- результаты каждого испытания;
- любое несоответствие между ожидаемыми и фактическими результатами;
- проведенный анализ и принятое решение о продолжении испытаний или выпуске запроса на изменение (при наличии несоответствия).

8.4.7 Для предотвращения ошибок во время интеграции Э/Э/ПЭ СБЗС системы должна быть использована необходимая группа методов и средств в соответствии с таблицей Б.3 приложения Б.

8.5 Интеграция Э/Э/ПЭ СБЗС систем в комплексную систему безопасности

8.5.1 Интеграцию Э/Э/ПЭ СБЗС систем в КСБ предусматривают на стадии распределения полного набора всех необходимых функций безопасности (и антитеррористической защищенности) объекта по Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска (см. примечание 2 к 8.4.2).

8.5.2 Интеграцию Э/Э/ПЭ СБЗС систем в КСБ осуществляют в соответствии с требованиями проектной и рабочей документации и планом проведения интеграции.

8.5.3 В ходе интеграции предусматривают действия по разрешению возможных конфликтов и сбоев АС и ПО при объединении Э/Э/ПЭ СБЗС систем в КСБ.

8.6 Подтверждение соответствия Э/Э/ПЭ СБЗС систем

8.6.1 Подтверждение соответствия Э/Э/ПЭ СБЗС систем осуществляют в целях подтверждения того, что каждая Э/Э/ПЭ СБЗС система полностью соответствует требованиям безопасности системы в терминах требований к функциям безопасности и полноте безопасности (см. 8.2 настоящего стандарта и ГОСТ 34332.2—2017, подраздел 7.10).

8.6.2 Требования

8.6.2.1 Подтверждение соответствия всех Э/Э/ПЭ СБЗС систем, включая КСБ, следует проводить в соответствии с подготовленным планом подтверждения соответствия (см. также ГОСТ 34332.4—2021, подраздел 7.7).

Примечания

1 Стадия подтверждения соответствия безопасности Э/Э/ПЭ системы на схеме ЖЦ Э/Э/ПЭ СБЗС системы предшествует стадии установки, но в некоторых случаях не может быть выполнена до окончания установки (например, если разработка прикладного ПО еще не завершена до окончания установки).

2 Подтверждение соответствия программируемой электроники системы, связанной с безопасностью, включает в себя подтверждение соответствия АС и ПО. Требования к подтверждению соответствия ПО приведены в ГОСТ 34332.4.

8.6.2.2 Испытательное оборудование, используемое для подтверждения соответствия, должно быть откалибровано и/или поверено в соответствии с нормативным(и) документом(ами), по возможности с межгосударственным(и) стандартом(ами), или с общепризнанной(ыми) процедурой(ами).

8.6.2.3 Для корректной реализации каждой функции безопасности, определенной в требованиях к Э/Э/ПЭ СБЗС системе [см. ГОСТ 34332.2—2017 (подраздел 7.10)], требованиях к проектированию системы (см. 8.3), и всех процедур эксплуатации и технического обслуживания должно быть выполнено подтверждение соответствия с использованием испытаний, тестирования и/или анализа. Если необходимую независимость или разделение между отдельными элементами или подсистемами невозможно показать аналитически, то должны быть испытаны связанные сочетания функционального поведения систем.

Примечание — Поскольку число необходимых тестовых комбинаций может быть значительным, то может требоваться переструктурирование системы.

8.6.2.4 Должна быть подготовлена необходимая документация по проведению испытаний на подтверждение соответствия Э/Э/ПЭ СБЗС системы, в которой для каждой функции безопасности должны быть указаны:

- версия используемого плана проведения подтверждения Э/Э/ПЭ СБЗС системы;
- функция безопасности, подвергаемая испытаниям (или анализу), вместе с конкретной ссылкой на указанные в документации требования к планированию проведения подтверждения соответствия Э/Э/ПЭ СБЗС системы;

- испытательные средства и оборудование вместе с данными об их калибровке и/или поверке;
- результаты каждого испытания;
- несоответствие между ожидаемыми и фактическими результатами.

Примечание — Для каждой функции безопасности отдельная документация не требуется, но каждая функция безопасности и каждое отклонение от функции безопасности должны быть отражены в информации по указанным в настоящем подпункте перечислениям.

8.6.2.5 Если фактические результаты отличаются от ожидаемых результатов более, чем это установлено допусками, результаты испытаний на подтверждение соответствия Э/Э/ПЭ СБЗС системы должны быть документально оформлены, включая:

- описание проведенного анализа;
- принятое решение о продолжении испытаний либо о выпуске извещения об изменении и возвращении к более раннему этапу испытаний на подтверждение соответствия.

8.6.2.6 Поставщик или производитель должны сделать доступными результаты испытаний подтверждения соответствия Э/Э/ПЭ СБЗС системы производителю УО и систем управления УО для обеспечения возможности выполнения требований подтверждения соответствия всей системы безопасности в соответствии с ГОСТ 34332.2.

8.6.2.7 Для предотвращения отказов при проведении подтверждения соответствия Э/Э/ПЭ системы используют группу методов и средств в соответствии с таблицей Б.5 приложения Б.

8.7 Дополнительные требования к процедурам на стадии эксплуатации

8.7.1 Процедуры эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС систем

8.7.1.1 На этапах разработки проектной и рабочей документации на Э/Э/ПЭ СБЗС системы должны быть разработаны процедуры, гарантирующие требуемую функциональную безопасность в период их эксплуатации и технического обслуживания.

8.7.1.2 Должны быть предусмотрены следующие действия и процедуры по эксплуатации и техническому обслуживанию Э/Э/ПЭ системы:

- действия, которые должны быть выполнены для поддержания «проектной» функциональной безопасности Э/Э/ПЭ СБЗС системы, включая замену компонентов с предварительно заданными сроками жизни, например вентиляторов или батарей;
- действия и ограничения, необходимые для предотвращения опасных отказов или уменьшения последствий опасных событий (например, во время установки, пуска в действие, режима эксплуатации, типовых испытаний, обозримых неисправностей, отказов или ошибок, отключений);
- оформление документации (которую следует поддерживать в период эксплуатации) по отказам системы и частотам запросов Э/Э/ПЭ СБЗС системы;
- оформление документации (которую следует поддерживать в период эксплуатации), хранящей результаты аудитов и испытаний Э/Э/ПЭ СБЗС системы;
- проведение процедур технического обслуживания, которым необходимо следовать в случае, если происходят отказы и ошибки в Э/Э/ПЭ СБЗС системе, в том числе:
  - диагностики отказов и восстановления (ремонта);
  - повторного подтверждения соответствия;
  - поддержания отчетности;
  - повторного подтверждения соответствия, если компоненты оригинального оборудования больше не доступны или были заменены новыми версиями;
- проведение процедур по поддержанию параметров отчетности, которые должны быть определены, в частности процедуры отчетности:
  - по отказам;
  - анализу отказов;
- применение инструментов, необходимых для технического обслуживания и повторного подтверждения соответствия, и выполнение процедур для поддержания инструментов и оборудования.

Примечания

1 По соображениям безопасности и экономичности может оказаться выгодным объединять процедуры эксплуатации и технического обслуживания Э/Э/ПЭ системы с полными процедурами эксплуатации и технического обслуживания управляемого оборудования.

2 В процедуры эксплуатации и технического обслуживания Э/Э/ПЭ системы должны быть включены процедуры модификации ПО [см. ГОСТ 34332.4—2021 (подраздел 7.8)].

8.7.1.3 Процедуры эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС системы следует непрерывно совершенствовать с учетом как результатов аудитов функциональной безопасности, так и результатов испытаний системы.

8.7.1.4 Действия по техническому обслуживанию, необходимые для поддержания требуемой (в соответствии с проектом) функциональной безопасности Э/Э/ПЭ СБЗС системы, должны быть заданы на основе систематического подхода. Этот подход должен определять необнаруженные отказы всех элементов, связанных с безопасностью (от датчиков до исполнительных элементов), которые могли бы вызвать снижение достигнутой полноты безопасности. Подходящие методы данного подхода включают в себя:

- экспертизу деревьев отказов;
- анализ видов и последствий отказов.

Примечания

1 Рассмотрение человеческого фактора является ключевым моментом в определении требуемых действий и соответствующих интерфейсов с Э/Э/ПЭ СБЗС системой.

2 Частота проведения контрольных проверок должна быть такой, чтобы была достигнута целевая мера отказов.

3 Частота контрольных проверок, интервал диагностических проверок и время последующего ремонта зависят от нескольких факторов, включая:

- целевую меру отказов, связанных с УПБ;
- архитектуру;
- охват диагностики диагностическими тестами;
- ожидаемую частоту запросов.

4 Частота контрольных проверок и интервал диагностических проверок могут иметь решающее влияние на достижение полноты безопасности АС. Одна из основных причин проведения анализа надежности АС (см. 8.3.6.2) состоит в гарантии соответствия частоты проведения этих двух типов испытаний целевой полноте безопасности АС.

5 Следует придерживаться требований к техническому обслуживанию изготовителя и не ориентироваться только на надежность методов центра обслуживания, пока они не будут полностью обоснованы (например, анализом надежности, демонстрирующим, что целевые меры по отказу Э/Э/ПЭ СБЗС системы).

8.7.1.5 Частота контрольных проверок и интервал диагностических проверок, вероятно, должны иметь решающее влияние на достижение полноты безопасности АС. Одна из основных причин проведения анализа надежности АС (см. 8.3.6.2) состоит в гарантии соответствия частоты проведения этих двух типов испытаний целевой полноте безопасности АС.

8.7.1.6 Следует придерживаться требований к техническому обслуживанию изготовителя и не ориентироваться только на надежность методов центра обслуживания, пока они не будут полностью обоснованы (например, анализом надежности, демонстрирующим, что целевые меры по отказу Э/Э/ПЭ СБЗС системы удовлетворены).

8.7.2 Процедуры модификации Э/Э/ПЭ СБЗС систем

8.7.2.1 Цель настоящего требования состоит в обеспечении гарантирования достижения и поддержания полноты безопасности функций безопасности Э/Э/ПЭ СБЗС систем после их модернизации и видоизменения.

8.7.2.2 На стадии разработки проектной и рабочей документации должны быть разработаны процедуры по модификации и видоизменению Э/Э/ПЭ СБЗС систем и документированию этих процессов по каждому действию по видоизменению и модификации Э/Э/ПЭ СБЗС систем.

8.7.2.3 В процедурах должны быть предусмотрены ведение и поддержка документации по каждому действию по видоизменению и модификации Э/Э/ПЭ СБЗС систем. В документацию должны быть включены:

- детальная спецификация модификации и/или изменений;
- анализ влияния действий по модификации на всю систему, включая АС и ПО (см. ГОСТ 34332.4), взаимодействие с человеком, окружение и возможные взаимодействия;
- утвержденные изменения;
- порядок проведения изменений;
- испытания подсистем и элементов, включая данные повторного подтверждения соответствия;
- предыстория управления конфигурацией Э/Э/ПЭ СБЗС системы;
- отклонения от нормальных действий и условий;
- необходимые изменения системных процедур;
- необходимые изменения документации.

8.7.2.4 Производители или поставщики систем, требующие подтверждения соответствия всем требованиям настоящего стандарта (или его части), должны осуществлять техническую поддержку систем при инициировании изменений в результате обнаруживаемых в АС или ПО дефектов и сообщать пользователям о необходимости модификации и/или изменения в случае обнаружения дефекта, затрагивающего безопасность.

8.7.2.5 Модификацию следует проводить, по крайней мере, с тем же уровнем компетентности специалистов, автоматизированных средств проектирования [см. ГОСТ 34332.4—2021 (подпункт 7.4.4.2), планирования и управления, что и при разработке Э/Э/ПЭ СБЗС систем.

8.7.2.6 После модификации Э/Э/ПЭ СБЗС системы должны быть повторно проверены и должно быть повторно подтверждено их соответствие.

Примечание — См. также ГОСТ 34332.2—2017 (подраздел 7.17).

8.8 Верификация Э/Э/ПЭ СБЗС систем

8.8.1 Цель требований, указанных в настоящем подразделе, состоит в проверке и оценке выходных результатов конкретной стадии ЖЦ Э/Э/ПЭ СБЗС систем для гарантирования их правильности и соответствия требованиям разделов стандартов, предусмотренных для этой стадии.

8.8.2 Верификация Э/Э/ПЭ СБЗС систем должна быть запланирована одновременно с их разработкой для каждой стадии ЖЦ Э/Э/ПЭ СБЗС систем и документально оформлена.

8.8.3 Планирование верификации Э/Э/ПЭ СБЗС системы следует относить ко всем критериям, методам и средствам, используемым для верификации на проверяемой стадии.

8.8.4 При планировании верификации Э/Э/ПЭ СБЗС системы следует определять на каждой стадии выполнение обязательных действий для гарантирования правильности выходных результатов и соответствия требованиям разделов стандартов, предусмотренных для этой стадии.

8.8.5 При планировании верификации Э/Э/ПЭ СБЗС системы следует предусматривать:

- выбор стратегии и методов верификации;
- выбор и использование испытательного оборудования;
- выбор и документальное оформление действий в ходе верификации;
- оценку результатов верификации, полученных непосредственно из верифицирующего оборудования и испытаний.

8.8.6 На каждой стадии проектирования и реализации должно быть показано, что требования функциональной безопасности и полноты безопасности выполняются.

8.8.7 Результат каждого действия по верификации должен быть документально оформлен с указанием, прошли ли Э/Э/ПЭ СБЗС системы проверку, или причины отказов. Должны быть описаны устройства, не соответствующие одному или более из следующих требований:

- ЖЦ Э/Э/ПЭ СБЗС системы (см. 8.2);
- стандартам проектирования (см. 8.3);
- управления функциональной безопасностью (см. раздел 7).

8.8.8 Для верификации спецификации требований к проектированию Э/Э/ПЭ СБЗС системы, после того как были установлены требования к проектированию Э/Э/ПЭ СБЗС системы (см. 8.2) и перед началом следующей стадии (проектирование и реализация), в результате проверки должно быть определено:

- адекватно ли требования к проектированию Э/Э/ПЭ СБЗС системы удовлетворяют спецификациям требований к Э/Э/ПЭ СБЗС системе [см. ГОСТ 34332.2—2017 (подраздел 7.5)]: по безопасности, функциональным возможностям и другим заданным требованиям при планировании безопасности;
- существуют ли несоответствия между:
  - требованиями к Э/Э/ПЭ СБЗС системе (см. ГОСТ 34332.2—2017, подраздел 7.5),
  - требованиями проектирования и реализации Э/Э/ПЭ СБЗС системы (см. 8.3),
  - тестами Э/Э/ПЭ СБЗС системы (см. 8.3),
  - документацией пользователя вместе с остальной документацией на систему.

8.8.9 Для верификации Э/Э/ПЭ СБЗС системы на стадии проектирования и реализации после завершения проектирования и реализации системы (см. 8.3) и до начала следующей стадии (интеграции) в результате проверки должно быть определено:

- адекватны ли тесты Э/Э/ПЭ СБЗС системы для стадий проектирования и реализации Э/Э/ПЭ СБЗС системы;

- обеспечивается ли согласованность и полнота (до уровня модулей, включительно) стадии проектирования и реализации Э/Э/ПЭ СБЗС системы (см. 8.3) в соответствии с требованиями к этой системе (см. ГОСТ 34332.2—2017, подраздел 7.5);
- существуют ли несоответствия между:
  - спецификациями требований к проектированию Э/Э/ПЭ СБЗС системы (см. 8.2),
  - результатами проектирования и реализации Э/Э/ПЭ СБЗС системы (см. 8.3),
  - тестами Э/Э/ПЭ СБЗС системы (см. 8.3).

Примечания

1 Методы подтверждения соответствия системы, анализ отказов и тестирование, рекомендуемые в таблице Б.5 (приложение Б), также могут быть использованы для верификации.

2 При верификации достижения необходимого охвата диагностикой в таблице А.1 (приложение А) следует учесть отказы и ошибки, которые должны быть обнаружены.

8.8.10 Для верификации интеграции Э/Э/ПЭ СБЗС системы и КСБ должна быть проверена интеграция системы и КСБ с тем, чтобы установить выполнение требований, приведенных в 8.4 и 8.5.

8.8.11 Проверки и их результаты должны быть документально оформлены.

8.9 Оценка функциональной безопасности

Требования по оценке функциональной безопасности Э/Э/ПЭ СБЗС систем — по ГОСТ 34332.2—2017 (раздел 8).

Приложение А
(обязательное)

Методы и средства управления отказами Э/Э/ПЭ СБЗС систем в период эксплуатации

А.1 Общие положения

Настоящее приложение следует использовать совместно с 8.3. Оно ограничивает максимальный охват диагностикой, что может потребоваться для выбора методов и средств управления отказами в процессе эксплуатации. Для каждого УПБ в настоящем приложении рекомендованы методы и средства управления случайными, систематическими, эксплуатационными отказами и отказами, связанными с окружающей средой. Более подробную информацию об архитектурах и методах см. в ГОСТ 34332.5—2021 (приложение А).

Перечислить каждую индивидуальную физическую причину отказов в сложных АС не представляется возможным по следующим основным причинам:

- причинно-следственные отношения между ошибками и отказами часто трудно определить;
- при использовании сложных АС и ПО характер отказов изменяется в диапазоне от случайных до систематических.

Отказы Э/Э/ПЭ СБЗС систем могут быть категорированы в зависимости от времени их возникновения как:

- отказы из-за ошибок, возникающих до установки или в период установки системы (например, вследствие ошибок в ПО, включая ошибки спецификации и ошибки программы; вследствие ошибок в АС, включая производственные ошибки и неправильный выбор элементов);
- отказы из-за технических ошибок или ошибок человека, возникающих после установки системы (например, случайные отказы АС или отказы, вызванные неправильным использованием).

Для предотвращения таких отказов или управления ими (если они происходят), как правило, требуется применение большого числа средств. Структура требований, приведенных в настоящем приложении и приложении Б, является следствием разделения средств на средства, используемые для предотвращения отказов на различных стадиях ЖЦ Э/Э/ПЭ СБЗС системы (см. приложение Б), и средства, используемые для управления отказами в период эксплуатации (см. настоящее приложение). Средства по управлению отказами — это собственные встроенные составляющие Э/Э/ПЭ СБЗС систем.

Охват диагностикой и долю безопасных отказов определяют в соответствии с таблицей А.1 и процедурами, описанными в приложении В. Таблицы А.2—А.14 поддерживают требования таблицы А.1 методами и средствами диагностического тестирования и требованиями максимальных уровней охвата диагностикой, которые могут быть достигнуты при их использовании. Требования, приведенные в этих таблицах, не отменяют требований, приведенных в приложении В. Требования, указанные в таблицах А.2—А.14, не являются полными. Могут быть использованы другие методы и средства диагностического тестирования, если приведены свидетельства о поддержке ими требующегося охвата диагностикой. Если требуется высокий уровень охвата диагностикой, то в каждой из таблиц А.2—А.14 должно быть выбрано и применено как минимум одно средство с высоким уровнем охвата диагностикой.

Таблицы А.15—А.17 содержат рекомендуемые меры и средства управления систематическими отказами для каждого УПБ. Таблица А.15 содержит общие меры, рекомендуемые для управления систематическими отказами (см. также ГОСТ 34332.4—2021). Таблица А.16 содержит рекомендуемые меры по управлению отказами из-за влияния окружающей среды. Таблица А.17 содержит рекомендуемые меры по управлению ошибками при эксплуатации. Большинство этих мер по управлению отказами может быть разделено по эффективности их применения в соответствии с таблицей А.18.

Методы и средства, приведенные в таблицах А.2—А.14, описаны в ГОСТ 34332.5—2021 (приложение А). Методы и средства, требуемые для каждого УПБ ПО, приведены в ГОСТ 34332.4. Руководящие указания по определению архитектуры Э/Э/ПЭ СБЗС системы устанавливают в соответствующем стандарте.

Руководящие указания, представленные в настоящем приложении, сами по себе не гарантируют достижение требуемой полноты безопасности. Необходимо учитывать:

- последовательность выбранных методов, средств и то, как они будут дополнять друг друга;
- какие методы и средства в наибольшей степени подходят для решения конкретных проблем, с которыми сталкиваются специалисты во время создания каждой Э/Э/ПЭ СБЗС системы.

А.2 Полнота безопасности аппаратных средств

Требования к ошибкам или отказам, которые должны быть обнаружены с помощью методов и средств управления отказами для достижения соответствующего уровня охвата диагностикой, представлены в таблице А.1 (см. также приложение В). Требования, представленные в таблицах А.2—А.14, поддерживают требования, приведенные в таблице А.1, методами и средствами для диагностического тестирования и требованиями максимальных уровней охвата диагностикой, которые могут быть достигнуты при их использовании. Данные диагностические тесты могут быть проведены непрерывно или периодически. Методы и средства, представленные в таблицах А.2—А.14, не

являются исчерпывающими. Могут быть использованы другие методы и средства, если представлены свидетельства, что они поддерживают необходимый охват диагностикой.

Примечания

1 Краткий обзор методов и средств, упомянутых в таблицах А.2—А.14, приведен в ГОСТ 34332.5—2021 (приложение А), а соответствующие ссылки — в колонках таблиц А.2—А.14.

2 Указания «низкий», «средний» и «высокий» (охват диагностикой) количественно определены как 60 %, 90 % и 99 % соответственно.

Таблица А.1 — Ошибки и отказы, которые подлежат рассмотрению при количественной оценке случайных отказов АС или учитывают при определении доли безопасных отказов

Компонент	См. таблицу настоящего приложения	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Электромеханические устройства	А.2	Невключение или неотключение. Приваренные контакты	Невключение или неотключение. Отдельные приваренные контакты	Невключение или неотключение. Отдельные приваренные контакты. Отсутствует принудительное управление контактами. Отсутствует принудительное включение
Дискретные АС:	А.3, А.7, А.9			
- цифровое устройство В—В		Непрерывный отказ (см. примечание 1)	Неисправности при постоянном токе (см. примечание 2)	Отказы типа отклонений и колебаний при постоянном токе
- аналоговое устройство В—В		Константный отказ	Отказы типа отклонений и колебаний при постоянном токе	Отказы типа отклонений и колебаний при постоянном токе
- источник питания		Непрерывный отказ	Отказы типа отклонений и колебаний при постоянном токе	Отказы типа отклонений и колебаний при постоянном токе
Шина:	А.3, А.7, А.8			
- общая шина		Непрерывный отказ адресов	Временная потеря работоспособности	Временная потеря работоспособности
- диспетчер памяти		Непрерывный отказ данных или адресов	Неверное декодирование адреса. Изменение адресов, вызванное кратковременными ошибками в регистрах диспетчера памяти (см. примечания 3 и 4)	Неверное декодирование адреса. Изменение адресов, вызванное кратковременными ошибками в регистрах диспетчера памяти
- прямой доступ к памяти		Нет доступа или непрерывный доступ	Неисправности данных и адресов при постоянном токе. Изменение информации, вызванное кратковременными ошибками в регистрах памяти прямого доступа. Неверное время доступа	Все отказы, влияющие на данные в памяти. Неверное время доступа
- управление доступом к шине (см. примечание 5)		Непрерывный отказ сигналов управления доступом к шине	Отсутствует или непрерывный доступ к шине	Отсутствует или непрерывный, или неправильный доступ к шине

Продолжение таблицы А.1

Компонент	См. таблицу настоящего приложения	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Процессор: - регистр - внутреннее ОЗУ	А.4, А.10	«Зависание» данных или адресов	Неисправности данных и адресов при постоянном токе. Изменение информации, вызванное исправимыми ошибками	Неисправности данных и адресов при постоянном токе. Динамическое перекрестное переключение ячеек памяти. Изменение информации, вызванное исправимыми ошибками. Отсутствует, неверная или множественная адресация
- устройство кодирования и выполнения, включая регистр признаков		Неверное кодирование или невыполнение	Неверное кодирование или неверное выполнение	Отсутствует определение предполагаемого отказа
- устройство вычисления адреса		Непрерывный отказ	Неисправности при постоянном токе. Изменение адресов, вызванное исправимыми ошибками	Отсутствует определение предполагаемого отказа
- счетчик команд, указатель стека		Непрерывный отказ	Неисправности при постоянном токе. Изменение адресов, вызванное исправимыми ошибками	Неисправности при постоянном токе. Изменение адресов, вызванное исправимыми ошибками
Устройство обработки прерываний: - устройство прерывания	А.4	Отсутствуют или непрерывные прерывания (см. примечание 6)	Отсутствуют или непрерывные прерывания. Пересечение прерываний	Отсутствуют или непрерывные прерывания. Пересечение прерываний
- схема возврата		«Зависание». Отдельные компоненты не инициализируют состояние возврата	Неисправности при постоянном токе. Отказы типа отклонений и колебаний. Отдельные компоненты не инициализируют состояние возврата	Неисправности при постоянном токе. Отказы типа отклонений и колебаний. Отдельные компоненты не инициализируют состояние возврата
Постоянная память (ПЗУ)	А.5	«Зависание» данных или адресов	Неисправности данных и адресов при постоянном токе	Все отказы, влияющие на данные в памяти
Память с произвольным доступом (ОЗУ)	А.6	«Зависание» данных или адресов	Неисправности данных и адресов при постоянном токе. Изменение информации, вызванное исправимыми ошибками	Неисправности данных и адресов при постоянном токе. Перекрестные помехи в ячейках памяти. Изменение информации, вызванное исправимыми ошибками. Отсутствует, неверная или множественная адресация

Окончание таблицы А.1

Компонент	См. таблицу настоящего приложения	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Устройство синхронизации (кварцевое)	А.11	Нижняя или верхняя гармоника	Неверная частота. Неустойчивость периода синхронизации	Неверная частота. Неустойчивость периода синхронизации
Устройство связи и запоминающее устройство большой емкости	А.12	Неверные данные или адреса. Отсутствует передача данных	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи. Неверная последовательность передачи	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи. Неверная последовательность передачи
Датчики	А.13	Непрерывный отказ	Неисправности при постоянном токе. Дрейф и колебания	Неисправности при постоянном токе. Дрейф и колебания
Исполнительные элементы	А.14	Непрерывный отказ	Неисправности при постоянном токе. Дрейф и колебания	Неисправности при постоянном токе. Дрейф и колебания

Примечания

1 «Непрерывный отказ» — это вид отказа, который может быть описан всеми нулями («0») или единицами («1») на выводах элемента.

2 «Неисправности при постоянном токе» включают в себя следующие виды отказов: константные отказы, открытые константные выходы, открытые выходы или выходы с высоким сопротивлением, а также короткие замыкания между линиями связи. Для интегральных схем — это короткое замыкание между любыми двумя соединениями (выводами).

3 Интенсивность исправимых ошибок для полупроводниковых приборов с низким напряжением питания, как известно, более чем на порядок (в 50—500 раз) превышает интенсивность устойчивых неисправностей (постоянное повреждение устройства).

4 Причинами исправимых ошибок являются: альфа-частицы, образовавшиеся в результате процесса распада атомов, нейтроны, внешний источник электромагнитного излучения и внутренние перекрестные помехи. Результаты исправимых ошибок могут быть обработаны только функционирующими средствами обеспечения полноты безопасности. Но такие средства обеспечения полноты безопасности эффективны для случайных отказов АС и могут оказаться неэффективными для исправимых ошибок.

Пример — Для ОЗУ такие тесты, как «блуждающая траектория», «GALPAT» и т. д., неэффективны, тогда как методы, использующие контроль четности и коды с исправлением ошибок, возвращающие содержимое ячеек памяти, или методы, использующие избыточность (и сравнение или голосование), могут быть эффективны.

5 Управление доступом к шине — это механизм, который определяет, какое из устройств может управлять шиной.

6 Отсутствие прерываний означает, что прерывания не выполняются, если они должны происходить. Непрерывные прерывания означают, что выполняются непрерывные прерывания, если они не должны происходить.

7 Данные настоящей таблицы и таблиц А.2—А.18 применяют для СИС в соответствующих уместных случаях.

Таблица А.2 — Электрические компоненты

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывными запросами)	Зависит от охвата диагностикой обнаружения отказов

Окончание таблицы А.2

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Мониторинг контактов реле	А.1.2	Высокий	Необходимо учесть скорость переключения реле при количественной оценке случайных отказов
Компаратор	А.1.3	Высокий	Высокий, если режимы отказов в основном безопасно диагностируются
Схема голосования по мажоритарному принципу	А.1.4	Высокий	Зависит от качества устройства голосования

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

Таблица А.3 — Электронные компоненты

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Схема голосования по мажоритарному принципу	А.1.4	Высокий	Зависит от качества устройства голосования
Тестирование избыточными аппаратными средствами	А.2.1	Средний	Зависит от охвата диагностикой обнаружения отказов
Электрические/электронные средства с автоматической проверкой	А.2.6	Высокий	Зависит от охвата диагностикой тестов
Текущий контроль аналоговых сигналов	А.2.7	Низкий	—
Динамическая обработка сигналов	А.2.2	Средний	Зависит от охвата диагностикой обнаружения отказов
Стандартный тестовый порт доступа и архитектура граничного сканирования	А.2.3	Высокий	Зависит от охвата диагностикой обнаружения отказов
Избыточный контроль	А.2.5	Высокий	Зависит от степени избыточности и текущего контроля

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

Таблица А.4 — Устройства обработки прерываний

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Компаратор	А.1.3	Высокий	Зависит от качества сравнения
Схема голосования по мажоритарному принципу	А.1.4	Высокий	Зависит от качества устройства голосования
Программное самотестирование: предельное количество комбинаций (одноканальное)	А.3.1	Низкий	—
Программное самотестирование: блуждающий бит (одноканальное)	А.3.2	Средний	—
Самотестирование, обеспечиваемое оборудованием (одноканальное)	А.3.3	Средний	—
Запрограммированная обработка (одноканальное)	А.3.4	Высокий	—
Программное обнаружение несовпадений	А.3.5	Высокий	Зависит от качества сравнения

Примечания

1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.

2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.

3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

4 Поскольку много отказов процессора приводят к изменению потока управления, то могут быть также рассмотрены диагностические методы и средства, перечисленные в таблице А.10. Данные диагностические методы и средства охватывают только поток управления, но не поток данных.

Таблица А.5 — Постоянная память

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Защита слов многобитовой избыточностью	А.4.1	Средний	Эффективность многобитовой избыточности защиты слов зависит от включения адреса слова в многоразрядную избыточность. При многобитовой избыточности защиты слов используют соответствующее средство для обнаружения многобитовых отказов по общей причине, например множественная адресация (многократный выбор строки), проблемы источника питания (например, дефекты генератора подкачки заряда), перестановка при формировании строк и столбцов (это позволяет скрыть ошибки формирования) и т. д.
Модифицируемая контрольная сумма	А.4.2	Низкий	—
Сигнатура из одного слова (8 битов)	А.4.3	Средний	Эффективность сигнатуры зависит от ее длины по отношению к длине блока защищаемой информации

Окончание таблицы А.5

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Сигнатура из двух слов (16 битов)	А.4.4	Высокий	Эффективность сигнатуры зависит от ее длины по отношению к длине блока защищаемой информации
Дублирование блока	А.4.5	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В. 2 Для определения охвата диагностикой применяют требования, приведенные в приложении В. 3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.			

Таблица А.6 — Память с произвольным доступом (ОЗУ)

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Тест ОЗУ «шахматная доска» или «марш»	А.5.1	Низкий	—
Тест ОЗУ «блуждающая траектория»	А.5.2	Средний	—
Тест ОЗУ «GALPAT» — попарная запись — считывание с помощью бегущего кода или «Прозрачный GALPAT»	А.5.3	Высокий	—
Тест ОЗУ «Абраам»	А.5.4	Высокий	—
Бит четности для ОЗУ	А.5.5	Низкий	—
Контроль ОЗУ с помощью модифицированного кода Хэмминга или обнаружение сбоев данных с помощью кодов обнаружения и коррекции ошибок (EDC)	А.5.6	Высокий	Эффективность контроля ОЗУ с помощью модифицированного кода Хэмминга или обнаружение сбоев данных с помощью кодов обнаружения и коррекции ошибок (EDC) зависят от включения адреса в код Хемминга и основаны на выполнении соответствующих средств для обнаружения многобитовых отказов по общей причине, например множественная адресация (многократный выбор строки), перестановка при формировании строк и столбцов (это позволяет скрыть ошибки формирования) и т. д.
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В. 2 Для определения охвата диагностикой применяют требования, приведенные в приложении В. 3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1. 4 Для ОЗУ, в котором считывание/ запись происходят не часто (например, во время конфигурирования), эффективны методы по ГОСТ 34332.5—2021 (приложение А, пункты А.4.1—А.4.4), если они осуществляются после каждой операции записи/считывания			

Таблица А.7 — Устройства ввода/вывода и интерфейс (внешний обмен)

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Тестирующая комбинация	А.6.1	Высокий	—
Кодовая защита	А.6.2	Высокий	—
Многоканальное параллельное выходное устройство	А.6.3	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Контролирование выходов	А.6.4	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Сравнение/голосование на входе (1oo2, 2oo3 или более высокая избыточность)	А.6.5	Высокий	Только если поток данных изменяется во время диагностического тестового интервала

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

Таблица А.8 — Информационные каналы (внутренний обмен)

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Однобитовая аппаратная избыточность	А.7.1	Низкий	Данную эффективность для различных типов сетевых коммутаторов каналов передачи данных можно предположить, только если адресные и управляющие шины обеспечены средствами безопасности
Многобитовая аппаратная избыточность	А.7.2	Средний	Данную эффективность для различных типов сетевых коммутаторов каналов передачи данных можно предположить, только если адресные и управляющие шины обеспечены средствами безопасности
Полная аппаратная избыточность	А.7.3	Высокий	—
Анализ с использованием тестирующих комбинаций	А.7.4	Высокий	—
Избыточность при передаче	А.7.5	Высокий	Эффективно только для неустойчивых сбоев
Информационная избыточность	А.7.6	Высокий	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

Таблица А.9 — Источник питания

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой
Защита от перенапряжения с защитным отключением (переключения на второй источник питания)	А.8.1	Низкий
Контроль напряжений (вторичного источника питания) с безопасным отключением/подключением ко второму источнику питания	А.8.2	Высокий
Отключение системы безопасности при снижении напряжения питания или подключение ко второму источнику питания	А.8.3	Высокий

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

Таблица А.10 — Последовательность выполнения программ (контрольный датчик времени)

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Контрольный датчик времени с отдельной временной базой без временного окна	А.9.1	Низкий	—
Контрольный датчик времени с отдельной временной базой и временным окном	А.9.2	Средний	—
Логический контроль последовательности выполнения программ	А.9.3	Средний	Зависит от качества контроля
Комбинация временного и логического контроля последовательности выполнения программ	А.9.4	Высокий	—
Первоначальный тест при включении	А.9.5	Средний	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

Таблица А.11 — Генератор тактовой частоты

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Контрольный датчик времени с отдельной временной базой без временного окна	А.9.1	Низкий	—
Контрольный датчик времени с отдельной временной базой и временным окном	А.9.2	Средний	Зависит от временных ограничений для временного окна
Логический контроль последовательности выполнения программ	А.9.3	Средний	Эффективно только при отказе часов, если внешние временные события влияют на процесс выполнения программы

Окончание таблицы А.11

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Комбинация временного и логического контроля последовательности выполнения программ	А.9.4	Высокий	—
Первоначальный тест при включении	А.9.5	Средний	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

Таблица А.12 — Устройство связи и запоминающее устройство большой емкости

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обмен информацией между Э/Э/ПЭ системой, связанной с безопасностью, и процессом	А.6	См. таблицу А.7	См. устройства входа/выхода и интерфейс

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

Таблица А.13 — Датчики

Диагностический метод/средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Текущий контроль аналоговых сигналов	А.2.7	Низкий	—
Тестирующая комбинация	А.6.1	Высокий	—
Сравнение/голосование на входе (1oo2, 2oo3 или более высокая избыточность)	А.6.5	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Эталонный датчик	А.12.1	Высокий	Зависит от охвата диагностикой обнаружения отказов
Положительно-управляемый переключатель	А.12.2	Высокий	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

Таблица А.14 — Исполнительные элементы (приводы)

Диагностический метод/ средство	Структурный элемент ГОСТ 34332.5—2021	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Мониторинг контактов реле	А.1.2	Высокий	Необходимо учесть скорость переключения реле при количественной оценке случайных отказов
Тестирующая комбинация	А.6.1	Высокий	—
Мониторинг	А.13.1	Высокий	Зависит от охвата диагностикой обнаружения отказов
Перекрестный контроль групповых приводов	А.13.2	Высокий	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении В.
2 Для определения охвата диагностикой применяют требования, приведенные в приложении В.
3 Общие сведения, касающиеся настоящей таблицы, приведены в таблице А.1.

А.3 Систематическая полнота безопасности

Таблицы А.15—А.17 содержат рекомендации для применения методов и средств с целью:
- управления отказами, связанными с проектированием АС (см. таблицу А.15);
- управления отказами, вызванными внешними нагрузками или влияниями (см. таблицу А.16);
- управления отказами на стадии эксплуатации (см. таблицу А.17).

Рекомендации, приведенные в таблицах А.15—А.17, сформированы для УПБ с указанием, во-первых, уровня важности метода или средства и, во-вторых, эффективности его использования. Уровень важности метода или средства обозначены следующим образом:

О — данные методы или средства требуются обязательно для данного УПБ;

ОР — методы или средства особо рекомендованы для данного УПБ. Если эти методы или средства не использованы, то должно быть приведено подробное обоснование их неиспользования;

Р — методы или средства рекомендованы для данного УПБ;

«- -» — методы или средства, не имеющие рекомендаций за и против применения;

НР — методы или средства явно не рекомендованы для данного УПБ. В случае применения этих методов или средств должно быть приведено подробное обоснование такого использования.

Требуемый уровень эффективности методов и средств обозначен:
- «низкий» — данные методы или средства следует использовать в степени, необходимой для достижения по крайней мере уровня низкой эффективности противодействия систематическим отказам;
- «средний» — данные методы или средства следует использовать в степени, необходимой для достижения по крайней мере уровня средней эффективности противодействия систематическим отказам;
- «высокий» — данные методы или средства следует использовать в степени, необходимой для достижения по крайней мере уровня высокой эффективности противодействия систематическим отказам.

Примечание — Данные наименования уровней эффективности и важности методов использованы в таблицах А.15—А.17.

Руководство по уровням эффективности для большинства методов и средств приведено в таблице А.18.

Если мера не является обязательной, то она может быть заменена другими мерами (отдельно или в комбинации с другими).

Все приведенные в таблицах А.15—А.17 методы и средства являются встроенными компонентами Э/Э/ПЭ СБЗС систем, которые могут помочь управлять отказами в неавтономном режиме. Процедурные и организационные методы и средства необходимы на протяжении всего ЖЦ Э/Э/ПЭ СБЗС системы для предотвращения введения в них ошибок. Методы оценки соответствия для проверки действия Э/Э/ПЭ СБЗС систем по противостоянию ожидаемым внешним влияниям необходимы для демонстрации того, что встроенные особенности соответствуют заявленным требованиям (см. приложение Б).

Примечание — Большинство методов, приведенных в таблицах А.15 — А.17, может быть использовано с разной эффективностью в соответствии с таблицей А.18, в которой приведены описания их применения для обеспечения низкой и высокой эффективности. Усилия, требуемые для получения средней эффективности, находятся в пределах усилий, необходимых для получения низкой и высокой эффективности.

Таблица А.15 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами, источниками которых являются этапы разработки аппаратных средств

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Мониторинг последовательности выполнения программ	А.9	ОР низкий	ОР низкий	ОР средний	ОР высокий
2 Обнаружение отказов путем мониторинга в режиме онлайн (см. примечание 5)	А.1.1	Р низкий	Р низкий	Р средний	Р высокий
3 Тестирование избыточными аппаратными средствами	А.2.1	Р низкий	Р низкий	Р средний	Р высокий
4 Стандартный тестовый порт доступа и архитектура граничного сканирования	А.2.3	Р низкий	Р низкий	Р средний	Р высокий
5 Кодовая защита	А.6.2	Р низкий	Р низкий	Р средний	Р высокий
6 Разнообразие аппаратных средств	В.1.4	- - низкий	- - низкий	Р средний	Р высокий

Примечания

1 Требуется выполнение, по крайней мере, одного из методов/средств 2 — 6 или одного из методов, определенных в ГОСТ 34332.4—2021 (таблица А.3).

2 Методы/средства могут быть использованы для различных уровней эффективности в соответствии с таблицей А.18, в которой приведены примеры для низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

3 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в ГОСТ 34332.5—2021 (приложения А, Б и В). Ссылки на соответствующие подпункты указаны во второй колонке.

4 Для Э/Э/ПЭ систем, связанных с безопасностью, действующих в режиме с низкой частотой запросов (например, для систем аварийного отключения), эффективность охвата диагностикой, осуществляемого путем обнаружения отказа с помощью мониторинга в неавтономном режиме, как правило, является низкой или отсутствует.

Таблица А.16 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами, вызванными внешними нагрузками или влияниями

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Меры против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения и других явлений, таких как изменение частоты переменного тока электропитания, которое может привести к опасному отказу	А.8	О низкий	О средний	О средний	О высокий
2 Разделение линий электрического питания и линий передачи информации (см. примечание 4)	А.11.1	О —	О —	О —	О —
3 Повышение устойчивости к электромагнитным воздействиям	А.11.3	О низкий	О низкий	О средний	О высокий

Окончание таблицы А.16

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
4 Средства против физического воздействия окружающей среды (например, температуры, влажности, воды, вибраций, пыли, разъедающих веществ)	А.14	О низкий	О высокий	О высокий	О высокий
5 Мониторинг последовательности выполнения программ	А.9	ОР низкий	ОР низкий	ОР средний	ОР высокий
6 Меры против повышения температуры	А.10	ОР низкий	ОР низкий	ОР средний	ОР высокий
7 Пространственное разделение групповых линий	А.11.2	ОР низкий	ОР низкий	ОР средний	ОР высокий
8 Принцип реактивного тока (отсутствует необходимость в непрерывном контроле для достижения или поддержки безопасного состояния УО)	А.1.5	Р —	Р —	Р —	Р —
10 Обнаружение отказов путем мониторинга в режиме онлайн (см. примечание 5)	А.1.1	Р низкий	Р низкий	Р средний	Р высокий
11 Тестирование избыточными аппаратными средствами	А.2.1	Р низкий	Р низкий	Р средний	Р высокий
12 Кодовая защита	А.6.2	Р низкий	Р низкий	Р средний	Р высокий
13 Передача неэквивалентных сигналов	А.11.4	Р низкий	Р низкий	Р средний	Р высокий
14 Разнообразие аппаратных средств (см. примечание 6)	Б.1.4	- - низкий	- - низкий	- - средний	Р высокий
15 Архитектура программного обеспечения	ГОСТ 34332.4—2021, пункт 7.4.3	См. ГОСТ 34332.4—2021, таблицы А.2 и В.2			

Примечания

1 Все методы с уровнем важности Р в настоящей таблице разделены на две группы: первая группа — метод 8, вторая группа — методы 10—15. Методы в каждой из этих групп взаимозаменяемы. Но требуется выполнение по крайней мере одного из методов из первой группы и одного метода из второй группы.

2 Большинство средств, перечисленных в настоящей таблице, может быть использовано для различных уровней эффективности в соответствии с таблицей А.18, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

3 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в ГОСТ 34332.5—2021 (приложения А и Б). Ссылки на соответствующие подпункты указаны во втором столбце.

4 Отделение линий электропитания от линий передачи информации не является необходимым в случае, если информация передается по оптоволокну, а также для низковольтных линий, спроектированных для питания элементов Э/Э/ПЭ СБЗС системы и передачи информации к ним или от них.

5 Для Э/Э/ПЭ СБЗС систем, действующих в режиме с низкой частотой запросов (например, для систем аварийного отключения), эффективность охвата диагностикой, осуществляемого путем обнаружения отказа с помощью мониторинга в режиме онлайн, как правило, является низкой или этот метод не применяют.

6 Разнообразие АС не требуется, если путем подтверждения соответствия или большим опытом эксплуатации может быть продемонстрировано, что АС в достаточной степени свободны от ошибок на стадии проектирования и в достаточной степени защищены от отказов по общей причине для достижения целевых мер отказов.

Таблица А.17 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами при эксплуатации

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Защита от модификаций	Б.4.8	О низкий	О средний	О высокий	О высокий
2 Обнаружение отказов путем мониторинга в режиме онлайн (см. примечание 4)	А.1.1	Р низкий	Р низкий	Р средний	Р высокий
3 Подтверждение ввода	Б.4.9	Р низкий	Р низкий	Р средний	Р высокий
4 Программирование с проверкой ошибок	Б.3.3	См. ГОСТ 34332.4—2021, таблицы А.2 и Б.2			

Примечания

1 Требуется выполнение по крайней мере одного из методов 2—4.

2 Большинство средств, перечисленных в настоящей таблице, может быть использовано для различных уровней эффективности в соответствии с таблицей А.18, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

3 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в ГОСТ 34332.5—2021 (приложения А, Б и В). Ссылки на соответствующие подпункты указаны во второй колонке.

4 Для Э/Э/ПЭ СБЗС систем, действующих в режиме с низкой частотой запросов (например, для систем аварийного отключения), эффективность охвата диагностикой, осуществляемого путем обнаружения отказа с помощью мониторинга в режиме онлайн, как правило, является низкой или отсутствует.

Таблица А.18 — Эффективность методов и средств управления систематическими отказами

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	Низкая эффективность	Высокая эффективность
Обнаружение отказов путем мониторинга в режиме онлайн (см. примечание)	А.1.1	Запускающие сигналы от управляемого оборудования и его системы управления используются для подтверждения надлежащего действия Э/Э/ПЭ СБЗС систем (только характер изменения во времени и когда система не используется)	Э/Э/ПЭ СБЗС системы перезапускаются временными и логическими сигналами от управляемого оборудования и его системы управления (временное окно для временной функции контрольного датчика времени)
Тестирование избыточными аппаратными средствами (см. примечание)	А.2.1	Дополнительные аппаратные средства проверяют сигналы запускающие Э/Э/ПЭ СБЗС системы (только характер изменения во времени и если система не используется). Эти средства включают в себя вспомогательный исполнительный элемент	Дополнительные аппаратные средства повторно перезапускаются временными и логическими сигналами Э/Э/ПЭ СБЗС систем (временное окно для контрольного датчика времени); голосование между несколькими каналами
Стандартный тестовый порт доступа и архитектура граничного сканирования	А.2.3	Твердотельная логика проверяется с помощью граничных тестовых испытаний в период контрольных испытаний	Диагностический контроль твердотельной логики на соответствие спецификации функций безопасности Э/Э/ПЭ СБЗС систем. Проверяют все функции для всех интегральных схем
Кодовая защита	А.6.2	Обнаружение ошибок с помощью временной избыточности передачи сигналов	Обнаружение ошибок с помощью временной и информационной избыточности передачи сигналов

Окончание таблицы А.18

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	Низкая эффективность	Высокая эффективность
Меры против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения	А.8	Защита от перенапряжения с безопасным отключением или переключением ко второму блоку питания	Регулировка напряжения (повторная) с безопасным отключением или переключением ко второму блоку питания; или выключение питания с безопасным отключением или переключением ко второму блоку питания
Средства против повышения температуры	А.10	Температурный датчик, определяющий превышение температуры	Применение безопасного выключателя с использованием плавкого предохранителя, или измерение нескольких уровней превышения температуры с подачей аварийных сигналов, или применение принудительного воздушного охлаждения с индикацией состояния
Повышение устойчивости к электромагнитным воздействиям (см. примечание)	А.11.3	Помехозащищающий фильтр в источнике питания и на критических входах и выходах; экранирование (при необходимости)	Фильтр против электромагнитных воздействий, которые, как правило, не ожидаются; экранирование
Средства против физического воздействия окружающей среды	А.14	Общепринятая практика, соответствующая прикладному применению	Методы, упомянутые в стандартах для специфического применения
Разнообразие аппаратных средств	Б.1.4	Два или более устройств спроектированы по-разному, но выполняют одну и ту же функцию	Два или более устройств выполняют различные функции
Защита от модификаций	Б.4.8	Модификация требует использования специальных средств	Модификация требует использования блокирующего ключа или специального инструмента с паролем
Подтверждение ввода	Б.4.9	Отображение входных действий для оператора	Проверка по строгим правилам входных данных, вводимых оператором, с отклонением неправильных входных данных
Примечание — При использовании методов и средств по А.1.1, А.2.1, А.11.3 и А.14 ГОСТ 34332.5—2021 в качестве высокоэффективных методов и средств предполагается, что методы и средства с низким уровнем эффективности также будут использованы.			

Приложение Б
(обязательное)

Методы и средства по предотвращению систематических отказов на стадиях жизненного цикла Э/Э/ПЭ СБЗС систем

Для каждого уровня безопасности рекомендуемые методы и средства предотвращения отказов в Э/Э/ПЭ СБЗС системах приведены в таблицах Б.1—Б.5. Более подробную информацию см. в ГОСТ 34332.5—2021 (приложение Б). Требования к методам по управлению отказами в период эксплуатации приведены в приложении А, а методы описаны в ГОСТ 34332.5—2021 (приложение А). Перечислить каждую причину систематических отказов, источники которых возникают на протяжении всех стадий ЖЦ, и каждое средство защиты не представляется возможным по следующим причинам:

а) влияние систематических ошибок зависит от стадии ЖЦ, на которой они вносятся;

б) эффективность любой конкретной меры или средства по предотвращению отказов зависит от их применения.

Поэтому количественный анализ для предотвращения систематических отказов невозможен.

Категории отказов в Э/Э/ПЭ СБЗС системах могут быть установлены в соответствии со следующими стадиями ЖЦ, которые явились источником внесения соответствующих ошибок:

- отказы, вызванные ошибками, возникающими до установки или в период установки системы (например, ошибки ПО включают в себя ошибки спецификации и ошибки программ; ошибки в АС включают в себя ошибки на этапе изготовления и неправильный выбор компонентов);
- отказы, вызванные ошибками, возникающими после установки системы (например, случайные отказы АС или отказы, вызванные неправильным использованием оборудования).

Для предотвращения отказов или управления ими (если они происходят), как правило, требуется применение большого числа средств. Структура требований, приведенных в настоящем приложении и приложении А, является следствием разделения средств и методов на средства и методы, используемые для предотвращения отказов на различных стадиях ЖЦ Э/Э/ПЭ СБЗС системы (см. настоящее приложение), и средства и методы, используемые для управления отказами в период эксплуатации (см. приложение А). Средства по управлению отказами — это собственные встроенные составляющие Э/Э/ПЭ СБЗС системы, а средства и методы для предотвращения отказов — используемые в течение ЖЦ системы.

Рекомендации, приведенные в таблицах Б.1—Б.5, сформированы для УПБ и устанавливают, во-первых, важность меры (метода или средства) и, во-вторых, эффективность их использования. Уровень важности метода или средства обозначают:

О — данные методы или средства требуются обязательно для данного УПБ;

ОР — методы или средства особо рекомендованы для данного УПБ. Если эти методы или средства не используются, то должно быть приведено подробное обоснование их неиспользования;

Р — методы или средства рекомендованы для данного УПБ;

«- -» — методы или средства, не имеющие рекомендаций за и против применения;

НР — методы или средства явно (положительно) не рекомендованы для данного УПБ. В случае применения этих методов или средств должно быть приведено подробное обоснование такого использования.

Уровни эффективности методов или средств обозначены следующим образом:

- «низкий» — данные методы или средства следует использовать в степени, необходимой для достижения по крайней мере уровня низкой эффективности противодействия систематическим отказам;
- «средний» — данные методы или средства следует использовать в степени, необходимой для достижения по крайней мере уровня средней эффективности противодействия систематическим отказам;
- «высокий» — данные методы или средства следует использовать в степени, необходимой для достижения по крайней мере уровня высокой эффективности противодействия систематическим отказам.

Примечания

1 Большинство методов и средств, приведенных в таблицах Б.1—Б.5, может использоваться с разной эффективностью в соответствии с таблицей Б.6, в которой приведены описания их применения для обеспечения низкой и высокой эффективности. Усилия, требуемые для получения средней эффективности, находятся в пределах усилий, необходимых для получения низкой и высокой эффективности.

2 Данные наименования уровней эффективности и важности методов для различных УПБ использованы в таблицах Б.1—Б.5.

Если мера не является обязательной, то она может быть заменена другими мерами (одной или в комбинации с другими).

Руководящие указания, представленные в настоящем приложении, не гарантируют требуемой полноты безопасности. Следует учитывать:

- последовательность выбранных методов и средств и то, как они будут дополнять друг друга;
- какие из методов и средств предназначены для каждой стадии ЖЦ;

- какие методы и средства в наибольшей степени подходят для решения конкретных проблем, с которыми сталкиваются специалисты во время создания каждой Э/Э/ПЭ СБЗС системы.

Таблица Б.1 — Рекомендации по предотвращению ошибок во время формирования спецификации требований к проектированию Э/Э/ПЭ СБЗС системы (см. 8.2)

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Управление проектами	Б.1.1	О низкий	О низкий	О средний	О высокий
2 Документация	Б.1.2	О низкий	О низкий	О средний	О высокий
3 Разделение систем, связанных с безопасностью, и систем, не связанных с безопасностью	Б.1.3	ОР низкий	ОР низкий	ОР средний	ОР высокий
4 Структурирование спецификации	Б.2.1	ОР низкий	ОР низкий	ОР средний	ОР высокий
5 Экспертиза спецификации	Б.2.6	- - низкий	ОР низкий	ОР средний	ОР высокий
6 Полуформальные методы	Б.2.3, см. также ГОСТ 34332.4—2021, таблица Б.7	Р низкий	Р низкий	ОР средний	ОР высокий
7 Таблица контрольных проверок	Б.2.5	Р низкий	Р низкий	Р средний	Р высокий
8 Автоматизированные средства разработки спецификаций	Б.2.4	- - низкий	Р низкий	Р средний	Р высокий
9 Формальные методы	Б.2.2	- - низкий	- - низкий	Р средний	Р высокий

Примечания

1 Методы 5 — 9, имеющие уровень важности Р, являются взаимозаменяемыми, но обязательно применение как минимум одного из них.

2 Для верификации данной стадии ЖЦ системы безопасности требуется выполнение по крайней мере одного из методов 5 — 9 или перечисленных в таблице Б.5.

3 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей Б.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, требуемые для среднего уровня эффективности, находятся между усилиями, требуемыми для низкого и высокого уровней эффективности.

4 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в ГОСТ 34332.5—2021, приложение Б.

Таблица Б.2 — Рекомендации по предупреждению внесения ошибок во время проектирования и разработки Э/Э/ПЭ СБЗС системы (см. 8.3)

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Соблюдение руководящих материалов и стандартов	Б.3.1	О высокий	О высокий	О высокий	О высокий
2 Управление проектами	Б.1.1	О низкий	О низкий	О средний	О высокий
3 Документация	Б.1.2	О низкий	О низкий	О средний	О высокий
4 Структурное проектирование	Б.3.2	ОР низкий	ОР низкий	ОР средний	ОР высокий

Окончание таблицы Б.2

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
5 Модульное проектирование	Б.3.4	OP низкий	OP низкий	OP средний	OP высокий
6 Использование достоверно испытанных компонент	Б.3.3	P низкий	P низкий	P средний	P высокий
7 Полуформальные методы	Б.2.3, см. также ГОСТ 34332.4—2021, таблица Б.7	P низкий	P низкий	OP средний	OP высокий
8 Таблица контрольных проверок	Б.2.5	- - низкий	P низкий	P средний	P высокий
9 Средства автоматизированного проектирования	Б.3.5	- - низкий	P низкий	P средний	P высокий
10 Моделирование	Б.3.6	- - низкий	P низкий	P средний	P высокий
11 Проверка (обзор и анализ), сквозной контроль аппаратных средств	Б.3.7, Б.3.8	- - низкий	P низкий	P средний	P высокий
12 Формальные методы	Б.2.2	- - низкий	- - низкий	P средний	P высокий

Примечания

1 Методы 6—12, имеющие уровень важности P, являются взаимозаменяемыми, но обязательно применение как минимум одного из них.

2 Для верификации данной стадии ЖЦ системы безопасности требуется выполнение по крайней мере одного из методов 6—12 или перечисленных в таблице Б.5.

3 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей Б.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

4 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в ГОСТ 34332.5—2021 (приложение Б).

Таблица Б.3 — Рекомендации для предотвращения ошибок на стадии интеграции Э/Э/ПЭ СБЗС системы (см. 8.4, 8.5)

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Функциональное тестирование	Б.5.1	O высокий	O высокий	O высокий	O высокий
2 Управление проектами	Б.1.1	O низкий	O низкий	O средний	O высокий
3 Документация	Б.1.2	O низкий	O низкий	O средний	O высокий
4 Тестирование методом «черного ящика»	Б.5.2	P низкий	P низкий	P средний	P высокий
5 Полевые испытания	Б.5.4	P низкий	P низкий	P средний	P высокий
6 Статистическое тестирование	Б.5.3	- - низкий	- - низкий	P средний	P высокий

Таблица Б.4 — Рекомендации по предотвращению ошибок и отказов в период эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС системы (см. 8.7.1)

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Инструкции по эксплуатации и техническому обслуживанию	Б.4.1	OP высокий	OP высокий	OP высокий	OP высокий
2 Удобство общения с пользователем	Б.4.2	OP высокий	OP высокий	OP высокий	OP высокий
3 Удобство технического обслуживания	Б.4.3	OP высокий	OP высокий	OP высокий	OP высокий
4 Управление проектами	Б.1.1	O низкий	O низкий	O средний	O высокий
5 Документация	Б.1.2	O низкий	O низкий	O средний	O высокий
6 Сокращение работ на стадии эксплуатации	Б.4.4	- - низкий	P низкий	OP средний	OP высокий
7 Защита от ошибок оператора	Б.4.6	- - низкий	P низкий	OP средний	OP высокий
8 Эксплуатация только квалифицированным оператором	Б.4.5	- - низкий	P низкий	P средний	OP высокий

Примечания

1 Методы 6 — 8, имеющие уровень важности P, являются взаимозаменяемыми, но обязательно применение как минимум одного из них.

2 Для верификации данной стадии ЖЦ системы безопасности требуется выполнение метода, основанного на таблице контрольных проверок (см. ГОСТ 34332.5—2021, приложение Б, подраздел Б.2.5), или метода, основанного на экспертизе спецификации (см. ГОСТ 34332.5—2021, приложение Б, подраздел Б.2.6).

3 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей Б.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

4 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в ГОСТ 34332.5—2021 (приложение Б).

Таблица Б.5 — Рекомендации по предотвращению ошибок при подтверждении соответствия безопасности Э/Э/ПЭ СБЗС системы (см. 8.6)

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Функциональное тестирование	Б.5.1	OP высокий	OP высокий	OP высокий	OP высокий
2 Функциональные испытания в условиях окружающей среды	Б.6.1	OP высокий	OP высокий	OP высокий	OP высокий
3 Испытания на устойчивость к пиковым выбросам внешних воздействий	Б.6.2	OP высокий	OP высокий	OP высокий	OP высокий
4 Испытание с введением неисправностей (при требуемом охвате диагностикой 90 % и более)	Б.6.10	OP высокий	OP высокий	OP высокий	OP высокий
5 Управление проектами	Б.1.1	O низкий	O низкий	O средний	O высокий

Окончание таблицы Б.5

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	УПБ 1	УПБ 2	УПБ 3	УПБ 4
6 Документация	Б.1.2	О низкий	О низкий	О средний	О высокий
7 Статический анализ, динамический анализ, анализ отказов	Б.6.4, Б.6.5, Б.6.6	- - низкий	Р низкий	Р средний	Р высокий
8 Моделирование и анализ отказов	Б.3.6, Б.6.6	- - низкий	Р низкий	Р средний	Р высокий
9 Анализ наихудшего случая, динамический анализ и анализ отказов	Б.6.7, Б.6.5, Б.6.6	- - низкий	Р низкий	Р средний	Р высокий
10 Статический анализ и анализ отказов (см. примечание 4)	Б.6.4, Б.6.6	Р низкий	Р низкий	НР —	НР —
11 Расширенное функциональное тестирование	Б.6.8	- - низкий	ОР низкий	ОР средний	ОР высокий
12 Тестирование методом «черного ящика»	Б.5.2	Р низкий	Р низкий	Р средний	Р высокий
13 Испытание с введением неисправностей (при требуемом охвате диагностикой менее 90 %)	Б.6.10	Р низкий	Р низкий	Р средний	Р высокий
14 Статистическое тестирование	Б.5.3	- - низкий	- - низкий	Р средний	Р высокий
15 Испытания в наихудших случаях	Б.6.9	- - низкий	- - низкий	Р средний	Р высокий
16 Полевые испытания	Б.5.4	Р низкий	Р низкий	Р средний	НР —

Примечания

1 Все методы 7 — 16, имеющие уровень важности Р, являются взаимозаменяемыми, но обязательно применение, как минимум, одного из методов 7 — 10 (аналитические методы) и одного из методов 11 — 16 (средства испытаний).

2 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей Б.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

3 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в ГОСТ 34332.5—2021 (приложение В).

4 Статистический анализ и анализ отказов не рекомендуются для УПБ 3 и УПБ 4, так как эти методы недостаточны, если не используются вместе с динамическим анализом.

Таблица Б.6 — Эффективность методов и средств для предотвращения систематических ошибок

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	Низкая эффективность	Высокая эффективность
Управление проектами (см. примечание)	Б.1.1	Определение действий и обязанностей, планирование и распределение ресурсов, обучение соответствующего персонала, последовательность проверок после модификаций	Подтверждение соответствия, независимое от проекта; регулярный контроль проекта; стандартизованная процедура подтверждения соответствия; управление конфигурацией; статистики отказов; автоматизированные расчеты; автоматизированная разработка программного обеспечения

Продолжение таблицы Б.6

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	Низкая эффективность	Высокая эффективность
Документация (см. примечание)	Б.1.2	Графические и естественные языки, например блок-схемы, потоковые диаграммы	Правила, описывающие порядок прохождения и размещения документации в организации; содержимое таблиц контрольных проверок; автоматизированное управление документацией; формальный контроль изменений
Разделение функций безопасности Э/Э/ПЭ системы и функций, не связанных с безопасностью	Б.1.3	Хорошо определенные интерфейсы между Э/Э/ПЭ системами, связанными с безопасностью, и системами, не связанными с безопасностью	Полное отделение Э/Э/ПЭ систем, связанных с безопасностью, от систем, не связанных с безопасностью, т. е. отсутствие доступа по записи систем, не связанных с безопасностью, к Э/Э/ПЭ системам, связанным с безопасностью, и физическое разделение в пространстве во избежание влияний общей причины
Структурирование спецификации	Б.2.1	Иерархическое разделение вручную требований на подтребования, описание интерфейсов	Формирование иерархического разделения с использованием средств автоматизированного расчета, автоматический контроль последовательности, уточнение на более низком функциональном уровне
Формальные методы	Б.2.2	Используемые персоналом, имеющим опыт в применении формальных методов	Используемые персоналом, имеющим опыт в применении формальных методов в аналогичных областях с применением автоматизированных средств поддержки
Полуформальные методы	Б.2.3	Использование полуформальных методов для описания некоторых критических частей	Полное описание Э/Э/ПЭ СБЗС систем различными полуформальными методами для демонстрации различных аспектов; проверка согласованности между методами
Автоматизированные средства разработки спецификации	Б.2.4	Средства без предпочтения конкретного метода проектирования	Моделеориентированные процедуры с иерархической структурой, описание всех объектов и их отношений, общая база данных, автоматический контроль непротиворечивости
Таблицы контрольных проверок	Б.2.5	Подготовленные таблицы контрольных проверок для всех стадий жизненного цикла системы безопасности, концентрация на главных проблемах безопасности	Подготовленные подробные таблицы контрольных проверок для всех стадий жизненного цикла системы безопасности
Экспертиза спецификации	Б.2.6	Экспертиза спецификации требований безопасности независимым лицом	Экспертиза и повторная экспертиза независимой организацией, использующей формальную процедуру с исправлением всех обнаруженных ошибок
Структурное проектирование	Б.3.2	Проектирование иерархических схем, выполненное вручную	Повторный контроль компонент схемы; отслеживание взаимосвязи между спецификацией, проектом, принципиальными схемами и перечнем компонентов системы; автоматизация; использование определенных методов (см. также 8.3.7)

Продолжение таблицы Б.6

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	Низкая эффективность	Высокая эффективность
Использование достоверно испытанных компонентов (см. примечание)	Б.3.3	Достаточно перепроверки; конструктивные характеристики	Проверено в эксплуатации (см. 8.3.14)
Модульное проектирование (см. примечание)	Б.3.4	Модули ограниченных размеров; каждый модуль функционально изолирован	Повторное использование хорошо проверенных модулей; модулей с ясными свойствами; модулей, имеющих максимум один вход, один выход и один отказавший выход
Средства автоматизированного проектирования	Б.3.5	Автоматизированная поддержка сложных стадий жизненного цикла системы безопасности	Использование средств, проверенных в эксплуатации (см. 8.3.14), или средств с подтвержденным соответствием; полная автоматизация создания системы для всех стадий жизненного цикла безопасности
Моделирование	Б.3.6	Моделирование на модульном уровне, используя входные/выходные данные внешних устройств	Моделирование на уровне компонентов, используя входные/выходные данные
Проверка аппаратных средств	Б.3.7	Проверка проводится лицом, не связанным с проектированием	Проверка и повторная проверка проводятся независимой организацией, использующей формальные процедуры с исправлением всех обнаруженных ошибок
Сквозной контроль аппаратных средств	Б.3.8	Сквозной контроль аппаратных средств проводится лицом, независимым от проектирования	Сквозной контроль аппаратных средств проводится независимой организацией, действующей по формальной процедуре, с исправлением всех обнаруженных ошибок
Ограничение эксплуатационных возможностей (см. примечание)	Б.4.4	Применение ключа или пароля для управления режимом работы	Определенная жесткая процедура для разрешенных действий
Эксплуатация исключительно квалифицированными операторами	Б.4.5	Базовое обучение по используемому типу систем безопасности плюс два года соответствующего опыта работы	Ежегодное обучение всех операторов; опыт работы каждого оператора не менее пяти лет с устройствами, связанными с безопасностью, более низкого уровня полноты безопасности
Защита от ошибок оператора (см. примечание)	Б.4.6	Подтверждение входного сообщения	Подтверждение и проверка согласованности каждой входной команды
Тестирование методом «черного ящика» (см. примечание)	Б.5.2	Классы эквивалентности и тестирование по отдельным диапазонам входных сигналов, тестирование по граничным значениям, использование предписанных условий испытаний	Условия испытаний по диаграммам последствий причин (отказов) в комбинации с критическими случаями в экстремальных диапазонах работы

Продолжение таблицы Б.6

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	Низкая эффективность	Высокая эффективность
Статистическое тестирование (см. примечание)	Б.5.3	Статистическое распределение для всех входных данных	Получение результатов испытаний автоматическими средствами, большое число тестовых испытаний, распределение входных данных в соответствии с условиями реального применения и принятыми моделями отказов
Полевые испытания (см. примечание)	Б.5.4	10 000 часов эксплуатации; по крайней мере, один год эксплуатации и не менее десяти устройств в различных применениях; статистическая точность 95 %; отсутствие каких-либо критических отказов безопасности	10 млн. часов эксплуатации; по крайней мере два года эксплуатации и не менее 10 устройств в различных применениях; статистическая точность 99,9 %; подробная документация всех изменений (включая мельчайшие) в период прошлой эксплуатации
Испытания на устойчивость к пиковым выбросам внешних воздействий	Б.6.2	—	Должна быть продемонстрирована устойчивость большая, чем для граничных значений реальных режимов эксплуатации
Статический анализ	Б.6.4	Применение блок-схем; выявление слабых мест; определение тестовых примеров	Применение подробных схем; предсказание ожидаемого поведения в случаях испытаний; применение инструментов испытаний
Динамический анализ и тестирование	Б.6.5	Применение блок-схем; выявление слабых мест; определение тестовых примеров	Применение подробных схем; предсказание ожидаемого поведения в случаях испытаний; применение инструментов испытаний
Анализ отказов	Б.6.6	На уровне модулей, используя входные/выходные данные периферийных устройств	На уровне компонентов, используя входные/выходные данные
Анализ наихудшего случая	Б.6.7	Выполняется для функций безопасности, проводится с использованием комбинаций граничных значений, соответствующих реальным условиям эксплуатации	Выполняется для функций, не относящихся к безопасности; проводится с использованием комбинаций граничных значений, соответствующих реальным условиям эксплуатации
Расширенное функциональное тестирование	Б.6.8	Испытания, при которых все функции безопасности проверяют при таких же статических входных состояниях, что и в случаях, вызванных процессами отказов или условиями эксплуатации	Испытания, при которых все функции безопасности проверяют при таких же статических входных состояниях и/или необычных входных изменениях, что и в случаях, вызванных процессами отказов или условиями эксплуатации (включая те, которые могут возникать редко)
Испытания в наихудших случаях	Б.6.9	Испытания, при которых функции безопасности проверяют для таких комбинаций граничных значений, которые встречаются в реальных условиях эксплуатации	Испытания, при которых функции, не относящиеся к безопасности, проверяются для таких комбинаций граничных значений, которые встречаются в реальных условиях эксплуатации

Окончание таблицы Б.6

Метод/средство	Структурный элемент ГОСТ 34332.5—2021	Низкая эффективность	Высокая эффективность
Испытания с введением неисправностей	Б.6.10	На уровне блоков устройств, используя входные/выходные данные периферийных устройств	На уровне компонентов, используя их входные/выходные данные
Примечание — При использовании методов и средств по Б.1.1, Б.1.2, Б.3.3, Б.3.4, Б.4.4, Б.4.6, Б.5.2, Б.5.3, Б.5.4, Б.6.7 и Б.6.9 ГОСТ 34332.5—2021 в качестве высокоэффективных методов и средств предполагается, что методы и средства с низким уровнем эффективности будут также использованы.			

Приложение В
(обязательное)

Охват диагностикой и доля безопасных отказов

В.1 Расчет охвата диагностикой и доли безопасных отказов элемента аппаратного средства

Охват диагностикой и доля безопасных отказов элемента АС рассчитывают следующим образом:

- проводят анализ видов отказов и их влияния для определения влияния каждого вида отказов каждого компонента или группы компонентов в элементе на поведение Э/Э/ПЭ СБЗС систем в отсутствие диагностических проверок. В результате предоставляют информацию (см. примечания), достаточную для того, чтобы убедиться в том, что влияние видов отказов и результаты анализа этого влияния с достаточной степенью достоверности соизмеримы с требованиями полноты безопасности.

Примечания

1 Для проведения данного анализа необходимы:

- подробная блок-схема Э/Э/ПЭ СБЗС системы, описывающая элемент вместе со взаимосвязями для той части Э/Э/ПЭ СБЗС системы, которая затрагивает рассматриваемую(ые) функцию(ии) безопасности;
- схемные решения элемента АС, описывающие каждый компонент или группу компонентов и взаимосвязи между компонентами;
- виды отказов и частоты (интенсивности) отказов для каждого компонента или группы компонентов и связанные соотношения безопасных и опасных отказов к полной средней частоте (интенсивности) отказов в процентах.

2 Требуемая точность этого анализа зависит от ряда факторов (см. ГОСТ 34332.2—2017, подраздел 5.1). В частности, должен быть принят во внимание УПБ рассматриваемых функций безопасности. Для более высоких УПБ ожидается, что виды отказов и анализ влияний будут специфичными в соответствии с конкретными типами компонентов и существующими условиями окружающей среды. Также важен полный и подробный анализ для элемента, используемого в архитектуре АС, имеющего нулевую устойчивость к отказам АС;

- все виды отказов подразделяют на категории по признаку, является ли он (в отсутствие диагностических испытаний):
  - безопасным отказом;
  - опасным отказом;
- отказы компонентов, не принадлежащих Э/Э/ПЭ СБЗС системе, а также отказы, не влияющие на поведение Э/Э/ПЭ СБЗС системы, не должны учитываться при вычислении ОД или ДБО;
- оценив частоты отказов каждого компонента или группы компонентов λ и с учетом видов отказов и результатов анализа последствий каждого вида отказа каждого компонента или группы компонентов, вычисляют частоту безопасных отказов λ_S и частоту опасных отказов λ_D. Если одна из этих интенсивностей отказов не будет иметь постоянного значения, то необходимо оценить ее среднее число за конкретный период времени и использовать для вычислений ОД и ДБО.

Примечание — Частота отказов каждого компонента или группы компонентов может быть оценена с использованием данных из признанного промышленного источника с учетом окружающей среды применения. Однако применение специфических данных предпочтительнее, особенно в случаях, если элемент состоит из небольшого числа компонентов и если любая ошибка в оценке вероятности безопасных и опасных отказов конкретного компонента может оказать существенное влияние на оценку доли безопасных отказов;

- оценивают для каждого компонента или группы компонентов доли опасных отказов, которые могут быть обнаружены диагностическими тестами (см. Г.2 приложения Г), и, следовательно, частоты опасных отказов, обнаруженных диагностическими тестами λ_{Dd};
- вычисляют полные частоты опасных отказов $\Sigma\lambda_D$, полные частоты опасных отказов, обнаруженных диагностическими тестами $\Sigma\lambda_{Dd}$, и полные частоты безопасных отказов $\Sigma\lambda_S$;
- вычисляют охват диагностикой элемента, как $\Sigma\lambda_{Dd}/\Sigma\lambda_D$;
- вычисляют долю безопасных отказов элемента как

$$\text{ДБО} = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du}). \quad \text{(В.1)}$$

Примечания

1 Формула (В.1) применима, если значения интенсивностей отказов постоянны.

2 Охват диагностикой каждого элемента в Э/Э/ПЭ системе, связанной с безопасностью, должен учитываться при оценке достигаемой меры отказов для функции безопасности (см. 8.3.6.2). Доля безопасных отказов должна учитываться при определении архитектурных ограничений на полноту безопасности АС (см. 8.3.4).

При анализе, выполняемом для определения охвата диагностикой и доли безопасных отказов, следует охватывать все компоненты, в том числе электрические, электронные, электромеханические, механические и т. п.,

необходимые элементу для выполнения функции(й) безопасности, которые требуются Э/Э/ПЭ СБЗС системе. Для каждого из компонентов должны быть рассмотрены все возможные виды опасных отказов, которые приводят к опасному состоянию, препятствуют реакции безопасности, если такая реакция определена, или ставят под угрозу полноту безопасности Э/Э/ПЭ СБЗС систем.

Ошибки и отказы, которые должны быть обнаружены в период эксплуатации или проанализированы при определении доли безопасных отказов, приведены в таблице А.1.

Если для анализа видов отказов и их влияния используют эксплуатационные данные, то достаточно обеспечить требования полноты безопасности. При этом требуемый нижний предел статистической односторонней достоверности должен быть не менее 70 %.

Примечание — Для вычисления степени охвата диагностикой допускается использовать альтернативные методы, например моделирование ошибок с помощью более точных компьютерных моделей как для схем Э/Э/ПЭ СБЗС систем, так и для используемых при их разработке электронных компонентов, например использование моделей транзисторов для моделирования ИС.

В.2 Определение факторов охвата диагностикой

При вычислении охвата диагностикой для элемента (см. В.1) для каждого компонента или группы компонентов необходимо оценить долю опасных отказов, обнаруживаемых диагностическими тестами. Диагностические тесты, которые могут внести вклад в охват диагностикой, включают в себя (но не ограничиваются) такие меры, как:

- сравнительные проверки, например контроль и сравнение избыточных (резервных) сигналов;
- дополнительные встроенные тестовые программы, например вычисление контрольных сумм в устройстве памяти;
- контроль с помощью внешних воздействий, например пропусканием импульсного сигнала через контролируемые тракты;
- непрерывный контроль аналогового сигнала, например для обнаружения выхода из диапазона уровней показаний при отказе сенсора.

Для вычисления охвата диагностикой необходимо определить те виды отказов, которые обнаруживаются диагностическими тестами. Возможно, что отказы, связанные с разомкнутыми или короткозамкнутыми цепями для простых компонентов (резисторов, конденсаторов, транзисторов), могут быть обнаружены методом стопроцентного охвата диагностикой. Однако для более сложных элементов типа Б (см. 8.3.4.3) должны быть учтены ограничения охвата диагностикой для различных компонентов, представленных в таблице А.1. Данный анализ должен быть проведен для каждого компонента или группы компонентов каждого элемента и каждой Э/Э/ПЭ СБЗС системы.

Примечания

1 Рекомендуемые методы и средства диагностического тестирования (испытания) и рекомендуемые максимальные диагностические охваты, которые могут потребоваться, приведены в таблицах А.2—А.14. Данные тесты проводят непрерывно или периодически (в зависимости от интервала диагностического тестирования). Требования таблиц А.2—А.14 не заменяют требований настоящего приложения.

2 Диагностические тесты могут обеспечить значительные преимущества в достижении функциональной безопасности Э/Э/ПЭ СБЗС системы. Однако следует не усложнять тестирование, что может привести к увеличению трудностей при проведении действий по проверке, подтверждению соответствия, оценке функциональной безопасности, технической поддержке и модификации. Усложнение тестирования может также затруднить длительное поддержание функциональной безопасности Э/Э/ПЭ СБЗС системы.

При расчетах охвата диагностикой и путей его использования предполагается, что УО успешно работают в присутствии другого опасного повреждения, обнаруженного диагностическими тестами. Если это предположение не верно, то Э/Э/ПЭ СБЗС систему следует рассматривать как систему, действующую в режиме с высокой частотой запросов или с непрерывным запросом (см. 8.3.9.3, 8.3.6.3 и 8.3.6.4).

Примечания

1 Диагностическое тестирование, используемое для обнаружения опасных отказов внутри элемента, может быть проведено другим элементом внутри Э/Э/ПЭ СБЗС системы.

2 Диагностические тесты могут быть проведены непрерывно или периодически, в зависимости от диагностического испытательного интервала. Могут существовать ситуации или интервалы времени, когда запуск диагностического испытания невозможен из-за того, что тестируемая система находится в неблагоприятном состоянии. В этом случае преимущества вычислений не могут помочь при диагностических испытаниях.

Приложение Г
(обязательное)

Руководство по безопасности для применяемых изделий

Г.1 Основные положения

Цель руководства по безопасности для применяемых изделий (элементов системы) состоит в документальном оформлении информации, связанной с применяемым изделием, которая необходима для обеспечения интеграции применяемого изделия в связанную с безопасностью систему, или подсистему, или элемент в соответствии с требованиями настоящего стандарта.

Г.2 Содержание

Г.2.1 Руководство по безопасности должно определить функции применяемого изделия. Эти функции могут быть использованы для того, чтобы поддержать функцию безопасности системы, связанной с безопасностью, или функции в подсистеме или элементе. В спецификации должны быть ясно описаны и функции, и интерфейсы входа и выхода.

Для каждого применяемого изделия руководство по безопасности должно содержать:

- функциональную спецификацию выполняемых функций;
- идентификацию конфигурации АС и/или ПО применяемого изделия для обеспечения управления конфигурацией Э/Э/ПЭ СБЗС системы в соответствии с ГОСТ 34332.2—2017 (подраздел 6.2);
- ограничения на использование применяемого изделия и/или предположения, на которых основан анализ поведения или интенсивности отказов этого изделия.

Г.2.2 Для каждой функции руководство по безопасности должно содержать:

а) виды отказов применяемого изделия (в зависимости от поведения его выхода) из-за случайных отказов АС, приводящих к отказу функции и не обнаруженных диагностикой, внутренней для применяемого изделия;

б) предполагаемую интенсивность отказов для каждого вида отказов, приведенных в перечислении а);

в) виды отказов применяемого изделия (в зависимости от поведения его выходов) из-за случайных отказов АС, приводящих к отказу функции и обнаруженных диагностикой, внутренней для применяемого изделия;

г) виды отказов диагностик, внутренних для применяемого изделия (в зависимости от поведения его выхода), из-за случайных отказов АС, приводящих к отказу диагностик для обнаружения отказов функции;

д) предполагаемую интенсивность отказов для каждого вида отказов по перечислениям в) и г);

е) диагностический испытательный интервал для каждого вида отказов по перечислению в), которые обнаружены диагностикой, внутренней для применяемого изделия;

ж) выходы применяемого изделия, инициируемые внешними диагностиками для каждого вида отказов по перечислению в).

Примечание — Результаты внутренней диагностики могут быть использованы, чтобы применить дополнительные меры (технические/процедурные) к Э/Э/ПЭ СБЗС системе, подсистеме или элементу, чтобы обеспечить или поддержать безопасное состояние УО;

и) требования к любому периодическому испытанию и/или техническому обслуживанию;

к) для тех видов отказа указанной функции, которые обнаруживаются внешней диагностикой, должно быть предоставлено достаточное количество информации, чтобы облегчить разработку возможностей внешней диагностики. Информация должна включать в себя подробное описание видов отказов и их интенсивности;

л) отказоустойчивость АС;

м) классификацию типа А или Б той части применяемого изделия, которая обеспечивает выполнение функции (см. 8.3.4.2 и 8.3.4.3).

Примечание — Виды отказов могут быть классифицированы на безопасные или опасные, только если известно, как применяемое изделие применяется в опасных ситуациях УО. Например, если датчик будет применен так, что высокий уровень его выходного сигнала используется, чтобы сигнализировать об опасности УО (например, из-за высокого давления), то вид отказа, который предотвращает корректную индикацию опасности (например, выходной сигнал имеет постоянный низкий уровень), будет классифицирован как опасный, тогда как вид отказа, в результате которого выходной сигнал датчика имеет высокий уровень, будет классифицирован как безопасный. Это зависит от того, как сигнал датчика интерпретируется логикой системы, связанной с безопасностью, и поэтому датчик не может быть специфицирован без ограничения способа его применения;

н) кроме того, уровень охвата диагностикой, требуемый для применяемого изделия, может меняться от одного применения к другому в зависимости от степени влияния любых диагностик на логику системы или обработку внешнего сигнала, к которым может добавляться любая внутренняя диагностика применяемого изделия.

Из этого следует, что любая оценка отказоустойчивости АС или доли безопасных отказов может быть выполнена, если только на применение применяемого изделия накладываются ограничения. Эти ограничения не

определяются поставщиком применяемого изделия. Поэтому в руководство по безопасности не следует включать требования к отказоустойчивости АС или к доле безопасных отказов, или к любым другим характеристикам функциональной безопасности, которые зависят от знания о безопасных и опасных видах отказов, если ясно не определены основные предположения о соотношении безопасных и опасных видов отказов.

Г.2.3 Для каждой функции применяемого изделия, для которой возможны систематические отказы, руководство должно содержать:

- стойкость к систематическим отказам применяемого изделия или той части элемента, которая реализует функцию;
- любые указания или ограничения, связанные с применением применяемого изделия, реализующего рассматриваемую функцию, которые должны предотвратить систематические отказы применяемого изделия.

Примечание — Систематическая полнота безопасности, определяемая стойкостью к систематическим отказам, может быть достигнута, только если указания и ограничения соблюдаются. При их нарушении требование к систематической способности частично или полностью недействительно.

Г.2.4 Дополнительные требования к ПО применяемого изделия представлены в ГОСТ 34332.4—2021 (приложение Г, подпункт 7.4.2.12).

Библиография

[1] Технический регламент Таможенного союза ТР ТС 002/2011 — О безопасности высокоскоростного железнодорожного транспорта

[2] Технический регламент Таможенного союза ТР ТС 003/2011 — О безопасности инфраструктуры железнодорожного транспорта

[3] Технический регламент Таможенного союза ТР ТС 014/2011 — Безопасность автомобильных дорог

[4] IEC 61508 (все части) — Functional safety of electrical/electronic/programmable electronic safety-related systems (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью)

УДК 621.5:814.8:006.354 МКС 13.200 13.220 13.310 13.320 91.120.99 NEQ

Ключевые слова: системы, связанные с безопасностью зданий и сооружений; функциональная безопасность систем, связанных с безопасностью зданий и сооружений; полнота безопасности; уровни полноты безопасности; требования к системам; проектирование систем; реализация систем

Редактор *Е.В. Зубарева*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 28.05.2021. Подписано в печать 15.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 8,37. Уч.-изд. л. 7,57.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

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

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

В каком месте	Напечатано	Должно быть		
Предисловие. Таблица согласования	—	Казахстан	KZ	Госстандарт Республики Казахстан

(ИУС № 4 2022 г.)

gost.e-ecolog.ru