ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53195.3— 2009

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ СИСТЕМ

Часть 3

Требования к системам

Издание официальное

БЗ 12—2008/468

Москва
Стандартинформ
2010

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизации в Российской Федерации. Основные положения»

Сведения о стандарте

1 РАЗРАБОТАН Университетом комплексных систем безопасности и инженерного обеспечения

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 439 «Средства автоматизации и системы управления» при поддержке Технического комитета по стандартизации ТК 465 «Строительство»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 13 августа 2009 г. № 293-ст

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

- МЭК 61508-4:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины, определения, сокращения» (IEC 61508-4:1998 «Functional safety of electrical/ electronic/ programmable electronic safety-related systems — Part 4: Definitions and abbreviations», NEQ);
- МЭК 61508-1:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Требования к электрическим, электронным, программируемым системам, связанным с безопасностью» (IEC 61508-1:1998 «Functional safety of electrical/ electronic/ programmable electronic safety-related systems — Part 1: Requirements for electrical/ electronic/ programmable electronic safety-related systems», NEQ);
- Руководство ИСО/МЭК 51:1999 «Аспекты безопасности. Руководящие указания по включению их в стандарты» (ISO/IEC Guide 51:1999 «Safety aspects – Guidelines for their inclusion in standards», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2010

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 . . . 4
5 Требования . . . 4
5.1 Соответствие требованиям стандарта . . . 4
5.2 Требования к документации . . . 4
5.3 Требования к управлению функциональной безопасностью . . . 4
5.4 Требования к жизненному циклу Е/Е/РЕ СБЗС-систем . . . 4
5.5 Требования к функциональной безопасности Е/Е/РЕ СБЗС-систем . . . 5
5.6 Планирование подтверждения соответствия Е/Е/РЕ СБЗС-систем . . . 6
5.7 Проектирование и реализация Е/Е/РЕ СБЗС-систем . . . 7
5.8 Требования к полноте безопасности АС . . . 9
5.9 Требования по предотвращению отказов . . . 16
5.10 Требования по управлению систематическими отказами . . . 16
5.11 Требования к действиям системы при обнаружении отказов . . . 17
5.12 Требования к реализации Е/Е/РЕ СБЗС-систем . . . 18
5.13 Требования к передаче-приему данных . . . 20
5.14 Интеграция Е/Е/РЕ СБЗС-систем . . . 20
5.15 Процедуры эксплуатации и технического обслуживания систем . . . 21
5.16 Подтверждение соответствия Е/Е/РЕ СБЗС-систем требованиям безопасности . . . 22
5.17 Модификация Е/Е/РЕ СБЗС-систем . . . 23
5.18 Верификация Е/Е/РЕ СБЗС-систем . . . 23
6 Оценка функциональной безопасности . . . 25
Приложение А (справочное) Методы и средства управления отказами Е/Е/РЕ СБЗС-систем . . . 25
Приложение Б (справочное) Методы и средства по предотвращению систематических отказов на стадиях жизненного цикла Е/Е/РЕ СБЗС-систем . . . 39
Приложение В (справочное) Охват диагностикой и доля безопасных отказов . . . 47
Приложение Г (справочное) Состав и интеграция Е/Е/РЕ СБЗС-систем . . . 49
Приложение Д (справочное) Организация центров управления кризисными ситуациями и размещение аппаратуры Е/Е/РЕ СБЗС-систем . . . 51
Приложение Е (справочное) Применение антропометрических характеристик человека для расчетов аппаратных управления . . . 56
Библиография . . . 58

Введение

Современные здания и сооружения — объекты капитального строительства, представляющие собой сложные системы и включающие в свой состав систему конструкций и ряд систем в разных сочетаниях, в том числе инженерные системы жизнеобеспечения, реализации технологических процесссов, энерго-, ресурсосбережения, обеспечения безопасности и другие системы. Эти системы взаимодействуют друг с другом, с внешней и внутренней средами.

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 построены объекты и установлены системы.

Безопасность зданий и сооружений обеспечивается применением совокупности мер, мероприятий и средств снижения риска причинения вреда до уровня приемлемого риска и поддержания этого уровня в течение периода эксплуатации или использования этих объектов. К средствам снижения риска относятся связанные с безопасностью зданий и сооружений системы (СБЗС-системы). Эти системы, состоящие из электрических и/или электронных компонентов, и/или программируемых электронных компонентов, в течение многих лет используются для выполнения функций безопасности. Для решения задач обеспечения безопасности зданий и сооружений во все больших объемах используются программируемые электронные (т.е. компьютерные) СБЗС-системы.

Настоящий стандарт входит в комплекс стандартов с наименованием «Безопасность функциональная связанных с безопасностью зданий и сооружений систем» 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;

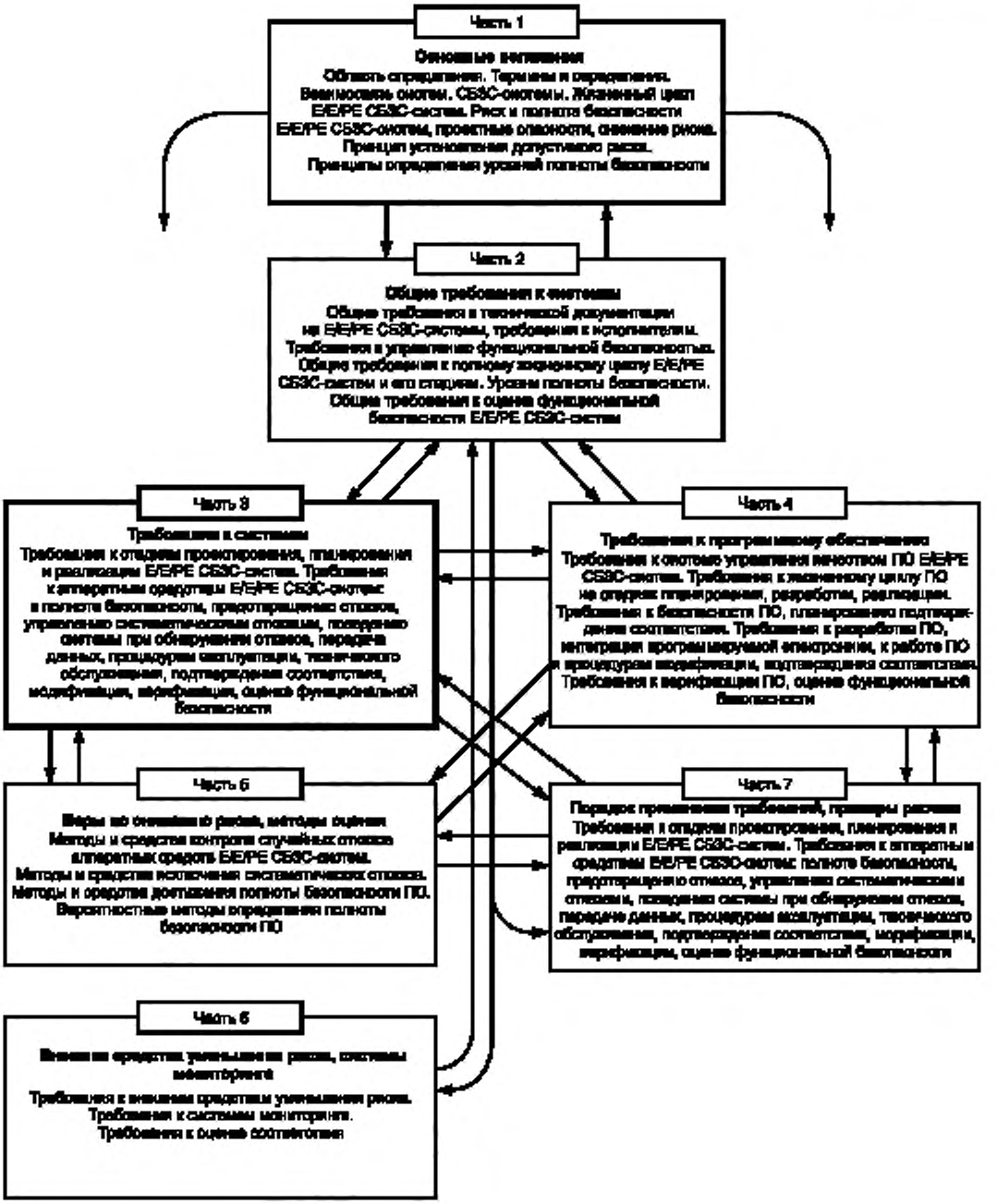
Часть 4. Требования к программному обеспечению;

Часть 5. Меры по снижению риска, методы анализа риска и оценки полноты безопасности;

Часть 6. Внешние средства уменьшения риска и системы мониторинга конструкций;

Часть 7. Порядок применения требований к системам и примеры расчетов.

Структура комплекса стандартов приведена ниже.


Часть 1
Основные положения
Область определения. Термины и определения.
Взаимосвязь систем. СБЗС-системы. Жизненный цикл
Е/Э/РЕ СБЗС-систем. Риск и полнота безопасности
Е/Э/РЕ СБЗС-систем, проектные опасности, снижение риска.
Принцип установления допустимого риска.
Принципы определения уровней полноты безопасности
Часть 2
Общие требования к системам
Общие требования к технической документации
на Е/Э/РЕ СБЗС-системы, требования к исполнителям.
Требования к управлению функциональной безопасностью.
Общие требования к полному жизненному циклу Е/Э/РЕ
СБЗС-систем и его стадиям. Уровни полноты безопасности.
Общие требования к оценке функциональной
безопасности Е/Э/РЕ СБЗС-систем
Часть 3
Требования к системам
Требования к стадиям проектирования, планирования
и реализации Е/Э/РЕ СБЗС-систем. Требования
к аппаратным средствам Е/Э/РЕ СБЗС-систем
в полноте безопасности, предотвращению отказов,
управлению систематическими отказами, поведению
системы при обнаружении отказов, передаче
данных, процедурам эксплуатации, технического
обслуживания, подтверждения соответствия,
модификации, верификации, оценке функциональной
безопасности
Часть 4
Требования к программному обеспечению
Требования к системе управления жизнетом ПО Е/Э/РЕ
СБЗС-систем. Требования к жизненному циклу ПО
на стадиях планирования, разработки, реализации.
Требования к безопасности ПО, планированию подтверж-
дения соответствия. Требования к разработке ПО,
интеграции программируемой электроники, к работе ПО
и процедурам верификации, подтверждения соответствия.
Требования к верификации ПО, оценке функциональной
безопасности
Часть 5
Меры по снижению риска, методы оценки
Методы и средства контроля случайных отказов
аппаратных средств Е/Э/РЕ СБЗС-систем.
Методы и средства исключения систематических отказов.
Методы и средства достижения полноты безопасности ПО.
Вероятностные методы определения полноты
безопасности ПО
Часть 7
Порядок применения требований, примеры расчета
Требования к стадиям проектирования, планирования и
реализации Е/Э/РЕ СБЗС-систем. Требования к аппаратным
средствам Е/Э/РЕ СБЗС-систем: полноте безопасности,
предотвращению отказов, управлению систематическими
отказами, поведению системы при обнаружении отказов,
передаче данных, процедурам эксплуатации, технического
обслуживания, подтверждения соответствия, модификации,
верификации, оценке функциональной безопасности
Часть 6
Внешние средства уменьшения риска, системы
мониторинга
Требования к внешним средствам уменьшения риска.
Требования к системам мониторинга.
Требования к оценке соответствия

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ СИСТЕМ

Часть 3

Требования к системам

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

Дата введения — 2010 — 06 — 01

1 Область применения

Настоящий стандарт

- применяют совместно с ГОСТ Р 53195.1 и ГОСТ Р 53195.2;
- применяют к электрическим, электронным, программируемым электронным связанным с безопасностью зданий и сооружений системам (далее — E/E/PE СБЗС-системам), а также к системам, подсистемам и компонентам внутри E/E/PE СБЗС-систем, которые содержат хотя бы один электрический, электронный или программируемый компонент;
- устанавливает требования к функциональной безопасности аппаратных средств (далее — АС) E/E/PE СБЗС-систем на стадиях проектирования, планирования и реализации E/E/PE СБЗС-систем;
- устанавливает требования к действиям и процедурам, которые должны быть выполнены на этих стадиях для обеспечения функциональной безопасности E/E/PE СБЗС-систем, а также оценки и подтверждения соответствия на стадиях их жизненного цикла, за исключением требований к программному обеспечению (далее — ПО), которые должны быть установлены в нормативных документах на ПО;
- устанавливает минимальный состав информации, необходимой для установки, ввода в эксплуатацию и подтверждения соответствия E/E/PE СБЗС-систем требованиям безопасности.

Примечание — Области применения настоящего стандарта и нормативных документов на ПО взаимосвязаны. Эта взаимосвязь (рисунок 1) должна учитываться при применении настоящего стандарта. Настоящий стандарт должен применяться совместно с нормативными документами на ПО.

Издание официальное

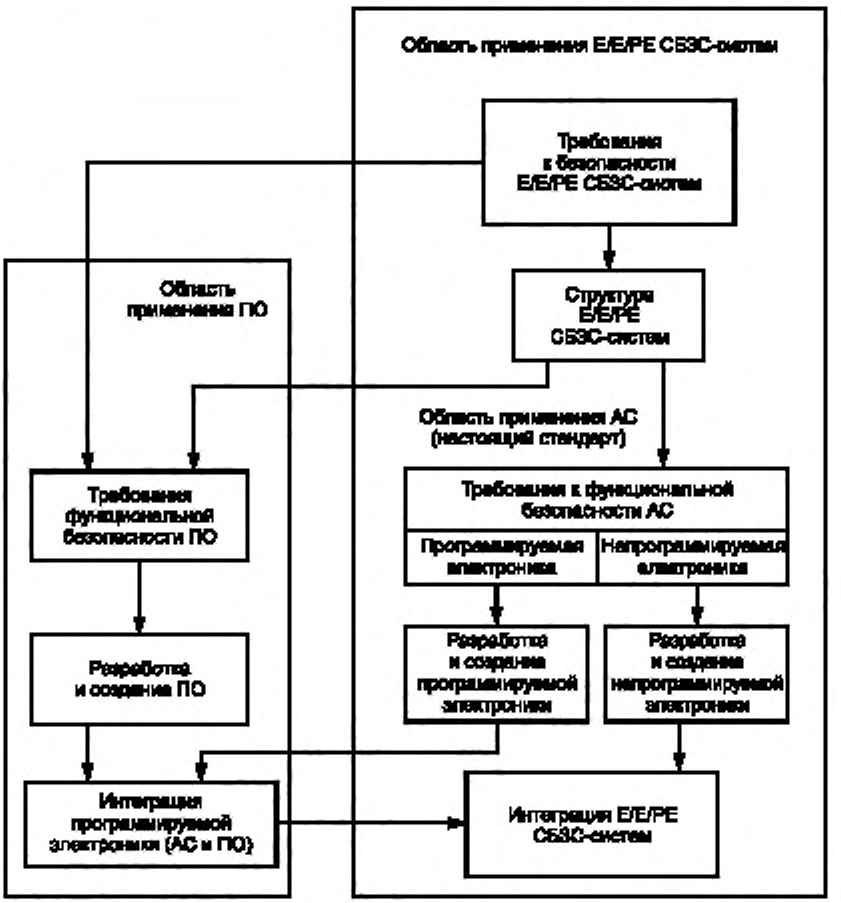


Рисунок 1 — Взаимосвязь областей применения АС и ПО

2 Нормативные ссылки

2.1 В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 52507—2005 Совместимость технических средств электромагнитная. Электронные схемы управления жилых помещений и зданий. Требования и методы испытаний

ГОСТ Р 53195.1—2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения

ГОСТ Р 53195.2—2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 2. Общие требования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 53195.1 и ГОСТ Р 53195.2, а также следующие термины с соответствующими определениями:

3.1 **автоматизированное рабочее место;** АРМ (local control station): Рабочее место оператора со средствами контроля и управления автоматизированным оборудованием.

3.2 **аппаратная управления** (control room): Центральный функциональный объект центра управления кризисными ситуациями вместе с его физической структурой, в котором размещаются автоматизированное рабочее место или автоматизированные рабочие места со средствами централизованного контроля и управления автоматизированным оборудованием.

3.3 **время безопасности процесса:** Интервал времени между опасным отказом и возникновением опасного события в случае невыполнения функции безопасности.

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

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 **комплект помещений управления** (control suite): Группа функционально связанных помещений (таких как офисы, технические аппаратные, зоны отдыха, помещения для тренинга и обучения персонала, сопряженных с аппаратной управления и включающая ее), которые обеспечивают реализацию функций эксплуатации и обслуживания аппаратной управления.

3.7 **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.

3.8 **модуль** (module): Элемент конструкции или сформированный набор подходящих друг к другу элементов конструкций в зданиях и сооружениях, или стандартная программа, дискретный компонент, или сформированный функциональный набор подходящих друг к другу стандартных программ или дискретных компонентов в электрической, электронной, программируемой электронной связанной с безопасностью зданий и сооружений системе.

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

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

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

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

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

3.14 **систематический отказ** (systematic failure): Отказ системы, аппаратного средства или программного обеспечения, связанный с некоторой повторяющейся причиной процесса проектирования, производства, монтажа или пусконаладки, и который может быть изменен только путем модификации этих процессов.

3.15 **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.

3.16 **тестовая программа** (test harness): Программный продукт, предназначенный для имитации среды, в которой должно действовать разрабатываемое программное обеспечение или аппаратное средство, осуществляемой путем передачи тестовых данных в программу и регистрации ответов.

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

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

3.19 **центр управления кризисными ситуациями,** ЦУКС (control centre): Совокупность функционально и территориально объединенных аппаратных управления, комплектов помещений управления и автоматизированных рабочих мест с соответствующим оборудованием для обеспечения централизованного контроля и управления кризисными ситуациями.

4 Обозначения и сокращения

В настоящем стандарте приняты обозначения и сокращения, приведенные ниже:

АРМ — автоматизированное рабочее место;
АС — аппаратное(ые) средство(а);
ОЗУ — оперативное запоминающее устройство;
ПЗУ — программируемое запоминающее устройство;
ПО — программное обеспечение;
СБЗС-система — связанная с безопасностью зданий и сооружений система;
УО — управляемое оборудование;
ЦУКС — центр управления кризисными ситуациями;
E/E/PE — электрическая и/или электронная, и/или программируемая электронная (в отношении системы);
PE — программируемая электроника;
SIL — обозначение уровня полноты безопасности;
NP — непрограммируемое устройство.

5 Требования

5.1 Соответствие требованиям стандарта

Признание соответствия E/E/PE СБЗС-систем требованиям настоящего стандарта — по ГОСТ Р 53195.2 (5.1).

Требования к конкретным E/E/PE СБЗС-системам должны быть установлены с учетом: природных факторов, характера опасностей, необходимого снижения риска и последствий, требуемого уровня полноты безопасности, сложности системы, физической среды применения, новизны разработки.

5.2 Требования к документации

Требования к документации E/E/PE СБЗС-систем — по ГОСТ Р 53195.2 (5.2).

5.3 Требования к управлению функциональной безопасностью

Требования к управлению функциональной безопасностью E/E/PE СБЗС-систем — по ГОСТ Р 53195.2 (раздел 6).

5.4 Требования к жизненному циклу E/E/PE СБЗС-систем

5.4.1 Для стадий проектирования, планирования и реализации жизненного цикла E/E/PE СБЗС-систем цели, которые должны быть достигнуты, требования к АС этих систем и действия, необходимые для выполнения этих требований и достижения целей, устанавливаются настоящим стандартом.

Цели и требования для полного жизненного цикла E/E/PE СБЗС-систем установлены в ГОСТ Р 53195.2.

Цели и требования к программному обеспечению (далее — ПО) E/E/PE СБЗС-систем должны быть установлены в нормативных документах на ПО.

5.4.2 Для каждой стадии жизненного цикла могут быть установлены необходимые промежуточные стадии (рисунок 2) с указанием для каждой из них области применения, входных данных (входов) и результатов (выходов) стадии.

Промежуточные стадии должны быть установлены на стадии планирования функциональной безопасности (ГОСТ Р 53195.2, раздел 6) и на них должны быть достигнуты все цели и выполнены все требования настоящего стандарта.

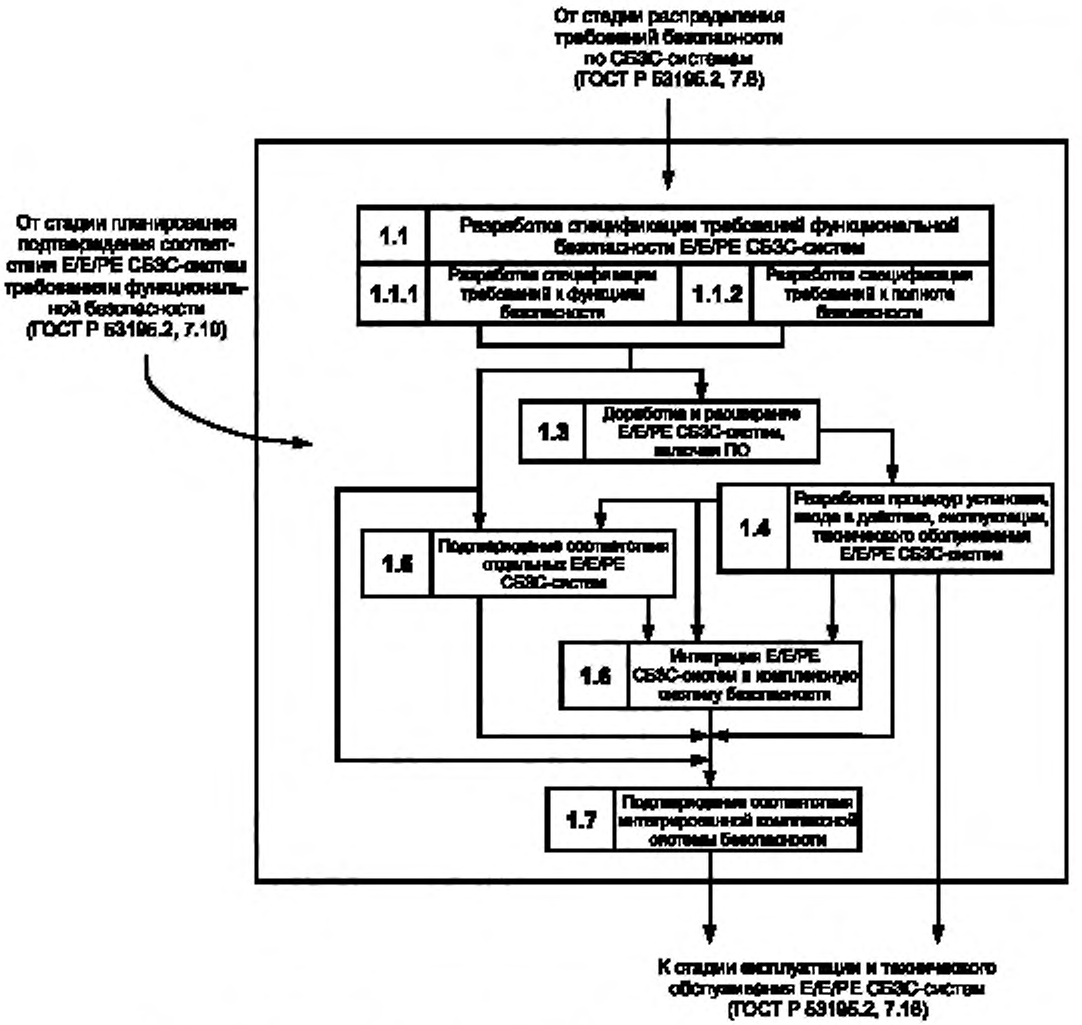


Рисунок 2 — Детализация промежуточных стадий жизненного цикла E/E/PE СБЗС-систем

5.4.3 Процедуры управления функциональной безопасностью по ГОСТ Р 53195.2 (раздел 6) должны выполняться параллельно рассматриваемым стадиям жизненного цикла E/E/PE СБЗС-систем.

5.4.4 Входные данные каждой стадии жизненного цикла E/E/PE СБЗС-систем должны соответствовать определенным для этих стадий целям и требованиям (см. 5.5—5.16). Результаты каждой стадии должны быть документированы лицами, ответственными за обеспечение функциональной безопасности на соответствующей стадии жизненного цикла систем.

5.5 Требования к функциональной безопасности E/E/PE СБЗС-систем

5.5.1 Для каждой E/E/PE СБЗС-системы на стадии проектирования должна быть разработана спецификация требований к функциональной безопасности, в которой устанавливаются требования к функциям безопасности и требования к полноте безопасности для достижения необходимой функциональной безопасности АС системы.

5.5.2 Спецификация требований к функциональной безопасности E/E/PE СБЗС-систем должна формироваться на основании распределения требований безопасности в соответствии с 7.6 ГОСТ Р 53195.2 и с учетом требований, определенных в ходе планирования функциональной безопасности в соответствии с требованиями раздела 6 ГОСТ Р 53195.2.

Примечание — Не рекомендуется выполнение E/E/PE СБЗС-системой каких-либо функций, не связанных с безопасностью.

5.5.3 Требования к функциональной безопасности должны быть реализуемыми, поддающимися проверке и пригодными для тестирования. Они должны быть документированы.

5.5.4 Спецификация требований к функциям безопасности E/E/PE СБЗС-систем должна:

а) содержать описание всех функций безопасности, необходимых для достижения функциональной безопасности, которое должно:

- устанавливать конкретные требования, достаточные для проектирования и реализации E/E/PE СБЗС-систем;
- включать в свой состав перечень мер по достижению и поддержанию безопасного состояния управляемого оборудования (далее — УО);
- определять, требуется ли непрерывное управление УО и чем обеспечивается достижение безопасного состояния УО;
- определять, к какому режиму относится функция безопасности E/E/PE СБЗС-системы (к режиму с низкой частотой запросов либо к режиму с высокой частотой запросов или с непрерывным запросом);

б) содержать характеристики производительности и время реакции системы;

в) содержать сведения об интерфейсах оператора-системы, необходимых для достижения требуемой функциональной безопасности;

г) содержать сведения о стыках E/E/PE СБЗС-систем с любыми другими системами (внутренними, внешними), с УО;

д) содержать описание всех используемых режимов работы УО, в том числе для:

- подготовки к эксплуатации, включая монтаж и наладку;
- обучения операторов, пуска систем в действие в автоматическом, полуавтоматическом, ручном и стационарном рабочих режимах работы;
- стационарного нерабочего режима, переустановки, останова, технического обслуживания;
- работы при предсказуемых нештатных условиях;

е) содержать подробное описание всех вариантов поведения E/E/PE СБЗС-систем, в том числе при отказе, и необходимой реакции на него (например тревожный сигнал, автоматический останов и т.п.);

ж) содержать описание значимости всех взаимодействий АС и ПО и любых необходимых ограничений, которые должны быть идентифицированы и документированы;

и) содержать предельные и ограничивающие условия для работы E/E/PE СБЗС-систем и связанных с ними систем, например временные ограничения;

к) содержать любые специфические требования, связанные с запуском или перезапуском E/E/PE СБЗС-систем.

5.5.5 Спецификация требований к полноте безопасности E/E/PE СБЗС-систем должна включать в свой состав:

а) уровень полноты безопасности для каждой функции безопасности и, при необходимости, значение требуемой целевой величины отказов в выполнении функции безопасности;

б) режим работы (с низкой частотой запросов либо с высокой частотой запросов или с непрерывным запросом) каждой функции безопасности;

в) требования, ограничения, функции и возможность проведения периодических испытаний E/E/PE СБЗС-систем;

г) экстремальные значения всех условий окружающей среды в течение жизненного цикла E/E/PE СБЗС-систем, включая испытания, установку, ввод в эксплуатацию, эксплуатацию и техническое обслуживание;

д) пределы электромагнитной устойчивости, необходимые для достижения электромагнитной совместимости по ГОСТ Р 52507.

Примечание — При разработке спецификации требований безопасности E/E/PE СБЗС-систем могут быть использованы методы и средства, приведенные в таблице Б.1 приложения Б.

5.6 Планирование подтверждения соответствия E/E/PE СБЗС-систем

5.6.1 Подтверждение соответствия АС E/E/PE СБЗС-систем установленным требованиям должно быть заранее запланировано лицом, ответственным за представление АС для подтверждения соответствия.

5.6.2 План должен содержать последовательность процедурных и технических шагов, необходимых для подтверждения соответствия АС E/E/PE СБЗС-систем предъявляемым к ним требованиям функциональной безопасности в соответствии с 5.5.

Примечание — Требования к планированию подтверждения соответствия ПО должны быть установлены в НД на ПО.

5.6.3 План подтверждения соответствия E/E/PE СБЗС-систем должен содержать:

а) требования, установленные в спецификации к функциональной безопасности E/E/PE СБЗС-систем;

б) процедуры и критерии («прошла»/«не прошла» система испытания), применяемые для подтверждения правильности выполнения каждой функции безопасности;

в) процедуры и критерии («прошла»/«не прошла» система испытания), применяемые для подтверждения соответствия требованиям полноты безопасности каждой функции безопасности;

г) условия окружающей среды, при которых проводят испытания, необходимые средства испытаний и испытательное оборудование (в том числе план калибровки и поверки этих средств и оборудования);

д) методы оценки с их обоснованием;

е) процедуры испытаний и критерии, применяемые для подтверждения соответствия заданных пределов электромагнитной устойчивости (в соответствии с ГОСТ Р 52507);

ж) меры по устранению подтвержденных отказов.

5.7 Проектирование и реализация E/E/PE СБЗС-систем

5.7.1 Проектирование и реализация E/E/PE СБЗС-систем должны осуществляться в соответствии с требованиями, установленными для функций безопасности и для полноты безопасности в 5.5, и с учетом требований 5.7.2—5.7.15.

5.7.2 Проектирование E/E/PE СБЗС-систем, включая полные структуры АС и ПО, в том числе сенсорные и исполнительные устройства, программируемую электронику, встроенное программное обеспечение, «зашитое» в программируемые запоминающие устройства (ПЗУ), прикладное ПО и т.п. (рисунок 3), должно осуществляться таким образом, чтобы удовлетворялись требования:

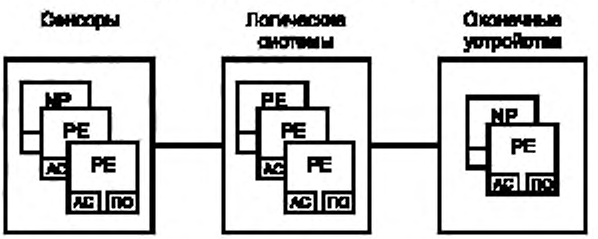
а) к полноте безопасности АС, в том числе:

- требования к структурным ограничениям на полноту безопасности АС (5.8);
- требования к вероятности опасных случайных отказов АС (5.8.2);

б) к полноте безопасности по отношению к систематическим отказам:

- требования по предотвращению отказов (5.9) и требования по управлению систематическими отказами (5.10) или
- требования к подтверждению того, что оборудование «проверено в эксплуатации» (5.12.5—5.12.12);

в) к действиям системы при обнаружении ошибок и отказов (5.11).



Обозначения:
PE — программируемая электроника; АС — аппаратное средство;
NP — непрограммируемое устройство, ПО — программное обеспечение; ПЗУ — программируемое запоминающее устройство

Структура программируемой электроники		
Структура аппаратных средств PE	Структура программного обеспечения PE (структура ПО включает встроенные в ПЗУ ПО и прикладные программы)	
Общие и конкретные особенности АС PE, например: - встроенные устройства диагностического тестирования; - избыточные процессоры; - сдвоенные платы ввода/вывода	ПО, встроенное в ПЗУ PE, например: - коммуникационные драйверы; - ПО обработки отказов; - исполнительное ПО	Прикладное ПО PE, например: - ПО функций ввода/вывода; - ПО обработки отказов; - ПО вторичных функций (например, контроля сенсора, если оно не обеспечено как сервис встроенного в ПЗУ ПО)

Рисунок 3 — Взаимосвязь между структурами АС и ПО программируемой электроники

5.7.3 Для установления необходимой полноты безопасности E/E/PE СБЗС-систем должен быть применен метод проектирования, обеспечивающий достижение уровня полноты безопасности АС и полноты безопасности по отношению к систематическим отказам, в ходе реализации которого:

- определяют требуемый уровень полноты безопасности функций безопасности (по ГОСТ Р 53195.2);
- устанавливают полноту безопасности АС равной полноте безопасности по отношению к систематическим отказам и равной уровню полноты безопасности (5.10);
- для установленной полноты безопасности АС определяют структуру, соответствующую ограничениям на структуру (5.8.1), и предоставляют доказательства соответствия вероятности отказов функций безопасности из-за случайных отказов аппаратных средств требуемым целевым значениям отказов (5.8.2);
- для установленной полноты безопасности по отношению к систематическим отказам выявляют особенности проектирования, которые приводят к систематическим отказам в реальной работе (5.10) или подтверждают соответствие требованиям «проверено при эксплуатации» (5.12.5—5.12.12);
- для полноты безопасности в отношении систематических отказов определяют методы и средства, предотвращающие систематические отказы в процессе проектирования и реализации (5.9), или предоставляют доказательства соответствия требованиям «проверено при эксплуатации» (5.12.5—5.12.12).

Примечание — Требования к структуре ПО, тестирования при интеграции ПО, связанные с ними требования к интеграции программируемой электроники должны быть установлены в нормативных документах на ПО.

5.7.4 Во всех случаях, когда E/E/PE СБЗС-система реализует функции безопасности, а также функции, не относящиеся к безопасности, все АС и ПО должны рассматриваться 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 становится причиной отказа функций, связанных с безопасностью).

Достаточная независимость этих функций доказывается предоставлением доказательств того, что вероятность зависимого отказа между компонентами, не относящимися к безопасности, и компонентами, связанными с безопасностью, достаточно низка по сравнению с самым высоким уровнем полноты безопасности, который относится к выполняемым функциями безопасности.

5.7.5 Функции, связанные с безопасностью, должны быть, по возможности, отделены от функций, не относящихся к безопасности.

Примечание — Совмещение этих функций, допускаемое настоящим стандартом, может привести к значительным сложностям при выполнении работ в процессе жизненного цикла E/E/PE-системы (например при проектировании, подтверждении соответствия, оценке функциональной безопасности и техническом обслуживании).

5.7.6 Требования к АС и ПО E/E/PE СБЗС-системы должны определяться уровнем полноты безопасности при выполнении ими функций безопасности с самым высоким уровнем полноты безопасности, если не будет доказано, что выполнение функций безопасности для различных уровней полноты безопасности достаточно независимо.

Достаточная независимость выполнения функций безопасности доказывается предоставлением доказательств того, что вероятность зависимого отказа компонентов, выполняющих функции безопасности для различных уровней полноты безопасности, достаточно низка по сравнению с самым высоким уровнем полноты безопасности, относящимся к рассматриваемым функциям безопасности.

5.7.7 В случае выполнения E/E/PE СБЗС-системой нескольких функций безопасности должна быть рассмотрена возможность возникновения отказа в выполнении нескольких функций безопасности из-за единственной ошибки. Требования к АС и ПО в этом случае допускается устанавливать, применяя уровень полноты безопасности более высокий, чем уровень, относящийся к выполнению любой из функций безопасности, в зависимости от риска, связанного с таким отказом.

5.7.8 Если функции безопасности должны быть независимыми в соответствии с 5.7.4 и 5.7.6, то в проектной документации должно быть приведено обоснование метода достижения независимости функций.

5.7.9 При разработке E/E/PE СБЗС-систем должна быть проверена корректность требований к ПО и АС в их сочетании: требования к функциям безопасности, требования к полноте безопасности E/E/PE СБЗС-системы и требования к интерфейсу между оборудованием и оператором. Результаты проверки должны быть отражены в проектной документации.

5.7.10 В проектной документации должно быть приведено обоснование методов и средств, принятых при проектировании для достижения необходимого уровня полноты безопасности в течение стадий жизненного цикла безопасности E/E/PE СБЗС-системы, а также методов и средств, выбранных для формирования интегрированного набора компонентов системы, обеспечивающего требуемый уровень полноты безопасности.

Примечание — Альтернативой такому обоснованию могут служить результаты независимой проверки (аудита) с письменным подтверждением правильности выбора E/E/PE СБЗС-системы и компонентов (включая сенсоры, датчики и т.д.).

5.7.11 Основные взаимодействия АС и ПО, предусмотренные в процессе проектирования и реализации E/E/PE СБЗС-системы, должны быть идентифицированы, оценены и отражены в проектной документации.

5.7.12 В состав проекта на сложную E/E/PE СБЗС-систему, в том числе комплексную систему безопасности, должны быть включены также индивидуальные проекты (части проекта) на более простые составляющие системы (подсистемы). Для каждой из них должен быть предусмотрен набор тестов для интеграции (5.14).

Примечания

1 Конкретная подсистема может состоять из одного компонента или группы компонентов. Полная E/E/PE СБЗС-система может состоять из множества отдельных подсистем, которые при их объединении обеспечивают выполнение предусмотренной функции безопасности. Подсистема может иметь несколько каналов.

2 Следует избегать избыточных функциональных возможностей, пропускной способности или производительности подсистем, если не может быть обеспечена защита от выполнения ими непредусмотренных функций.

5.7.13 Если подсистема имеет многоканальный выход, должно быть определено наличие комбинаций выходных состояний, которые могут быть вызваны отказом самой E/E/PE СБЗС-системы, способных непосредственно вызвать событие опасного отказа (ГОСТ Р 53195.2, 7.4). При наличии таких комбинаций их предотвращение должно быть расценено как функции безопасности, действующие в режиме с высокой частотой запросов или с непрерывным запросом.

5.7.14 Для любых компонентов E/E/PE СБЗС-системы в максимальной степени должно быть ограничено их использование в предельных режимах работы или предельных условиях окружающей среды. Обоснование работы на пределах любых компонентов должно быть документировано (ГОСТ Р 53195.2, раздел 5).

5.7.15 При ограничении допустимых значений должен использоваться коэффициент ограничения, равный 0,67.

5.8 Требования к полноте безопасности АС

5.8.1 Структурные ограничения полноты безопасности АС

5.8.1.1 Наиболее высокий уровень полноты безопасности функции безопасности, выполняемой E/E/PE СБЗС-системой, должен ограничиваться устойчивостью АС к отказам и составляющей безопасных отказов подсистем, которые выполняют эту функцию безопасности (приложение В).

E/E/PE СБЗС-подсистемы как составляющие более сложных систем подразделяют по этим признакам на подсистемы типов А и Б.

5.8.1.2 Конкретная E/E/PE СБЗС-подсистема (5.7.12, примечание 1) может быть отнесена к типу А, если для ее компонентов, необходимых для реализации функции безопасности, одновременно выполняются следующие условия:

а) определены виды отказов всех составляющих компонентов;

б) может быть полностью определено поведение системы в условиях отказа;

в) имеются достоверные эксплуатационные данные, показывающие, что частота диагностических проверок, требуемых для обнаруженных отказов и необнаруженных опасных отказов, обеспечивается.

5.8.1.3 Конкретная подсистема должна быть отнесена к типу Б, если для ее компонентов, необходимых для реализации функции безопасности, выполняется одно из условий:

а) не определен вид отказа, по крайней мере, одного составляющего компонента;

б) не может быть полностью определено поведение подсистемы в условиях отказа;

в) нет достоверных эксплуатационных данных по подтверждению требований для частот обнаруженных отказов и необнаруженных опасных отказов (5.12.3 и 5.12.4).

Примечание — Подсистема должна быть отнесена к подсистеме типа Б, если хотя бы один из компонентов подсистемы соответствует условиям, установленным для системы типа Б (см. также 5.7.12, примечание 1).

5.8.1.4 Наибольший уровень полноты безопасности, который может быть установлен для функции безопасности при использовании подсистем, с учетом устойчивости АС к отказам и составляющей безопасных отказов этих подсистем, должен быть таким, как указано в таблицах 1 и 2.

Требования таблиц 1 и 2 должны применяться к каждой подсистеме, выполняющей функцию безопасности, и к каждой части E/E/PE СБЗС-системы. Применяемость таблиц определяют на основании 5.8.1.2 — 5.8.1.4. Самый высокий уровень полноты безопасности, который может быть установлен для функции безопасности по запросу, определяют на основании 5.8.1.5 и 5.8.1.6.

При использовании таблиц 1 и 2 должны быть учтены следующие условия и допущения:

а) устойчивость АС к отказам N означает, что отказ N + 1 может привести к невыполнению функции безопасности;

Примечание — При определении устойчивости АС к отказам не должны учитываться средства, которые могут управлять влиянием ошибок, например средства диагностики;

Таблица 1 — Зависимость полноты безопасности АС СБЗС-подсистем типа А 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
До 60	SIL1	SIL2	SIL3
От 60 до 90	SIL2	SIL3	SIL4
От 90 до 99	SIL3	SIL4	SIL4
99 и св.	SIL3	SIL4	SIL4

Примечания
1 Расчет доли безопасных отказов — в приложении В.
2 Уровни полноты безопасности SIL1—SIL4 — по ГОСТ Р 53195.2 (7.6.12).

Таблица 2 — 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
До 60	Не оговаривается	SIL1	SIL2
От 60 до 90	SIL1	SIL2	SIL3
От 90 до 99	SIL2	SIL3	SIL4
99 и св.	SIL2	SIL4	SIL4

Примечания
1 Расчет доли безопасных отказов — в приложении В.
2 Уровни полноты безопасности SIL1—SIL4 — по ГОСТ Р 53195.2 (7.6.12).

б) если одна ошибка непосредственно приводит к одной или более последующим ошибкам, они должны быть учтены как одиночная ошибка;

в) при определении устойчивости к отказам часть ошибок может быть исключена, если вероятность их возникновения очень мала по сравнению с требованиями к полноте безопасности подсистемы. Любые исключения ошибок должны быть обоснованы и документированы [см. примечание 3 к перечислению г)];

г) доля безопасных отказов подсистемы должна определяться, как отношение суммы средних частот безопасных отказов и опасных отказов, обнаруженных тестами, к полной средней частоте отказов подсистемы (см. приложение В).

Примечания

1 Для получения достаточно устойчивой к отказам структуры подсистемы, с учетом уровня ее сложности, должны быть использованы структурные ограничения. Уровень полноты безопасности E/E/PE СБЗС-системы, полученный в результате учета требований настоящего пункта, — максимальный из заявленных.

2 Структура и подсистема, сформированные для обеспечения соответствия требованиям устойчивости АС к отказам, должны быть такими, какие обычно используются в режиме эксплуатации. Требования устойчивости к

отказам могут быть снижены, если E/E/PE СБЗС-система восстанавливается, находясь под внешним управлением основного оборудования. В этом случае основные параметры подсистемы, связанные с любым ослаблением требований, должны быть предварительно оценены (например среднее время восстановления по сравнению с вероятными интервалами времени между запросами).

3 Если некоторый компонент системы имеет очень низкую вероятность отказа, благодаря присущим ему свойствам, (например механический соединитель привода), то нет необходимости рассматривать на основе устойчивости АС к отказам ограничение полноты безопасности любой функции безопасности, для реализации которой используется этот компонент.

5.8.1.5 Структурные ограничения по доле безопасных отказов (см. таблицу 1 или таблицу 2) должны применяться к каждой подсистеме, выполняющей функцию безопасности так, чтобы:

а) достигались требования устойчивости АС к отказам для полной E/E/PE СБЗС-системы;

б) для любой подсистемы типа А, составляющей часть E/E/PE СБЗС-системы, применялись требования таблицы 1.

Примечание — Если E/E/PE СБЗС-система содержит только подсистемы типа А, то требования, приведенные в таблице 1, следует применять к полной E/E/PE СБЗС-системе;

в) для любой подсистемы типа Б, составляющей часть полной E/E/PE СБЗС-системы, применялись требования таблицы 2.

Примечание — Если E/E/PE СБЗС-система содержит только подсистемы типа Б, то требования, приведенные в таблице 2, следует применять к полной E/E/PE СБЗС-системе;

г) к E/E/PE СБЗС-системам, содержащим подсистемы типов А и Б, применялись требования таблиц 1 и 2.

5.8.1.6 В E/E/PE СБЗС-системах, в которых функция безопасности реализуется одноканальной структурой (рисунок 4), максимальный уровень полноты безопасности АС, который может быть достигнут для функции безопасности, должен определяться подсистемой АС с наименьшим требованием безопасности АС, определяемым по таблицам 1 и 2.



Примечание — E/E/PE СБЗС-система, представляющая собой объединение подсистем, включающих все элементы (от сенсоров до исполнительных устройств), выполняющих функцию безопасности, например, функцию пожарной сигнализации, является полной E/E/PE СБЗС-системой.

Рисунок 4 — Пример ограничения полноты безопасности АС для одноканальной структуры E/E/PE-системы, реализующей функцию безопасности

Пример — Система, в которой реализована конкретная функция безопасности, выполнена по одноканальной структуре, состоящей из подсистем 1, 2 и 3, типы которых указаны на рисунке 4, и эти подсистемы удовлетворяют требованиям таблиц 1 и 2 следующим образом:

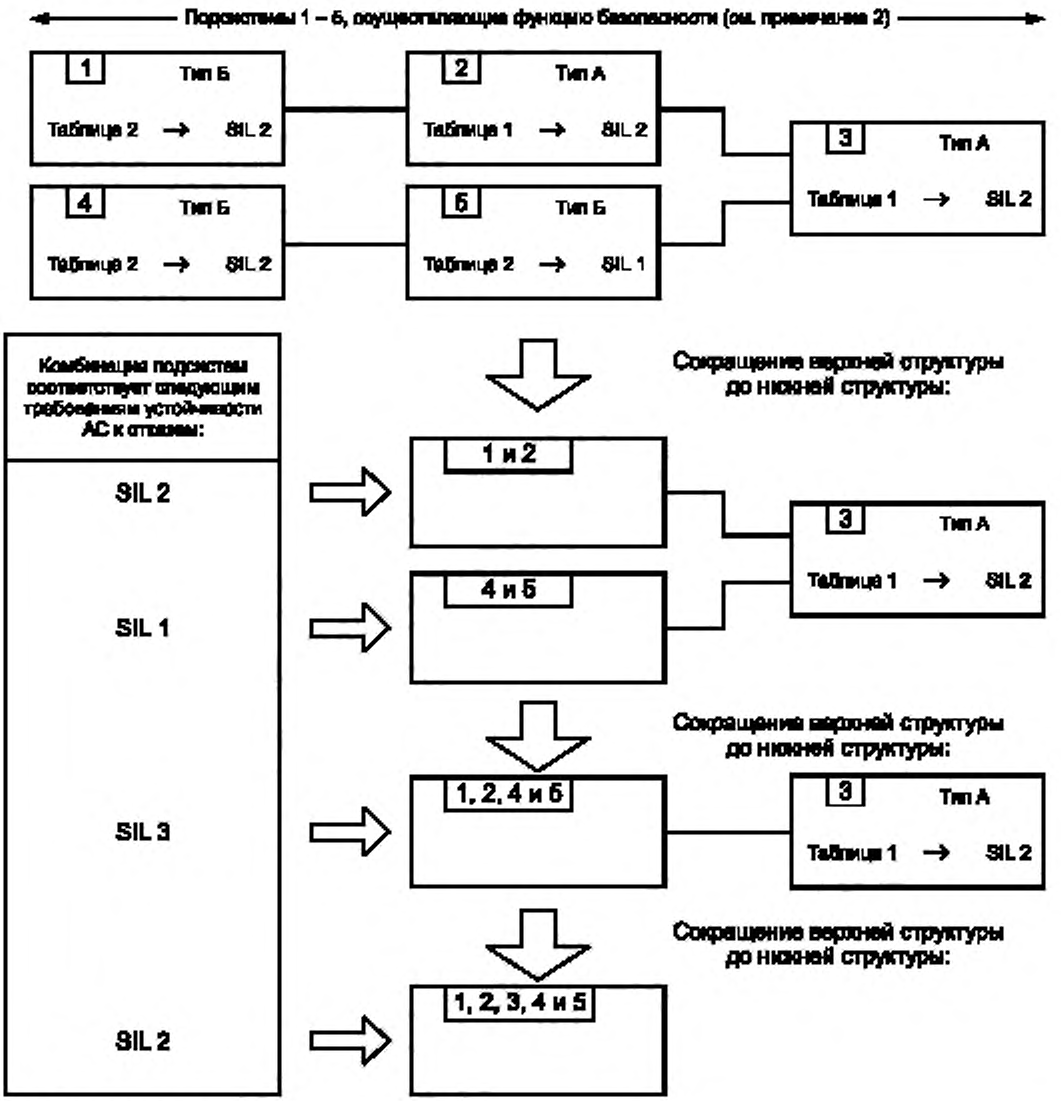
- для подсистемы 1 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL1;

- для подсистемы 2 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL2;

- для подсистемы 3 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL1.

Для этой структуры каждая из подсистем 1 и 3 имеет уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам, равный SIL1, а подсистема 2 имеет уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам, равный SIL2. Поэтому подсистемы 1 и 3 ограничивают уровень полноты безопасности, который может потребоваться для соблюдения устойчивости АС к отказам для рассматриваемой функции безопасности, до значения SIL1.

5.8.1.7 В E/E/PE СБЗС-системах, в которых функция безопасности реализуется многоканальной структурой (рисунок 5), максимальный уровень полноты безопасности, достигаемый для рассматриваемой функции безопасности, должен быть определен путем:



Примечания

1 Подсистемы 1, 2 и подсистемы 4, 5 имеют одинаковые функциональные возможности в отношении функции безопасности и обеспечивают раздельные входы в подсистему 3.

2 Подсистемы, включающие все элементы (от сенсоров до исполнительных устройств), выполняющие функцию безопасности, например, функцию пожарной сигнализации, образуют полную E/E/PE СБЗС-систему.

Рисунок 5 — Пример ограничения полноты безопасности АС для многоканальной структуры E/E/PE-системы, реализующей функцию безопасности

а) оценки каждой подсистемы в соответствии с требованиями, представленными в таблицах 1 и 2;

б) группирования подсистем в комбинации;

в) последующего анализа этих комбинаций для определения полного уровня полноты безопасности АС.

Пример — Структура, в которой реализуется конкретная функция безопасности, образована либо комбинацией подсистем 1, 2 и 3, либо комбинацией подсистем 4, 5 и 3, (см. рисунок 6). Комбинация подсистем 1 и 2 и комбинация подсистем 4 и 5 имеют одинаковые функциональные возможности в отношении функции безопасности и имеют раздельные входы в подсистему 3. В этом примере комбинация параллельных подсистем, 1, 2 и 4, 5, соответственно, реализует требуемую часть функции безопасности, независимо от другой (параллельной) подсистемы. Функцию безопасности считают выполненной:

- при событии отказа в подсистеме 1 или подсистеме 2 (поскольку комбинация подсистем 4 и 5 позволяет реализовать функцию безопасности) или

- при событии отказа в подсистеме 4 или подсистеме 5 (поскольку комбинация подсистем 1 и 2 позволяет реализовать функцию безопасности).

Каждая подсистема удовлетворяет требованиям таблиц 1 и 2 следующим образом:

- для подсистемы 1 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL3;

- для подсистемы 2 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL2;

- для подсистемы 3 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL2;

- для подсистемы 4 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL 2;

- для подсистемы 5 уровень полноты безопасности, соответствующий требованиям устойчивости АС к отказам и доле безопасных отказов, равен SIL 1.

Процедура определения максимального уровня полноты безопасности АС, которая может потребоваться для рассматриваемой функции безопасности, следующая:

а) объединение подсистем 1 и 2: устойчивость АС к отказам и доля безопасных отказов, обеспеченная комбинацией подсистем 1 и 2 (каждая в отдельности соответствует требованиям для SIL 3 и SIL 2), соответствует требованиям SIL2 (определенным подсистемой 2);

б) объединение подсистем 4 и 5: устойчивость АС к отказам и доля безопасных отказов, обеспеченная комбинацией подсистем 4 и 5 (каждая в отдельности соответствует требованиям для SIL 2 и SIL 1), соответствует требованиям SIL 1 (определенным подсистемой 5);

в) дальнейшее объединение комбинации подсистем 1 и 2 с комбинацией подсистем 4 и 5: уровень полноты безопасности АС в отношении устойчивости АС к отказам комбинации подсистем 1, 2, 4 и 5 определяется:

- оценкой, какая из комбинаций подсистем (т.е. комбинация подсистем 1 и 2 или 4 и 5) достигла самого высокого возможного уровня полноты безопасности АС (в показателях соответствия требованиям устойчивости к отказам) и

- анализом влияния другой комбинации подсистем на устойчивость к отказам для комбинаций подсистем 1, 2, 4 и 5.

В настоящем примере комбинация подсистем 1 и 2 имеет максимально допустимое требование SIL 2 [см. перечисление а)], в то время как комбинация подсистем 4 и 5 имеет максимально допустимое требование SIL 1 [см. перечисление б)]. Однако в случае отказа, встречающегося в комбинации подсистем 1 и 2, функция безопасности могла бы быть выполнена комбинацией подсистем 4 и 5. С учетом этого устойчивость АС к отказам, достигнутая комбинацией подсистем 1 и 2, увеличивается на единицу. Увеличение устойчивости АС к отказам на единицу приводит к увеличению на единицу уровня полноты безопасности АС, которое может потребоваться (см. таблицы 1 и 2). Поэтому комбинация подсистем 1, 2, 4 и 5 имеет максимально допустимый уровень полноты безопасности в отношении устойчивости к отказам и доли безопасных отказов, равный SIL 3 (т.е. уровень полноты безопасности АС, достигнутый комбинацией подсистем 1 и 2, составляет SIL 2 плюс единица);

г) полная E/E/PE СБЗС-система: уровень полноты безопасности АС в отношении их устойчивости к отказам, который может потребоваться для рассматриваемой функции безопасности, определяют анализом комбинации подсистем 1, 2, 4 и 5 (которая достигает уровня устойчивости к отказам, равного SIL 3 [см. перечисление с)] и подсистемы 3 (которая достигает уровня устойчивости к отказам, равного SIL 2). Подсистема, достигшая самого низкого уровня полноты безопасности АС (в данном случае подсистема 3), определяет максимальный уровень полноты безопасности всей E/E/PE СБЗС-системы. Поэтому максимальный уровень полноты безопасности АС в отношении устойчивости к отказам аппаратных средств, который может быть достигнут для функции безопасности в данном примере, равен SIL 2.

5.8.2 Требования к оценке вероятности отказа функций безопасности из-за случайных отказов АС

5.8.2.1 Вероятность отказа каждой функции безопасности из-за случайных отказов АС не должна превышать значение целевой величины отказов, установленное в спецификации требований к функциональной безопасности (5.5.4, 5.5.5).

Примечания

1 Для функции безопасности, выполняемой АС в режиме с низкой частотой запросов, целевая величина отказов, выраженная как средняя вероятность отказов выполнения по запросу предусмотренной функции безопасности (ГОСТ Р 53195.2, таблица 2), не должна превышать целевой уровень полноты безопасности, установленный для функции безопасности E/E/PE СБЗС-системы (5.5.5). Например, если значение целевой величины отказов (средней вероятности отказов по запросу) для удовлетворения требуемого снижения риска задано равным $1,5 \cdot 10^{-6}$, то значение вероятности отказа по запросу функции безопасности, вызванного случайными отказами АС, не должно быть более $1,5 \cdot 10^{-6}$.

2 Для функции безопасности, выполняемой АС в режиме с высокой частотой запросов или с непрерывным запросом, целевая величина отказов, выраженная в вероятности опасного отказа в час (ГОСТ Р 53195.2, таблица 3), не должна превышать целевой уровень полноты безопасности, установленный для функции безопасности E/E/PE СБЗС-системы. Например, если целевая величина отказов (вероятность опасного отказа в час) для выполнения требований по снижению риска задана равной $1,5 \cdot 10^{-6}$, то вероятность отказа в выполнении функции безопасности, вызванного случайными отказами АС, не должна быть более $1,5 \cdot 10^{-6}$.

3 Для доказательства выполнения данного требования необходимо провести расчет надежности для соответствующей функции безопасности, используя соответствующие средства (5.8.2.2), и сравнить полученный результат с целевой величиной отказов конкретной полноты безопасности для соответствующей функции безопасности (ГОСТ Р 53195.2, таблицы 2 и 3).

5.8.2.2 Вероятность отказа каждой функции безопасности из-за случайных отказов АС должна быть оценена с учетом:

а) структуры E/E/PE СБЗС-системы каждой рассматриваемой функции безопасности.

Примечание — При этом должно быть определено, какие виды отказов подсистем находятся в последовательной связи (при которой любой отказ вызывает отказ соответствующей выполняемой функции безопасности), а какие виды отказов находятся в параллельной связи (при которой отказ соответствующей функции безопасности происходит при совпадающих отказах);

б) оцененной интенсивности отказов каждой подсистемы в любых режимах, которые могли бы вызвать опасные отказы E/E/PE СБЗС-системы, но обнаружены в результате диагностической проверки;

в) восприимчивости E/E/PE СБЗС-системы к отказам по общей причине [см. примечание 5 к перечислению ж)];

г) охвата диагностикой (см. приложение В) и связанного с ним интервала диагностических проверок.

Примечания

1 В модели надежности системы среднее время восстановления принимается как сумма интервала диагностических проверок и последующего времени ремонта. При работе E/E/PE СБЗС-системы в режиме с высокой частотой запросов или с непрерывным запросом, когда любые опасные отказы каналов приводят к опасным отказам E/E/PE СБЗС-системы, в модели надежности интервал диагностических проверок должен быть учтен непосредственно (то есть, дополнительно к среднему времени восстановления), если его значение не является значительно меньшим, чем интервал времени между ожидаемыми запросами (см. 5.8.2.5).

2 При установлении интервала диагностических проверок должны быть учтены интервалы времени между всеми испытаниями, которые влияют на охват диагностикой;

д) интервалов времени, на которых реализуются интервалы диагностических проверок для обнаружения опасных ошибок, не обнаруживаемых диагностическими тестами;

е) времени ремонта системы при обнаруженных отказах.

Примечание — Время ремонта составляет часть среднего времени восстановления, включающего в себя также время обнаружения отказа и период времени, в течение которого ремонт невозможен. Для ситуаций, когда ремонт может быть выполнен в течение конкретного периода времени, например, в то время как УО отключено или находится в надежном (закрытом) состоянии, важно, чтобы при полном расчете был учтен период времени, когда ремонт не может быть проведен, особенно если этот период может быть относительно большим.

ж) вероятности необнаруженного отказа любого процесса передачи данных (см. примечание 5 и 5.13.1).

Примечания

1 Для оценки вероятности опасного отказа в выполнении функции безопасности из-за случайных отказов АС и определения возможности аппаратуры обеспечивать требуемое значение целевой величины отказов может быть применен упрощенный метод.

2 Для каждой функции безопасности должна быть определена отдельно количественным методом надежность E/E/PE СБЗС-системы с учетом влияния разнообразия видов отказов компонентов и изменения структуры (при использовании избыточности) самих E/E/PE СБЗС-систем.

3 Для осуществления анализа и расчетов вероятности необнаруженных отказов метод моделирования определяется проектировщиком. Могут быть применены следующие методы моделирования:

- анализ последствий причин отказа,
- анализ дерева ошибок,
- марковские модели,
- блок-диаграммы надежности.

4 При определении значения среднего времени восстановления АС, рассматриваемого в модели надежности, следует учитывать интервал диагностических проверок, время восстановления и любые другие задержки до момента восстановления.

5 При анализе отказов по общей причине и процессов передачи данных следует учитывать влияние других факторов, отличных от реальных отказов компонентов АС (например электромагнитную интерференцию, ошибки декодирования и т.п.). Такие отказы в настоящем стандарте рассматриваются как случайные отказы аппаратных средств.

5.8.2.3 Интервал диагностических проверок любой подсистемы с устойчивостью АС к отказам выше нуля должен быть таким, чтобы для E/E/PE СБЗС-системы обеспечивалась возможность удовлетворения требований к вероятности случайных отказов АС.

5.8.2.4 Интервал диагностических проверок любой подсистемы с устойчивостью АС к отказам, равной нулю, от которой полностью зависит функция безопасности (см. примечание 1) и которая является лишь средством реализации функции или функций безопасности, действующей(их) в режиме с низкой частотой запросов, должен быть таким, чтобы для E/E/PE СБЗС-системы обеспечивалась возможность удовлетворения требований по вероятности случайных отказов АС.

Примечания

1 В настоящем стандарте принято, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы вызывает отказ этой функции безопасности E/E/PE СБЗС-системы и если эта функция безопасности не относится к другой СБЗС-системе.

2 Если существует вероятность того, что некоторые комбинации выходных состояний подсистем могут непосредственно привести к опасному событию, и если комбинация их выходных состояний при наличии ошибки в подсистеме не может быть определена (например в подсистеме типа Б), то обнаружение опасных отказов в подсистеме следует рассматривать как функцию безопасности, действующую в режиме с высокой частотой запросов или с непрерывным запросом, и применять требования 5.11.3 и 2.8.2.5.

5.8.2.5 Интервал диагностических проверок любой подсистемы с устойчивостью АС к отказам, равной нулю, от которой полностью зависит функция безопасности (см. примечание 1) и которая является лишь средством реализации функции безопасности, действующей в режиме с высокой частотой запросов или с непрерывным запросом (см. примечание 2), должен быть таким, чтобы значение суммарного времени, в которое входит интервал диагностических проверок и время выполнения предусмотренного действия (реакции на отказ), необходимое для достижения или поддержания безопасного состояния, было меньше времени безопасности процесса.

Примечания

1 В настоящем стандарте принято, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы вызывает отказ этой функции безопасности E/E/PE СБЗС-системы, и если эта функция безопасности не относится к другой связанной с безопасностью системе.

2 Подсистему, осуществляющую конкретную функцию безопасности, для которой отношение частоты диагностических проверок к частоте запросов превышает 100, допускается рассматривать как осуществляющую функцию безопасности в режиме с низкой частотой запросов при условии, что функция безопасности не предотвращает комбинацию состояний выходов, которые могли бы привести к опасному событию (см. примечание 3).

3 Если функция безопасности служит для предотвращения специфической комбинации состояний выходов, которые могут непосредственно вызвать опасное событие, то необходимо расценивать такую функцию безопасности как функцию, действующую в режиме с высокой частотой запросов или с непрерывным запросом.

5.8.2.6 Если для конкретного проекта целевая величина отказов требуемой полноты безопасности для выполняемой функции безопасности не достигается, то следует:

- определить критические компоненты, подсистемы и/или параметры;

- оценить эффект возможных мер усовершенствования критических компонентов, подсистем или параметров (например, применение более надежных компонентов, дополнительных мер защиты от отказов по общей причине, расширенного охвата диагностикой, расширенной избыточности, уменьшения интервала контрольных испытаний и т.п.);

- выбрать и осуществить подходящие меры усовершенствования;

- повторить вычисление нового значения вероятности отказов аппаратных средств.

5.9 Требования по предотвращению отказов*

5.9.1 Для предотвращения внесения ошибок во время разработки и создания АС Е/Е/РЕ СБЗС-системы должна быть использована соответствующая группа методов и средств (таблица Б.2 приложения Б).

5.9.2 В соответствии с требуемым уровнем полноты безопасности системы выбранный метод проектирования должен обладать возможностями, способствующими достижению:

а) прозрачности, модульности и других свойств, позволяющих управлять сложностью проекта;

б) ясности и точности представления функциональных возможностей, интерфейсов между подсистемами, а также информации, устанавливающей последовательность и время, параллельность работы подсистем и синхронизацию;

в) ясности и точности документирования и передачи информации;

г) обеспечения верификации (проверки) и подтверждения соответствия.

5.9.3 Для гарантированного поддержания требуемой полноты безопасности Е/Е/РЕ СБЗС-системы на необходимом уровне требования к техническому обслуживанию должны быть формализованы на стадии проектирования и представлены в проектной документации.

5.9.4 Следует использовать, по возможности, автоматические средства измерения и интегрированные инструментальные средства разработки.

5.9.5 На стадии проектирования должны быть запланированы испытания Е/Е/РЕ СБЗС-систем, в том числе интегрированных комплексных систем безопасности. План должен быть отражен в проектной документации. В нем должны быть указаны:

а) типы проводимых испытаний и сопровождающие их процедуры;

б) условия окружающей среды при испытаниях, испытательные средства, схемы испытаний и программы испытаний;

в) критерии оценки «прошла»/«не прошла» система испытание.

5.9.6 Действия, выполняемые на автоматизированном рабочем месте проектировщика на стадии проектирования, должны отличаться от действий, которые должны быть доступными на автоматизированном рабочем месте пользователя (оператора).

5.10 Требования по управлению систематическими отказами**

5.10.1 Для управления систематическими отказами проектирование Е/Е/РЕ СБЗС-систем должно осуществляться с использованием таких средств проектирования и таким образом, чтобы Е/Е/РЕ СБЗС-системы оказывались устойчивыми:

а) к любым остаточным ошибкам проектирования АС, если вероятность ошибок проектирования не может быть исключена (таблица А.16);

б) к внешним влияниям, включая электромагнитные воздействия (см. таблицу А.17);

в) к ошибкам оператора управляемого оборудования (таблица А.18);

г) к любым остаточным ошибкам в программном обеспечении;

д) к любым ошибкам, возникающим в результате выполнения любого процесса передачи данных.

5.10.2 Для облегчения реализации свойств ремонтопригодности и тестируемости в созданных Е/Е/РЕ СБЗС-системах эти свойства должны быть учтены в процессе проектирования и создания Е/Е/РЕ СБЗС-систем.

---

* Для подсистемы, соответствующей требованиям, которые расцениваются как «проверено в эксплуатации» (5.12.6—5.12.12), требования 5.9.1—5.9.6 не применяют.

** Для подсистемы, соответствующей требованиям, которые расцениваются как «проверено в эксплуатации» (5.12.6—5.12.12), требования 5.10.1—5.10.3 не применяют.

5.10.3 При проектировании Е/Е/РЕ СБЗС-систем должны быть учтены способности и возможности человека, а созданные Е/Е/РЕ СБЗС-системы должны быть удобными при эксплуатации и техническом обслуживании. Разработка всех интерфейсов должна осуществляться с учетом человеческого фактора и с ориентацией на возможный уровень специальной подготовки или квалификации операторов.

Примечание — При эксплуатации Е/Е/РЕ СБЗС-систем на объектах массового жилищного строительства оператором может быть человек без специальной подготовки.

5.10.4 Проектирование Е/Е/РЕ СБЗС-систем должно осуществляться таким образом, чтобы предсказуемые ошибки, допущенные оператором или персоналом, осуществляющим техническое обслуживание, не приводили к критическим последствиям, и/или чтобы действия для выполнения операций, могущих повлечь критические последствия, требовали повторного подтверждения.

5.10.5 Размещение органов управления, средств отображения Е/Е/РЕ СБЗС-систем, размещение АС и коммуникаций должно осуществляться на основе эргономического проектирования с учетом конструктивных особенностей здания и сооружения, объемно-планировочных решений, свойств АС, местных условий и окружения систем.

5.11 Требования к действиям системы при обнаружении отказов

5.11.1 Обнаружение опасного отказа (диагностическими тестами, контрольными испытаниями или иным способом) в любой подсистеме Е/Е/РЕ СБЗС-систем с устойчивостью АС к отказам больше нуля должно завершаться:

а) конкретным действием для достижения или поддержания безопасного состояния системы [примечание к перечислению б)] или

б) изоляцией дефектной части подсистемы для обеспечения возможности продолжения выполнения УО защитного действия до завершения ремонта дефектной части. Если ремонт не завершен в пределах среднего времени восстановления, принятого при вычислении вероятности случайных отказов АС, то для достижения и поддержания их безопасного состояния должно быть выполнено конкретное действие.

Примечание — Конкретное действие (реакция на отказ), которое требуется для достижения или поддержания безопасного состояния Е/Е/РЕ СБЗС-системы должно быть определено в требованиях безопасности аппаратных средств Е/Е/РЕ СБЗС-системы. Оно может состоять, например, в отключении УО на подсистеме с дефектом или его части, относящейся к снижению риска.

5.11.2 Обнаружение опасного отказа (диагностическими проверками, контрольными испытаниями или иным способом) в любой подсистеме с устойчивостью к отказам АС, равной нулю, функция безопасности которой является полностью зависимой (примечание 1), в случае, если такая подсистема используется только функцией(ями) безопасности в режиме с низкой частотой запросов, должно завершаться:

а) конкретным действием для достижения и поддержания безопасного состояния или

б) восстановлением дефектной подсистемы в пределах периода среднего времени восстановления, полученного при расчете вероятности случайных отказов аппаратных средств.

В течение этого времени безопасность УО должна обеспечиваться дополнительными мерами и ограничениями. Снижение риска, обеспеченное дополнительными мерами и ограничениями должно, по крайней мере, равняться снижению риска, обеспеченному Е/Е/РЕ СБЗС-системой в отсутствие любых отказов. Дополнительные меры и ограничения должны быть определены в процедурах эксплуатации и технического обслуживания АС Е/Е/РЕ СБЗС-систем. Если восстановление не предпринято в пределах заданного значения среднего времени восстановления, то для достижения и поддержания безопасного состояния должны быть предприняты конкретные действия (примечание 2).

Примечания

1 В настоящем стандарте принято, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы приводит к отказу функции безопасности рассматриваемой Е/Е/РЕ СБЗС-системы, и функция безопасности не предназначена для другой системы, связанной с безопасностью.

2 Для достижения и поддержания безопасного состояния требуется конкретное действие (реакция на отказ), которое должно быть определено в требованиях безопасности АС Е/Е/РЕ СБЗС-систем. Это действие может состоять, например, в безопасном отключении УО в дефектной подсистеме или ее части с целью снижения риска.

5.11.3 Обнаружение опасного отказа (путем осуществления диагностических проверок, контрольных испытаний или иным способом) в любой подсистеме с устойчивостью к отказам, равной нулю, в которой функция безопасности является зависимой (примечание 1), в случае подсистемы, выполняющей любую(ые) функцию(ии) безопасности, действующую(ие) в режиме с высокой частотой запросов или непрерывным

запросом (примечания 2 и 3), для достижения и поддержания безопасного состояния, должно завершаться конкретными действиями (примечание 3).

Примечания

1 В настоящем стандарте принято, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы служит причиной отказа функции безопасности рассматриваемой E/E/PE СБЗС-системы, а также функция безопасности не относится к другой связанной с безопасностью системе.

2 Если имеется вероятность того, что некоторая комбинация состояний выходов подсистемы может стать непосредственной причиной опасного события, и если комбинацию выходных состояний в случае отказа в подсистеме невозможно определить (например для подсистемы типа Б), то детектирование опасных событий в подсистеме следует расценивать как функцию безопасности, действующую в режиме с высокой частотой запросов или с непрерывным запросом, и применять требования 5.11.3 и 5.7.6.

3 Для достижения и поддержания состояния безопасности, которое должно быть определено в требованиях безопасности E/E/PE СБЗС-систем, необходимо выполнить конкретное действие (реакцию на отказ). Это действие может состоять, например, в безопасном отключении в дефектной подсистеме управляемого оборудования или его части для снижения риска.

5.12 Требования к реализации E/E/PE СБЗС-систем

5.12.1 E/E/PE СБЗС-системы должны быть реализованы (изготовлены, установлены) в соответствии с проектом.

5.12.2 Подсистемы, используемые для реализации одной или более функций безопасности, должны быть идентифицированы и документированы как связанные с безопасностью подсистемы.

5.12.3 Для каждой связанной с безопасностью подсистемы в проекте должна быть представлена следующая информация:

а) перечень функций, интерфейсов и стыков подсистемы, которые могут быть использованы при реализации функций безопасности;

б) расчетные или оценочные значения частоты отказов (из-за случайных отказов АС в любых режимах), обнаруживаемых диагностическими проверками, которые могли бы привести к отказу E/E/PE СБЗС-системы;

в) расчетные или оценочные значения частоты отказов (из-за случайных отказов АС), не обнаруживаемых диагностическими проверками, которые могли бы привести к отказу E/E/PE СБЗС-системы;

г) ограничения на параметры окружающей среды подсистемы, которые должны быть соблюдены для обеспечения правомерности расчетных (оценочных) значений частот отказов из-за случайных отказов АС;

д) ограничение срока службы подсистемы, который не должен быть превышен для обеспечения правомерности расчетных (оценочных) значений частот отказов из-за случайных отказов АС;

е) требования к контрольным испытаниям и/или техническому обслуживанию подсистемы;

ж) охват диагностикой подсистемы в соответствии с приложением Б (при необходимости, см. примечание).

Примечание — Испытания по перечислениям е), ж) относятся к диагностическим испытаниям, которые являются внутренними для подсистемы. Перечисленная информация необходима, если требуется обеспечение доверия к действиям по проведению диагностических испытаний в подсистемах в модели надежности E/E/PE СБЗС-систем;

и) интервал диагностических испытаний [при необходимости, см. примечание перечисления ж)];

к) любая дополнительная информация (например время восстановления), необходимая для обеспечения возможности получения значения среднего времени восстановления после обнаружения отказа с помощью диагностических проверок.

Примечания

1 Испытания по параметрам, приведенным в перечислениях б) — к), необходимы для использования их результатов при оценке вероятности отказов функции безопасности по запросу или вероятности отказов в час.

2 Требования перечислений б), в), е), ж), к) необходимы для оценки отдельных параметров подсистем, таких как сенсорные устройства и приводы, которые могут быть объединены в избыточные структуры для улучшения полноты безопасности АС. Для логических решающих устройств, которые обычно не объединяют в избыточные структуры в одиночной E/E/PE СБЗС-системе, с учетом требований перечислений б), в), е), ж), к) допускается использовать такие характеристики, как вероятность отказов по запросам или вероятность отказов в час. Для логических устройств необходимо также устанавливать интервал контрольных испытаний для необнаруженных отказов;

л) информация, необходимая для обеспечения выделения составляющей безопасных отказов подсистемы, как принято в E/E/PE СБЗС-системе, в соответствии с приложением Б;

м) устойчивость к отказам подсистемы.

Примечание — Требования перечислений л), м) необходимы для определения самого высокого уровня полноты безопасности, который может потребоваться для функции безопасности в соответствии со структурными ограничениями системы;

н) любые ограничения по применению подсистемы, которые должны быть рассмотрены во избежание систематических отказов;

п) самый высокий уровень полноты безопасности, который может потребоваться для функции безопасности в подсистеме, на основе:

- методов и средств, используемых для предотвращения систематических ошибок, которые вносятся на этапах проектирования и реализации АС и ПО,

- особенностей проекта, которые делают подсистему устойчивой к систематическим отказам.

Примечание — Не требуется, если эти подсистемы расцениваются как «проверенные в эксплуатации»;

р) информация, необходимая для идентификации конфигурации АС и ПО подсистемы для обеспечения возможности управления конфигурацией E/E/PE СБЗС-системы в соответствии с 6.2.1 ГОСТ Р 53195.2.

5.12.4 Расчетные (оценочные) значения частоты отказов подсистем из-за случайных отказов АС [5.12.3, перечисления б) и в)] могут быть определены:

а) исследованием видов отказов и анализом влияния подсистем на основе данных по отказам компонентов из признанного промышленного источника по надежности.

Примечания

1 Уровень доверия любых используемых данных о частоте отказов должен быть не менее 70 %.

2 Хотя понятие «постоянная частота отказов» подсистемы принято большинством вероятностных оценочных методов, оно применимо лишь при условии, что не превышен срок службы компонентов подсистемы. Поэтому любая вероятностная оценка должна включать в себя спецификацию срока службы компонентов;

б) из предыдущего опыта использования подсистемы в похожих условиях применения и окружающей среды.

5.12.5 Для подсистем, «проверенных в эксплуатации», информация о методах и средствах предотвращения и управления систематическими отказами не требуется.

5.12.6 Ранее разработанная подсистема должна рассматриваться как «проверенная в эксплуатации» только в случае, если ее функциональные возможности явно ограничены, и имеется соответствующее документальное свидетельство, основанное на предыдущей эксплуатации конкретной конфигурации этой подсистемы (в течение которого все отказы были документально зарегистрированы) и учитывающее любые требующиеся дополнительные анализы и тесты. Документальное подтверждение должно свидетельствовать, что вероятность любого отказа подсистемы (из-за случайных и систематических отказов АС) в E/E/PE СБЗС-системе настолько мала, что достигается(ются) требуемый(ые) уровень(ни) полноты безопасности функции(ий) безопасности.

5.12.7 Документальное свидетельство, в соответствии с 5.12.6, должно подтверждать, что предыдущие условия эксплуатации конкретной подсистемы являются такими же или достаточно близкими к тем, в которых будет эксплуатироваться подсистема в E/E/PE СБЗС-системе и свидетельствовать, что вероятность любых необнаруженных систематических отказов настолько низка, что достигается требуемый уровень(ни) полноты безопасности функции(ий) безопасности для подсистемы.

Примечание — Условия эксплуатации подсистемы включают в себя все факторы, которые могут повлиять на вероятность систематических отказов АС и ПО подсистемы. Например, условия окружающей среды, виды использования, выполняемые функции, конфигурацию, связи с другими системами, операционную систему, тип транслятора, человеческий фактор.

5.12.8 Если имеются различия между предыдущими условиями эксплуатации подсистемы и условиями, в которых будет эксплуатироваться E/E/PE СБЗС-система, то такие различия должны быть идентифицированы и с использованием комбинации соответствующих методов анализа и испытаний в проектной документации должно быть представлено доказательство того, что вероятность любой необнаруженной систематической ошибки настолько низка, что достигается требуемый уровень(ни) полноты безопасности для функции(ий) безопасности подсистемы.

5.12.9 Документальное свидетельство по 5.12.6 должно установить, что время предыдущего использования конкретной конфигурации подсистемы (в часах эксплуатации) является достаточным, чтобы статистически рассматривать заявленное значение частоты отказов. Как минимум, требуется достаточное время эксплуатации для установления значения заявленной частоты отказов в одностороннем нижнем пределе доверия, по крайней мере, 70 %. При статистическом анализе время эксплуатации любой индивидуальной подсистемы в течение менее одного года не рассматривается как часть полного времени эксплуатации.

Примечание — Требуемое время эксплуатации подсистемы для установления заявляемого значения частоты отказов может быть получено по результатам эксплуатации нескольких идентичных подсистем при условии, что отказы всех подсистем были обнаружены и документированы. Например, если имеется 100 подсистем, каждая из которых проработала без отказов 10000 ч, то полное время эксплуатации без отказов можно считать равным 1000000 ч. В этом случае каждая подсистема должна эксплуатироваться более одного года и действия при расчетах должны быть отнесены к полученному выше полному числу часов эксплуатации.

5.12.10 При проверке выполнения требований к подсистеме по 5.12.6 и 5.12.9 должна быть принята во внимание только предыдущая эксплуатация подсистемы, при которой все отказы подсистем были обнаружены и документированы.

5.12.11 При проверке выполнения или невыполнения требований 5.12.6 и 5.12.9 следует учитывать диапазон охвата и уровень детализации имеющейся информации для следующих факторов: сложность подсистемы, вклад, внесенный конкретной подсистемой в снижение риска, последствия, связанные с отказом системы, новизну проекта.

5.12.12 Термин «проверено в эксплуатации» следует применять к связанной с безопасностью подсистеме в Е/Е/РЕ СБЗС-системе и ограничивать его применение к функциям и интерфейсам подсистемы (5.12.6—5.12.10).

Примечание — Требования 5.12.4—5.12.12 применимы также к подсистемам, содержащим ПО. В случае применения таких подсистем следует убедиться, что конкретная подсистема выполняет в Е/Е/РЕ СБЗС-системе только те функции, для которых задана требуемая полнота безопасности.

5.13 Требования к передаче-приему данных

5.13.1 При любой форме передачи данных, используемой при выполнении функции безопасности, должна быть оценена вероятность необнаруженного отказа процесса передачи-приема данных с учетом ошибок передачи, повторов, удалений, вставок, повторного упорядочения, искажения, задержки и ошибок идентификации (5.13.2). Эта вероятность должна быть учтена при оценке вероятности опасного отказа функции безопасности из-за случайных отказов аппаратных средств (5.8.2.2).

Примечание — Ошибка идентификации означает, что истинное содержание сообщения идентифицировано неправильно (например, сообщение от компонента, не связанного с безопасностью, идентифицировано как сообщение от компонента, связанного с безопасностью).

5.13.2 При оценке вероятности отказа функции безопасности из-за процесса передачи-приема данных, в частности, должны быть учтены:

а) остаточный коэффициент ошибок;

б) остаточный коэффициент потери информации;

в) пределы и непостоянство скорости передачи информации (битовой скорости);

г) пределы и непостоянство задержки распространения информации.

Примечание — Вероятность опасного отказа в час равна отношению вероятности коэффициента остаточных ошибок к длине сообщения (в битах), умноженному на скорость передачи сообщений в шине, относящихся к безопасности, и на 3600.

5.14 Интеграция Е/Е/РЕ СБЗС-систем

5.14.1 Требования к интеграции и испытаниям должны быть предусмотрены для всех Е/Е/РЕ СБЗС-систем, устанавливаемых и интегрируемых в зданиях и сооружениях.

5.14.2 СБЗС-системы должны быть интегрированы в соответствии с конкретным проектом Е/Е/РЕ СБЗС-систем и испытаны в соответствии с конкретными тестами для интеграции Е/Е/РЕ СБЗС-систем (ГОСТ Р 53195.2, 7.8.3).

5.14.3 В ходе интеграции всех модулей в E/E/PE СБЗС-системы отдельные E/E/PE СБЗС-системы должны быть испытаны (5.7). Испытания должны показать, правильно ли взаимодействуют все модули и не выполняют ли непредназначенные для них функции.

Примечания

1 В этом случае испытание всех входных комбинаций не проводится. Достаточно провести испытание всех классов эквивалентности. Для сокращения числа испытаний до приемлемого уровня могут быть применены методы статического анализа, динамического анализа или анализа отказов. Проведение проектирования в соответствии с правилами, приводящими к структурному проектированию или полуформальным методам, облегчает выполнение этих требований.

2 Если при разработке используются формальные методы или формальные доказательства и утверждения, а также статистические методы, то возможности таких испытаний могут быть ограничены.

5.14.4 Для проведения испытаний интегрированных E/E/PE СБЗС-систем должна быть разработана соответствующая документация, устанавливающая методику испытаний и определяющая достижение целей и критериев, установленных на этапах проектирования и реализации систем. В случае отказа системы должны быть документированы причины и способы его устранения.

5.14.5 В период интеграции и испытаний любые модификации или изменения E/E/PE СБЗС-систем должны быть проанализированы. При анализе должны быть идентифицированы все компоненты, на которые влияют проведенные модификации или изменения, и все необходимые действия по повторному подтверждению выполнения требований к системам.

5.14.6 При испытаниях интегрированных E/E/PE СБЗС-систем должна быть документирована следующая информация:

а) конкретное место установки интегрированной E/E/PE СБЗС-системы;

б) версия спецификации требований к испытаниям интегрированных E/E/PE СБЗС-систем;

в) критерии оценки испытаний интегрированной E/E/PE СБЗС-системы: «прошла»/»не прошла» система испытания;

г) версия испытуемой E/E/PE СБЗС-системы;

д) используемые средства испытаний и оборудование с датой поверки;

е) результаты каждого испытания системы;

ж) любое несоответствие между ожидаемыми и фактическими результатами испытаний интегрированных E/E/PE СБЗС-систем;

и) проведенный анализ и принятое решение о продолжении испытаний систем или оформлении запроса на их изменение (в случае несоответствия требованиям).

5.14.7 Для предотвращения ошибок во время интеграции E/E/PE СБЗС-систем должна быть использована соответствующая группа методов и средств, приведенных в таблице Б.3 приложения Б.

5.15 Процедуры эксплуатации и технического обслуживания систем

5.15.1 На этапе проектирования должны быть разработаны порядок действий, процедуры и документы, гарантирующие поддержание необходимой функциональной безопасности E/E/PE СБЗС-систем во время эксплуатации и технического обслуживания.

5.15.2 Разрабатываемые порядок действий, процедуры и документы по эксплуатации и техническому обслуживанию E/E/PE СБЗС-систем должны устанавливать:

а) действия, которые должны быть выполнены для поддержания предусмотренной проектом функциональной безопасности E/E/PE СБЗС-систем, включая замену компонентов с предварительно заданными сроками службы, например батарей электропитания и др.;

б) действия и ограничения, необходимые для предотвращения опасных отказов или уменьшения последствий опасных событий (например, во время установки, пуска в действие, режима эксплуатации, периодических испытаний, прогнозируемых неисправностей, отказов или ошибок, отключений);

в) документацию по отказам системы и частотам запросов E/E/PE СБЗС-систем;

г) документацию с результатами аудитов и испытаний E/E/PE СБЗС-систем, подлежащую сохранению;

д) процедуры технического обслуживания, которым необходимо следовать в случае, если происходят отказы и ошибки в E/E/PE СБЗС-системах, в том числе:

- процедуры диагностики отказов и восстановления (ремонта) E/E/PE СБЗС-систем, подсистем и компонентов,

- процедуры повторного подтверждения соответствия E/E/PE СБЗС-систем установленным требованиям,

- требования по поддержанию отчетности;

е) процедуры по поддержанию параметров отчетности, которые должны быть определены, в частности процедуры отчетности: по отказам, по анализу отказов;

ж) инструменты и средства, необходимые для технического обслуживания и подтверждения соответствия, и процедуры для поддержания инструментов и средств в рабочем состоянии.

Примечание — В процедуры эксплуатации и технического обслуживания Е/Е/РЕ СБЗС-систем должны быть включены процедуры модификации программного обеспечения.

5.15.3 Действия по техническому обслуживанию Е/Е/РЕ СБЗС-систем, необходимые для поддержания их проектной функциональной безопасности, должны быть установлены на основе системного подхода, который должен обеспечивать определение необнаруженных отказов всех компонентов, связанных с безопасностью (от сенсорных устройств до оконечных элементов), которые могли бы вызвать снижение достигнутой полноты безопасности.

Примечания

1 Для реализации системного подхода могут быть применены методы, включающие в себя:

- экспертизу деревьев отказов;
- анализ видов отказов и анализ влияния;
- поддержание надежности тщательного технического обслуживания.

2 Должен быть учтен человеческий фактор — ключевой момент в определении требуемых действий и соответствующих интерфейсов между человеком и Е/Е/РЕ СБЗС-системой(ами).

3 Частота проведения периодических испытаний должна быть выбрана такой, чтобы была обеспечена целевая величина отказов.

4 При выборе частоты периодических испытаний, интервала диагностических проверок и времени для последующего ремонта Е/Е/РЕ СБЗС-систем должны быть учтены:

- целевая величина отказов, связанных с уровнем полноты безопасности Е/Е/РЕ СБЗС-систем;
- структура системы;
- охват систем диагностикой;
- ожидаемая частота запросов к системам.

5.15.4 Процедуры эксплуатации и технического обслуживания Е/Е/РЕ СБЗС-систем должны быть оценены на возможность воздействия, которое они могут оказать на УО.

5.15.5 Для предотвращения отказов и ошибок во время процедур эксплуатации и технического обслуживания Е/Е/РЕ СБЗС-систем рекомендуется использовать методы/средства, приведенные в таблице Б.4 приложения Б.

5.16 Подтверждение соответствия Е/Е/РЕ СБЗС-систем требованиям безопасности

5.16.1 Для каждой Е/Е/РЕ СБЗС-системы должно быть получено подтверждение того, что заданная Е/Е/РЕ СБЗС-система полностью соответствует требованиям функциональной безопасности (требованиям к функциям безопасности и требованиям к полноте безопасности).

5.16.2 Подтверждение соответствия Е/Е/РЕ СБЗС-систем требованиям функциональной безопасности должно выполняться согласно разработанному плану подтверждения соответствия.

Примечания

1 Подтверждение соответствия отдельных Е/Е/РЕ СБЗС-систем требованиям функциональной безопасности осуществляется на основании результатов (выходов) стадий жизненного цикла Е/Е/РЕ СБЗС-систем после их установки (например, если разработка прикладного ПО для интегрированных систем еще не завершена, а отдельные системы уже установлены), а подтверждение соответствия интегрированных Е/Е/РЕ СБЗС-систем осуществляется после их интеграции.

В случаях, предусмотренных технической документацией, допускается осуществлять подтверждение соответствия отдельных Е/Е/РЕ СБЗС-систем в составе интегрированной Е/Е/РЕ СБЗС-системы.

2 Подтверждение соответствия программируемой электроники, связанной с безопасностью, включает в себя подтверждение соответствия АС и ПО.

5.16.3 Подтверждение соответствия каждой функции безопасности, указанной в спецификации требований к функциональной безопасности Е/Е/РЕ СБЗС-систем, требованиям безопасности, процедурам эксплуатации и технического обслуживания систем должно осуществляться в результате проведения испытаний и/или анализа.

5.16.4 Должна быть подготовлена необходимая документация по проведению испытаний на подтверждение соответствия Е/Е/РЕ СБЗС-систем требованиям функциональной безопасности, в которой для каждой функции безопасности должны быть указаны:

а) конкретное место установки Е/Е/РЕ СБЗС-систем;

б) версия используемого плана проведения подтверждения соответствия Е/Е/РЕ СБЗС-систем;

в) функция безопасности, подвергаемая испытаниям (или анализу), вместе с ссылкой на указанные в документах конкретные требования по планированию проведения подтверждения соответствия Е/Е/РЕ СБЗС-систем требованиям безопасности;

г) испытательные средства и оборудование, данные об их поверке и аттестации;

д) результаты испытаний систем;

е) несоответствие между ожидаемыми и фактическими результатами испытаний.

Примечание — Для каждой функции безопасности отдельная документация не требуется, но каждая функция безопасности и каждое отклонение по перечислениям а) — е) должны быть отражены в документации.

5.16.5 Если фактические результаты отличаются от ожидаемых результатов более, чем это установлено допусками, результаты испытаний на подтверждение соответствия Е/Е/РЕ СБЗС-систем требованиям безопасности должны быть документированы, включая:

а) описание проведенного анализа,

б) принятое решение о продолжении испытаний или об оформлении извещения об изменении и возвращении к более раннему этапу испытаний на подтверждение соответствия.

5.16.6 Для предотвращения отказов при проведении подтверждения соответствия Е/Е/РЕ СБЗС-систем требованиям функциональной безопасности следует использовать методы/средства, приведенные в таблице Б.5 приложения Б.

5.17 Модификация Е/Е/РЕ СБЗС-систем

5.17.1 Модификация Е/Е/РЕ СБЗС-систем должна осуществляться в соответствии с требованиями и процедурами, установленными в ГОСТ Р 53195.2, 7.17.

5.17.2 Действия по модификации любой Е/Е/РЕ СБЗС-системы должны обеспечивать достижение и поддержание требуемой полноты безопасности после изменения, расширения или адаптации этой системы.

5.17.3 По каждому действию по модификации Е/Е/РЕ СБЗС-систем должна быть разработана и сохранена документация. Документация должна включать в себя:

а) детальный перечень модификаций или изменений системы;

б) анализ влияния действий по модификации на полную систему (включая АС и ПО), на взаимодействие «оператор/система», на окружающую среду и возможные взаимодействия с другими системами;

в) утвержденные изменения системы;

г) порядок проведения изменений;

д) результаты испытаний составляющих модулей, в том числе данные повторного подтверждения их соответствия установленным требованиям;

е) предысторию управления конфигурацией Е/Е/РЕ СБЗС-систем;

ж) отклонения от нормальных действий и условий;

и) необходимые изменения системных процедур;

к) необходимые изменения документации.

5.17.4 Изготовители или поставщики Е/Е/РЕ СБЗС-систем, требующих подтверждения соответствия требованиям настоящего стандарта, должны осуществлять техническую поддержку системы при инициировании изменений в результате обнаруживаемых в АС или ПО дефектов и сообщать пользователям о необходимой модификации в случае обнаружения дефекта, затрагивающего безопасность.

5.17.5 Модификация Е/Е/РЕ СБЗС-систем должна проводиться, по крайней мере, с таким же уровнем экспертизы, автоматизированных средств планирования и управления, какой применялся при разработке Е/Е/РЕ СБЗС-систем.

5.17.6 После модификации Е/Е/РЕ СБЗС-системы должны быть повторно верифицированы, а также должно быть повторно подтверждено их соответствие требованиям функциональной безопасности.

5.18 Верификация Е/Е/РЕ СБЗС-систем

5.18.1 Каждая Е/Е/РЕ СБЗС-система должна быть верифицирована с проверкой и оценкой выходных результатов каждой рассмотренной стадии жизненного цикла этой системы для гарантирования правильности всех действий и соответствия в отношении продукции и требований стандартов, предусмотренных на входах этих стадий.

Примечания

1 Все требования к действиям по верификации объединены в 5.18, но фактически они должны выполняться на всех стадиях жизненного цикла Е/Е/РЕ СБЗС-систем.

2 На стадии разработки проектной (рабочей) документации верификация может быть проведена в форме нормоконтроля. На других стадиях жизненного цикла Е/Е/РЕ СБЗС-систем верификация может осуществляться независимыми лицами, отделами или организациями (в зависимости от жесткости требований, предъявляемых к Е/Е/РЕ СБЗС-системам и объектам, в которых они установлены).

5.18.2 Верификация Е/Е/РЕ СБЗС-систем должна быть запланирована одновременно с разработкой этих систем для каждой стадии их жизненного цикла и документирована.

5.18.3 В плане верификации Е/Е/РЕ СБЗС-систем должны быть указаны критерии, методы/средства, используемые для верификации на проверяемой стадии их жизненного цикла.

5.18.4 При планировании верификации Е/Е/РЕ СБЗС-систем должны быть предусмотрены обязательные действия, обеспечивающие правильность установления соответствия требований к продукции и требований стандартов, примененных на входе каждой стадии их жизненного цикла.

5.18.5 Планирование верификации Е/Е/РЕ СБЗС-систем должно предусматривать:

а) выбор порядка и методов верификации;

б) выбор и использование испытательного оборудования и средств испытаний;

в) выбор и документирование действий в ходе верификации;

г) оценку результатов верификации, полученных непосредственно от оборудования, используемого для верификации, и испытаний.

5.18.6 При проектировании и разработке каждой стадии Е/Е/РЕ СБЗС-системы должно быть показано, что требования к функциям безопасности и полноте безопасности выполняются.

5.18.7 Результат каждого действия по верификации должен быть документирован с указанием о прохождении верификации Е/Е/РЕ СБЗС-системой или причины отказа. Должны быть описаны устройства, не соответствующие:

а) одному или более требованиям жизненного цикла Е/Е/РЕ СБЗС-системы,

б) одному или более требованиям стадии проектирования системы,

в) одному или более требованиям управления функциональной безопасностью системы (раздел 6).

5.18.8 Для верификации требований функциональной безопасности Е/Е/РЕ СБЗС-системы, после того как они были установлены и перед началом следующей стадии (проектирования и реализации), проверка должна обеспечивать:

а) определение адекватности требований функциональной безопасности Е/Е/РЕ СБЗС-систем требованиям, установленным при распределении требований безопасности по Е/Е/РЕ СБЗС-системам для безопасности, функциональных возможностей и других требований, установленных при планировании безопасности;

б) проверку на несовместимость:

- требований безопасности Е/Е/РЕ СБЗС-систем (5.5),
- распределения требований безопасности (ГОСТ Р 53195.2),
- испытаний Е/Е/РЕ СБЗС-систем (5.7),
- документации пользователя и остальной документацией на систему.

5.18.9 Для верификации стадии проектирования и реализации Е/Е/РЕ СБЗС-систем после ее завершения и до начала следующей стадии (интеграции) проверка должна:

а) определить адекватность тестов для стадии проектирования и реализации Е/Е/РЕ СБЗС-систем (5.7);

б) определить связанность и завершенность (до уровня модулей, включительно) стадии проектирования и разработки Е/Е/РЕ СБЗС-систем (5.7) в отношении требований безопасности (5.5);

в) проверить на несовместимость:

- требования безопасности Е/Е/РЕ СБЗС-систем (5.5),
- результат проектирования и разработки Е/Е/РЕ СБЗС-систем (5.7),
- испытания Е/Е/РЕ СБЗС-систем (5.7).

Примечания

1Методы подтверждения соответствия безопасности, анализа отказов и тестирования, приведенные в таблице Б.5 приложения Б, могут быть использованы также для верификации.

2 При верификации достижения необходимого охвата диагностикой Е/Е/РЕ СБЗС-систем следует учитывать отказы и ошибки, которые должны быть обнаружены (таблица А.1 приложения А).

5.18.10 Для верификации интеграции АС Е/Е/РЕ СБЗС-систем должна быть проверена интеграция Е/Е/РЕ СБЗС-систем для установления выполнения требований подраздела 5.14.

5.18.11 Все проверки и их результаты должны быть документированы.

6 Оценка функциональной безопасности

Требования к оценке функциональной безопасности E/E/PE СБЗС-систем — по ГОСТ Р 53195.2, раздел 8.

Приложение А
(справочное)

Методы и средства управления отказами E/E/PE СБЗС-систем

А.1 Общие положения

Настоящее приложение следует использовать совместно с 5.7. Оно ограничивает максимальный охват диагностикой, что может потребоваться для выбора подходящих методов и средств управления отказами. Для каждого уровня полноты безопасности в приложении рекомендованы методы и средства управления случайными, систематическими, эксплуатационными отказами и отказами, обусловленными влиянием окружения систем.

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

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

Отказы в E/E/PE СБЗС-системах могут быть разделены на две категории в зависимости от времени их возникновения:

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

Для предотвращения таких отказов или управления ими, когда они происходят, требуется применение большого числа мер. «Меры» — это проведение мероприятий с использованием определенных «методов» и/или «средств», которые обозначены в таблицах и тексте как «метод/средство». Структура требований, приведенных в приложениях А и Б, является следствием разделения всех методов/средств на методы/средства, используемые для предупреждения отказов в течение различных стадий жизненного цикла E/E/PE СБЗС-систем (приложение Б), и методы/средства, используемые для управления отказами в период эксплуатации (настоящее приложение). Методы/средства управления отказами — это методы/средства, основанные на применении собственных встроенных составляющих E/E/PE СБЗС-систем.

Охват диагностикой и доля безопасных отказов E/E/PE СБЗС-систем определяются на основе таблицы А.1 и в соответствии с процедурами, детализированными в приложении Б. Таблицы А.2 — А.15 дополняют требования таблицы А.1 методами и средствами для диагностических тестов и требованиями к минимальным уровням охвата диагностикой, которые могут быть достигнуты при их использовании. Требования этих таблиц не заменяют требования, приведенные в приложении Б. Требования таблиц А.2 — А.15 не являются исчерпывающими. Могут быть использованы другие методы и средства, если приведено свидетельство об обеспечении необходимого охвата диагностикой. Если требуется высокий уровень охвата диагностикой, то из каждой из этих таблиц должна быть применена как минимум одна мера (метод/средство) по охвату диагностикой высокого уровня.

По аналогии таблицы А.16 — А.18 содержат рекомендуемые меры (методы/средства) для управления систематическими отказами для каждого уровня полноты безопасности. В таблице А.16 рекомендуются полные меры для управления систематическими отказами. В таблице А.17 даны рекомендуемые меры по управлению отказами из-за влияния окружающей среды. В таблице А.18 приведены меры (методы/средства) по управлению ошибками при эксплуатации. Большинство этих мер по управлению систематическими отказами может быть структурировано в соответствии с таблицей А.19.

Руководящие указания в настоящем приложении не гарантируют сами по себе требуемую полноту безопасности. При их применении важно определить:

- последовательность выбранных методов/средств и то, как они будут дополнять друг друга,
- какие методы/средства в наибольшей степени подходят для решения конкретных задач, которые возникают во время создания каждой заданной E/E/PE СБЗС-системы.

А.2 Полнота безопасности АС

В таблице А.1 представлены требования к ошибкам или отказам, которые должны быть обнаружены с использованием методов/средств по управлению отказами АС E/E/PE СБЗС-систем для достижения соответствующего уровня охвата диагностикой (см. также приложение Б). Таблицы А.2 — А.15 дополняют требования, приведенные в таблице А.1, рекомендуемыми методами/средствами для диагностических тестов и рекомендуемыми минимальными требованиями к охвату диагностикой, который может быть достигнут с их применением. Эти диагностические тесты могут выполняться непрерывно или периодически. Указанные таблицы не заменяют ни одного из требований подраздела 5.7.

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

Наименование компонента(ов) системы	Номер таблицы	Наименование, описание ошибок и отказов, моделей их обнаружения при уровне охвата диагностикой АС систем		
		низком (60 %)	среднем (90 %)	высоком (99 %)
Электромеханические устройства	А.2	Невключение или неотключение. Приваривание («залипание») контактов	Не включение или не отключение. Приваривание («залипание») отдельных контактов	Не включение или не отключение. Приваривание («залипание») отдельных контактов. Конкретные руководства отсутствуют
Дискретные АС: - цифровой вход/выход	А.3, А.7, А.9, А.11	Непрерывный отказ	Модель отказов из-за отклонений и колебаний постоянного тока	Модель отказов из-за отклонений и колебаний постоянного тока
- аналоговый вход/выход		Непрерывный отказ	Модель отказов из-за отклонений и колебаний постоянного тока	Модель отказов из-за отклонений и колебаний постоянного тока
- источник питания		Непрерывный отказ	Модель отказов из-за отклонений и колебаний постоянного тока	Модель отказов из-за отклонений и колебаний постоянного тока
Шина: - общая шина	А.3, А.7, А.8	Непрерывный отказ адресов	Молчание	Молчание
- элемент управления памятью		Непрерывный отказ данных или адресов	Неверное декодирование адреса	Неверное декодирование адреса
- прямой доступ к памяти		Непрерывный отказ данных или адресов	Модель непрерывного отказа данных и адресов. Неверное время доступа	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время доступа
- управление доступом к шине (см. примечание 1)		Непрерывный отказ сигналов управления доступом к шине	Отсутствует или неправильное управление доступом к шине	Отсутствует или неправильное управление доступом к шине
Процессор: - регистр, внутреннее ОЗУ	А.4, А.10	Непрерывный отказ для данных или адресов	Модель отказов по постоянному току для данных и адресов	Модель отказов по постоянному току для данных и адресов. Динамическая переброска ячеек памяти. Отсутствует, неверная или множественная адресация

Окончание таблицы А.1

Наименование компонента(ов) системы	Номер таблицы	Наименование, описание ошибок и отказов, моделей их обнаружения при уровне охвата диагностикой АС систем		
		низком (60 %)	среднем (90 %)	высоком (99 %)
- 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	Модель отказов при постоянном токе	Отсутствует определение предполагаемого отказа
- счетчик команд, указатель стека		Непрерывный отказ	Модель отказов при постоянном токе	Модель отказов при постоянном токе
Устройство обработки прерываний	А.4	Отсутствуют или непрерывные прерывания	Отсутствуют или непрерывные прерывания. Пересечение прерываний	Отсутствуют или непрерывные прерывания. Пересечение прерываний
Постоянная память	А.5	Непрерывный отказ для данных или адресов	Модель отказов по постоянному току для данных и адресов	Все отказы, влияющие на данные в памяти
Переменная память	А.6	Непрерывный отказ для данных или адресов	Модель отказов по постоянному току для данных и адресов. Изменение информации, вызванное ошибками ПО для ОЗУ 1 МБ и выше	Модель отказов по постоянному току для данных и адресов. Динамическое пересечение ячеек памяти. Отсутствует, неверная или множественная адресация. Изменение информации, вызванное ошибками ПО для ОЗУ 1 МБ и выше
Устройство синхронизации (кварцевое)	А.12	Нижняя или верхняя гармоника	Нижняя или верхняя гармоника	Нижняя или верхняя гармоника
Устройство связи и запоминающее устройство большой емкости	А.13	Неверные данные или адреса. Отсутствует передача данных	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи	Все ошибки, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи
Сенсоры	А.14	Непрерывный отказ	Неверная последовательность передачи. Модель отказов из-за отклонений и колебаний постоянного тока	Неверная последовательность передачи. Модель отказов из-за отклонений и колебаний постоянного тока
Оконечные элементы	А.15	Непрерывный отказ	Модель отказов из-за отклонений и колебаний постоянного тока	Модель отказов из-за отклонений и колебаний постоянного тока

Примечания

1 «Непрерывный» — категория отказа, которая может быть описана всеми нулями (0) или единицами (1) на контактах компонента.

2 «Модель отказов по постоянному току» включает следующие модели отказов: непрерывные отказы, открытые непрерывные, открытые выходы или выходы с высоким сопротивлением, а также короткие замыкания в соединительных линиях.

Таблица А.2 — Уровень охвата диагностикой электрических подсистем в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме внешнего управления	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой для обнаружения отказов
Мониторинг контактов реле	Высокий	—
Компаратор		Высокий уровень, если отказы преимущественно безопасны
Мажоритарная схема голосования	Высокий	Зависит от качества устройства голосования
Принцип реактивного тока	Низкий	Только для E/E/PE СБЗС-систем, где не требуется непрерывное управление для достижения и поддержания безопасного состояния УО
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.3 — Уровень охвата диагностикой электронных подсистем в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме внешнего управления (онлайн)	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой для обнаружения отказов
Компаратор	Высокий	Высокий, если режимы отказов, в основном, безопасно диагностируются
Мажоритарная схема голосования	Высокий	Зависит от качества устройства голосования
Тестирование с использованием избыточных аппаратных средств	Средний	Зависит от охвата диагностикой для обнаружения отказов
Динамические принципы		Зависит от охвата диагностикой для обнаружения отказов
Стандартный тестовый порт доступа и структура граничного сканирования	Высокий	Зависит от охвата диагностикой для обнаружения отказов
Контролируемая избыточность		Зависит от степени избыточности и текущего контроля

Окончание таблицы А.3

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Аппаратные средства с автоматической проверкой	Высокий	Зависит от охвата диагностикой тестами
Текущий контроль аналоговых сигналов	Низкий	—
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.4 — Уровень охвата диагностикой устройств обработки в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Компаратор	Высокий	Зависит от качества сравнения
Мажоритарная схема голосования		Зависит от качества устройства голосования
Самотестирование с использованием ПО: ограниченное число модулей (один канал)	Низкий	—
Самотестирование с использованием ПО: «блуждающий бит» (один канал)	Средний	
Самотестирование с использованием АС (один канал)		
Запрограммированная обработка (один канал)	Высокий	
Взаимное сравнение с использованием ПО		Зависит от качества сравнения
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.5 — Уровень охвата диагностикой неизменяемых областей в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Многобитовая избыточность защиты слов	Средний	—
Модифицированная контрольная сумма	Низкий	
Сигнатура из одного слова (8 бит)	Средний	Эффективность сигнатуры зависит от ее длины по отношению к длине блока защищаемой информации

Окончание таблицы А.5

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Сигнатура из двух слов (16 бит)	Высокий	Эффективность сигнатуры зависит от ее длины по отношению к длине блока защищаемой информации
Дублирование блока		—
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.6 — Уровень охвата диагностикой переменных областей памяти в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой
Тест ОЗУ «шахматная доска» или «марш»	Низкий
Тест ОЗУ «блуждающая траектория»	Средний
Тест ОЗУ «GALPAT» — попарная запись — считывание с использованием бегущего кода или «Прозрачный GALPAT»	Высокий
Тест ОЗУ «Авраам»	
Бит четности для ОЗУ	Низкий
Контроль ОЗУ с использованием модифицированного кода Хэмминга или обнаружение сбоев данных с использованием кодов обнаружения и коррекции ошибок	Высокий
Дублированное ОЗУ с аппаратным или программным сравнением и контролем считывания/записи	
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.	

Таблица А.7 — Уровень охвата диагностикой устройства входа/выхода и интерфейсов (внешняя связь) в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Тестирующая комбинация	Высокий	—
Обнаружение отказов путем мониторинга в режиме внешнего управления	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой для обнаружения отказов
Кодовая защита	Высокий	—
Многоканальный параллельный выход		Только если поток данных изменяется во время интервала тестовых проверок

Окончание таблицы А.7

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Контролируемый выход	Высокий	Только если поток данных изменяется во время интервала тестовых проверок
Сравнение / голосование на входе (избыточность 1oo2, 2oo3 или более высокая избыточность)		
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.8 — Уровень охвата диагностикой маршрутизаторов данных (внутренняя связь) в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Однобитовая аппаратная избыточность	Низкий	—
Многобитовая аппаратная избыточность	Средний	
Полная аппаратная избыточность	Высокий	
Анализ с использованием тестирующих комбинаций		
Избыточность при передаче		Эффективно только для неустойчивых сбоев
Информационная избыточность		—
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.9 — Уровень охвата диагностикой источников питания в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Защита от перенапряжения с защитой от короткого замыкания или отключением /подключением ко второму источнику питания	Низкий	Рекомендуется использовать всегда в дополнение к другим методам настоящей таблицы
Контроль напряжения (вторичного) с безопасным отключением /подключением ко второму источнику питания	Высокий	—
Отключение питания с защитой от короткого замыкания и отключение / подключение ко второму источнику питания	Высокий	Рекомендуется использовать всегда в дополнение к другим методам настоящей таблицы

Окончание таблицы А.9

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Принцип реактивного тока	Низкий	Полезен только против отключения питания
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.10 — Уровень охвата диагностикой в зависимости от применяемых методов/средств диагностики последовательности выполнения программ (дежурного таймера)

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Дежурный таймер с отдельной временно́й базой без временно́го окна	Низкий	—
Дежурный таймер с отдельной временно́й базой и временны́м окном	Средний	—
Логический мониторинг последовательности выполнения программ		Зависит от качества мониторинга
Комбинация временно́го и логического мониторинга последовательности выполнения программ	Высокий	—
Временно́й мониторинг-тест с внешним контролем	Средний	—
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.		

Таблица А.11 — Уровень охвата диагностикой в зависимости от применяемых методов/средств диагностики системы вентиляции и подогрева (при необходимости)

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой
Датчик температуры	Средний
Управление вентиляцией	
Безопасное выключение с использованием плавкого предохранителя	Высокий
Пороговые сообщения от термодатчиков и условная тревога	
Соединение устройства принудительного охлаждения воздуха и индикатора состояния	
Примечания 1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б. 2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.	

Таблица А.12 — Уровень охвата диагностикой в зависимости от применяемых методов/средств диагностики генератора тактовой частоты

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Дежурный таймер с отдельным временны́м периодом без временно́го окна	Низкий	—
Дежурный таймер с отдельной временно́й базой и временны́м окном	Средний	Зависит от временных ограничений для временно́го окна
Логический мониторинг последовательности выполнения программ		Эффективно только при отказе генератора тактовой частоты, если внешние временны́е события влияют на процесс выполнения программы
Комбинация временно́го и логического мониторинга последовательности выполнения программ	Высокий	—
Временно́й мониторинг с внешним контролем	Средний	—

Примечания

1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б.

2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.

Таблица А.13 — Уровень охвата диагностикой в зависимости от применяемых методов/средств диагностики устройства связи и запоминающе́е устройство большой емкости

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Обмен информацией между E/E/PE СБЗС-системой и процесс обработки информации	См. таблицу А.7	См. устройства вх/вых и интерфейс
Обмен информацией между E/E/PE СБЗС-системами	См. таблицу А.8	См. цепи/шины данных
Разделение линий электрического питания и линий передачи информации	Высокий	Рекомендуется использовать всегда в дополнение к другим методам в этой таблице
Пространственное разделение групповых линий		—
Увеличение устойчивости к электромагнитным воздействиям		—
Передача сигнала без наводок		—

Примечания

1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б.

2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.

Таблица А.14 — Уровень охвата диагностикой в зависимости от применяемых методов/средств диагностики датчиков (сенсорных устройств)

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме с внешним управлением (онлайн)	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от диагностического охвата обнаружения отказов
Принцип реактивного тока	Низкий	Только для E/E/PE СБЗС-систем, где не требуется непрерывное управление для достижения и поддержания безопасного состояния УО
Текущий контроль аналоговых сигналов	Низкий	—
Тестирующая комбинация	Высокий	—
Сравнение/голосование на входе (избыточность 1oo2, 2oo3 или более высокая избыточность)	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Эталонный датчик		Зависит от охвата диагностикой обнаружения отказов
Положительно активизированный переключатель	Высокий	—

Примечания

1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б.

2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.

Таблица А.15 — Уровень охвата диагностикой оконечных элементов (приводов) в зависимости от применяемых методов/средств диагностики

Метод/средство диагностики	Максимально достижимый рассматриваемый уровень охвата диагностикой	Примечание
Обнаружение отказов путем мониторинга в оперативном режиме (онлайн)	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от диагностического охвата обнаружения отказов
Мониторинг контактов реле	Высокий	—
Тестирующая комбинация		—
Мониторинг		Зависит от диагностического охвата обнаружения отказов
Принцип реактивного тока	Низкий	Только для E/E/PE СБЗС-систем, где не требуется непрерывное управление для достижения и поддержания безопасного состояния УО
Перекрестный контроль сложных приводов	Высокий	—

Примечания

1 Данные требования не заменяют ни одного из требований, приведенных в приложении Б.

2 Требования, приведенные в приложении Б, могут быть применены для определения уровня охвата диагностикой.

А.3 Полнота безопасности в отношении систематических отказов

Рекомендации к мерам (методам/средствам), применяемым для управления отказами, приведены в таблицах А.16 — А.18. Рекомендуемые методы/средства управления отказами, связанными с проектированием АС и ПО, приведены в таблице А.16, вызванными воздействиями или влияниями окружения на системы — в таблице А.17, возникающими в ходе эксплуатации, — в таблице А.18.

Рекомендации, приведенные в таблицах А.16 — А.18, отнесенные к уровням полноты безопасности, устанавливают, во-первых, важность метода /средства и, во-вторых, эффективность его использования.

Таблица А.16 — Уровень эффективности методов/средств управления систематическими отказами при разработке АС и ПО для различных уровней полноты безопасности

Вид заливки	Метод/средство	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Мониторинг последовательности выполнения программ	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Обнаружение отказов путем мониторинга в режиме онлайн (см. примечание 2)	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Тестирование избыточными аппаратными средствами	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Стандартный тестовый порт доступа и структура граничного сканирования	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Кодовая защита	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Разнообразие аппаратных средств	— низкий	— низкий	Р (R) средний	Р (R) высокий
	Обнаружение и диагностика ошибок	Методы и средства должны быть определены в нормативных документах на ПО			
	Обнаружение и исправление ошибок				
	Программирование с проверкой ошибок				
	Методы «подушки безопасности»				
	Многовариантное программирование				
	Блоки восстановления				
	Восстановление предыдущего состояния				
	Прямое восстановление				
	Повторный запуск механизмов восстановления после отказов				
	Сохранение достигнутых состояний				
	Постепенное отключение функций				
	Исправление ошибок методами искусственного интеллекта				
	Динамическое реконфигурирование				

Примечания

1 Пояснение обозначений, приведенных под каждым уровнем полноты безопасности, приведено в тексте, предшествующем настоящей таблице.

2 Для E/E/PE СБЗС-систем, действующих в режиме с низкой частотой запросов (например систем аварийного отключения системы или оборудования), охват диагностикой, достигаемый путем обнаружения отказа с помощью мониторинга в режиме внешнего управления (онлайн), обычно является низким или отсутствует.

3 Для управления систематическими отказами при разработке АС и ПО E/E/PE СБЗС-систем требуется выполнение хотя бы одного из методов, помеченных серой заливкой.

Таблица А.17 — Уровень эффективности методов/средств управления систематическими отказами, вызванными воздействиями окружения на E/E/PE СБЗС-системы с различным уровнем полноты безопасности

Вид заливки	Метод/средство управления систематическими отказами	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Методы/средства против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Разделение линий электропитания и линий передачи информации (см. примечание 2)	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Повышение устойчивости к электромагнитным воздействиям	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Средства против физического воздействия окружающей среды (например температуры, влажности, воды, вибраций, пыли, разъедающих веществ)	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Мониторинг последовательности выполнения программ	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Методы/средства против повышения температуры	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Пространственное разделение групповых линий связи	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Обнаружение отказов путем мониторинга в режиме внешнего управления (см. примечание 3)	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Тестирование избыточными аппаратными средствами	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Передача неэквивалентных сигналов	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Разнообразие аппаратных средств (см. примечание 4)	— низкий	— низкий	— средний	Р (R) высокий
	Структура программного обеспечения	Методы / средства должны быть определены в нормативных документах на ПО			

Примечания

1 Пояснение обозначений, приведенных под каждым уровнем полноты безопасности, приведено в тексте, предшествующем таблице А.16.

2 Разделение линий электропитания и линий передачи информации не является необходимым при передаче информации по оптоволокну, а также в случаях передачи информации по низковольтным электрическим линиям, которые запроектированы для электропитания АС E/E/PE-систем и одновременной передачи по ним информации.

3 Для E/E/PE СБЗС-систем, действующих в режиме с низкой частотой запросов (например систем аварийного отключения системы или оборудования), охват диагностикой, достигаемый путем обнаружения отказа с помощью мониторинга в режиме внешнего управления, обычно является низким или отсутствует.

4 Для достижения целевых величин отказа разнообразие АС не требуется, если путем подтверждения соответствия или на основании большого опыта эксплуатации аналогичных АС может быть доказано, что они достаточно свободны от ошибок, возникающих на стадии проектирования и достаточно защищены от отказов по общей причине.

5 Для управления систематическими отказами в период эксплуатации при воздействии окружения на E/E/PE СБЗС-системы требуется выполнение хотя бы одного из методов/средств, помеченных серой заливкой.

Таблица А.18 — Уровень эффективности методов/средств управления систематическими отказами при эксплуатации E/E/PE СБЗС-систем

Вид заливки	Метод/средство управления систематическими отказами	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Защита от модификаций	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Обнаружение отказов путем мониторинга в режиме внешнего управления (см. примечание 3)	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Подтверждение ввода	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Программирование с проверкой ошибок	Методы/средства должны быть определены в нормативных документах на ПО			

Примечания

1 Пояснение обозначений, приведенных под каждым уровнем полноты безопасности, приведено в тексте, предшествующем таблице А.16.

2 По крайней мере два средства/метода, приведенных в таблице, могут быть использованы для изменения эффективности в соответствии с таблицей А.19, в которой приведены примеры для низкого и высокого уровней эффективности.

3 Для E/E/PE СБЗС-систем, действующих в режиме с низкой частотой запросов (например систем аварийного отключения), охват диагностикой, достигаемый путем обнаружения отказа с использованием мониторинга в режиме внешнего управления, обычно является низким или отсутствует.

4 Для управления систематическими отказами в период эксплуатации E/E/PE СБЗС-системы требуется выполнение, по крайней мере, хотя бы одного из методов/средств, помеченных серой заливкой.

Важность методов/средств, указанных в таблицах А.16—А.18, обозначена и характеризуется следующим образом:

КР (HR) — метод/средство крайне рекомендован(о) для указанного в таблице уровня полноты безопасности. Если он (оно) не используются, то должно быть приведено подробное обоснование неиспользования;

Р (R) — метод/средство рекомендован(о) для указанного в таблице уровня полноты безопасности. Требуется применение хотя бы одного из методов/средств, помеченных слева в левой колонке таблицы серой заливкой;

знак «—» — метод/средство, в отношении которого нет рекомендаций ни для применения, ни против применения;

Уровни эффективности и необходимость применения методов/средств управления отказами, приведенные в таблицах А.16 — А.18, обозначены и характеризуются следующим образом:

«обязательный» — метод/средство следует применять для всех уровней полноты безопасности, и он (оно) должен(но) быть использован(но) максимально эффективно [т.е. он (оно) обладает максимальной эффективностью];

«низкий» — метод/средство должен(но) быть использован(но) в степени, необходимой для получения, по крайней мере, низкого уровня эффективности противодействия систематическим отказам;

«средний» — метод/средство должен(но) быть применен(но) в степени, необходимой для получения, по крайней мере, среднего уровня эффективности противодействия систематическим отказам;

«высокий» — метод/средство должен(но) быть применен(о) в степени, необходимой для получения высокого уровня эффективности противодействия систематическим отказам.

Руководство по уровням эффективности для ряда методов/средств приведено в таблице А.19.

Если мера не является обязательной, то она может быть заменена другими мерами (индивидуальными или в комбинации), отмеченными серой заливкой в таблицах А.16 — А.18.

Таблица А.19 — Описание методов/средств управления систематическими отказами с различными уровнями эффективности

Метод/средство управления систематическими отказами	Описание метода/средства для уровней эффективности:	
	низкого	высокого
Обнаружение отказов путем мониторинга в режиме внешнего управления (онлайн)*	Сигналы запуска от УО и его системы управления используются для контроля правильности действия E/E/PE СБЗС-систем (только характера изменения во времени и максимального времени реакции)	E/E/PE СБЗС-системы перезапускаются временными и логическими сигналами от УО и его системы управления (временно́е окно для временно́й функции дежурного таймера)
Тестирование избыточными аппаратными средствами*	Дополнительные проверки сигналов запуска E/E/PE СБЗС-систем с использованием АС (только характера изменения во времени и максимального времени реакции). Эти средства включают вспомогательное оконечное устройство	Дополнительные АС повторно перезапускаются временными и логическими сигналами E/E/PE СБЗС-систем (временно́е окно для временно́го дежурного таймера); голосование между несколькими каналами
Стандартный тестовый порт доступа и структура граничного сканирования	Проверка твердотельных логических интегральных микросхем (ИС) с использованием граничных тестовых испытаний в период контрольных испытаний	Диагностический контроль твердотельных логических ИС на соответствие спецификации функций безопасности E/E/PE СБЗС-систем. Проверяются все функции для всех интегральных микросхем
Кодовая защита	Обнаружение ошибок с использованием временно́й избыточности при передаче сигналов	Обнаружение ошибок с использованием временно́й и информационной избыточности при передаче сигналов
Мониторинг последовательности выполнения программ	Временно́й или логический мониторинг последовательности выполнения программ	Временно́й и логический мониторинг последовательности выполнения программ с большим числом контрольных точек в программе
Средства против повышения температуры	Температурный датчик, определяющий превышение температуры	Применение защитного отключения с использованием плавкого предохранителя
Повышение устойчивости к электромагнитным воздействиям*	Помехозащитный фильтр в источнике питания и на критических входах и выходах; экранирование, при необходимости	Фильтр против электромагнитных воздействий, которые обычно не ожидаются; экранирование
Средства против физического воздействия окружающей среды	Средства общепринятой практики в соответствии с применением	Средства, предусмотренные стандартами для конкретного применения
Разнообразие аппаратных средств	Два или более устройств, спроектированные по-разному, выполняют одну и ту же функцию	Два или более устройств, выполняющих различные функции
Подтверждение ввода	Отображение входных действий оператору	Проверка по строгим правилам входных данных, вводимых оператором, с отклонением неправильных входных данных

* В случае применения этих методов/средств для получения высокого уровня эффективности предполагается, что они могут быть также использованы для получения низкого уровня эффективности.

Все перечисленные выше методы/средства являются встроенными компонентами Е/Е/РЕ СБЗС-систем, предназначенными для облегчения управления отказами в режиме внешнего управления. Для предотвращения введения ошибок следует применять процедурные и организационные методы /средства на протяжении всего жизненного цикла Е/Е/РЕ СБЗС-систем. Для проверки противодействия Е/Е/РЕ СБЗС-систем ожидаемым внешним воздействиям необходимо применять методы оценки соответствия для предоставления доказательств того, что встроенные компоненты соответствуют установленным требованиям (приложение В).

Примечание — Большинство методов/средств, приведенных в таблицах А.16 — А.18, может быть использовано с разным уровнем эффективности в соответствии с таблицей А.19, в которой приведено описание ряда методов/средств с низким и высоким уровнями эффективности. Затраты, требуемые для получения среднего уровня эффективности, находятся в пределах между затратами, необходимыми для получения низкого и высокого уровней эффективности.

Приложение Б
(справочное)

Методы и средства по предотвращению систематических отказов на стадиях жизненного цикла Е/Е/РЕ СБЗС-систем

В таблицах Б.1 — Б.5 настоящего приложения для каждого уровня безопасности Е/Е/РЕ СБЗС-систем приведены рекомендуемые методы и средства для предотвращения отказов в Е/Е/РЕ СБЗС-системах.

Отказы в Е/Е/РЕ СБЗС-системах могут быть идентифицированы в соответствии со стадиями жизненного цикла, на которых появились источником внесения ошибок:

- отказы, вызванные ошибками, возникающими *до установки или в период установки системы* (например ошибки ПО включают в свой состав ошибки спецификации и ошибки программ, а ошибки в АС включают в свой состав производственные ошибки и неправильный выбор компонентов);
- отказы, вызванные ошибками, возникающими после установки системы (например случайные отказы аппаратных средств, вызванные неправильным использованием оборудования).

Для предотвращения таких отказов или управления ими при возникновении обычно требуется применение большого числа мер. «Меры» — это проведение мероприятий с использованием определенных «методов» и/или «средств», которые обозначены в таблицах и тексте как «метод/средство». В приложениях А и Б требования связаны с мерами, которые предпринимают для *предотвращения отказов* из-за ошибок на разных стадиях жизненного цикла аппаратных средств Е/Е/РЕ СБЗС-систем (настоящее приложение), и мерами, которые предпринимают для *управления отказами* в период эксплуатации Е/Е/РЕ СБЗС-систем (приложение А). Меры для управления отказами — это применение средств, встроенных в Е/Е/РЕ СБЗС-системы, а меры для предотвращения отказов — это проведение мероприятий с использованием методов, выполняемых в течение жизненного цикла систем.

Рекомендации, приведенные в таблицах Б.1 — Б.5, соотносятся с уровнями полноты безопасности. Они устанавливают, во-первых, важность метода/средства и, во-вторых, эффективность его использования.

Важность обозначена следующим образом:

КР (HR) — метод/средство крайне рекомендован(но) для указанного в графе таблицы уровня полноты безопасности. Если он (оно) не применен(но), то в проектной документации должно быть приведено подробное обоснование отказа от их применения;

Р (R) — метод/средство рекомендован(о) для указанного в графе таблицы уровня полноты безопасности. Требуется применение хотя бы одного метода/средства, из помеченных в таблицах серой заливкой;

знак «—» — метод/средство, который(ое) не имеют рекомендаций ни для применения, ни против применения;

НР (NR) — метод/средство не рекомендован(но) к применению для указанного в графе таблицы уровня полноты безопасности. Если он (оно) применен(но), то в проектной документации должно быть приведено подробное обоснование такого применения.

Уровень эффективности и необходимость применения методов/средств по предотвращению систематических отказов на стадиях жизненного цикла Е/Е/РЕ СБЗС-систем приведены в таблицах Б.1 — Б.5. Уровни эффективности, приведенные в таблице, означают следующее:

«обязательный» — требуется обязательное применение указанного в таблице метода/средства для всех уровней полноты безопасности, и которые должны использоваться настолько эффективно, насколько это возможно (т.е. с максимальной эффективностью);

«низкий» — при использовании указанного в таблице метода/средства он (оно) должен(но) быть применен(но) в степени, необходимой для получения, по крайней мере, низкого уровня эффективности противодействия систематическим отказам;

«средний» — при использовании указанного в таблице метода/средства он (оно) должен(но) быть применен(но) в степени, необходимой для получения, по крайней мере, среднего уровня эффективности противодействия систематическим отказам;

«высокий» — при использовании указанного в таблице метода/средства он (оно) должен(но) быть применен(но) в степени, необходимой для получения высокого уровня эффективности противодействия систематическим отказам.

Примечание — Большинство методов/средств, приведенных в таблицах Б.1 — Б.5, может быть использовано с различным уровнем эффективности, в соответствии с таблицей Б.6, в которой приведено описание ряда методов/средств с низким и высоким уровнями эффективности. Затраты, необходимые для достижения среднего уровня эффективности, находятся в пределах между затратами, необходимыми для получения низкого и высокого уровней эффективности.

Если метод/средство не является обязательным, то он (оно) может быть заменен(но) другими методами/средствами (индивидуальным или в комбинации), которые помечены в таблицах Б.1 — Б.5 серой заливкой.

Само по себе выполнение требований настоящего приложения еще не гарантирует достижения требуемой полноты безопасности. При выборе методов/средств следует учитывать следующие факторы:

- взаимное соответствие выбранных методов/средств, и как они дополняют друг друга;
- какие из них предназначены для каждой стадии создания E/E/PE СБЗС-систем;
- какие из них являются наиболее подходящими для решения проблем, встречающихся в процессе создания каждой отдельной E/E/PE СБЗС-системы.

Таблица Б.1 — Рекомендации по предотвращению ошибок во время задания спецификации требований к E/E/PE СБЗС-системам

Вид заливки	Метод/средство предотвращения ошибок на стадии задания спецификации требований к системам	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Управление проектами	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Документирование	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Разделение E/E/PE СБЗС-систем и систем, не связанных с безопасностью	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Структурирование спецификации	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Экспертиза спецификации	— низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Полуформальные методы	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Таблица контрольных проверок	P (R) низкий	P (R) низкий	KP (HR) средний	KP (HR) высокий
	Компьютерные средства разработки спецификаций	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
	Формальные методы	— низкий	— низкий	P (R) средний	P (R) высокий
Примечание — Пояснение обозначений, приведенных под каждым уровнем полноты безопасности (SIL), приведено в тексте, предшествующем настоящей таблице.					

Все методы и средства, обозначенные «P (R)» в таблице Б.1, заменяемые, но требуется применение хотя бы одного из них.

Для проверки соответствия требованиям на стадии задания спецификации требований к E/E/PE СБЗС-системам должен быть применен хотя бы один (одно) из методов/средств, помеченных серой заливкой в таблице Б.1 или перечисленных в таблице Б.5.

Таблица Б.2 — Рекомендации по предупреждению внесения ошибок на стадиях проектирования и реализации E/E/PE СБЗС-систем

Вид заливки	Метод/средство предупреждения внесения ошибок на стадиях проектирования и реализации систем	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Соблюдение требований законов, руководящих материалов, стандартов, сводов правил, проектной документации	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Управление проектами	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Документирование	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Структурированное проектирование	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Модульное проектирование	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Использование достоверно испытанных компонентов	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Полуформальные методы	Р (R) низкий	Р (R) низкий	КР (HR) средний	КР (HR) высокий
	Таблица контрольных проверок	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Средства автоматизированного проектирования	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Моделирование	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Поверка аппаратных средств или сквозной анализ	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
	Формальные методы	— низкий	— низкий	Р (R) средний	Р (R) средний
Примечание — Пояснение обозначений, приведенных под каждым уровнем полноты безопасности (SIL), приведено в тексте, предшествующем настоящей таблице.					

Методы/средства, обозначенные «Р (R)» в таблице Б.2, заменяемые, но требуется применение хотя бы одного из них.

Для проверки соответствия требований на стадиях проектирования и реализации E/E/PE СБЗС-систем должен быть применен хотя бы один из методов или средств, помеченных серой заливкой в таблице Б.2 или перечисленных в таблице Б.5.

Таблица Б.3 — Рекомендации для предотвращения ошибок на стадии интеграции E/E/PE СБЗС-систем

Вид заливки	Метод/средство предотвращения ошибок на стадии интеграции систем	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Функциональное тестирование	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Управление проектами	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
	Управление документацией	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий

Окончание таблицы Б.3

Вид заливки	Метод/средство предотвращения ошибок на стадии интеграции систем	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Тестирование методом «черного ящика»	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
	Полевые испытания	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
	Статистическое тестирование	— низкий	— низкий	P (R) средний	P (R) высокий

Примечания

1 Пояснение обозначений, приведенных под каждым уровнем полноты безопасности (SIL), приведено в тексте, предшествующем настоящей таблице.

2 Методы/средства, обозначенные «P (R)» в настоящей таблице, заменяемые, но требуется применение хотя бы одного из них.

3 Для проверки соответствия требований к E/E/PE СБЗС-системам на стадии интеграции должен быть применен хотя бы один (одно) из методов/средств, помеченных серой заливкой в таблице Б.3 или перечисленных в таблице Б.5.

Таблица Б.4 — Рекомендации по предотвращению ошибок и отказов в период эксплуатации и технического обслуживания E/E/PE СБЗС-систем

Вид заливки	Метод/средство предотвращения ошибок в период эксплуатации и технического обслуживания систем	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Инструкции по эксплуатации и техническому обслуживанию	KP (HR) обязательный	KP (HR) обязательный	KP (HR) обязательный	KP (HR) обязательный
	Обеспечение удобства системы для пользователя	KP (HR) обязательный	KP (HR) обязательный	KP (HR) обязательный	KP (HR) обязательный
	Обеспечение удобства системы для обслуживающего персонала	KP (HR) обязательный	KP (HR) обязательный	KP (HR) обязательный	KP (HR) обязательный
	Управление проектами	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Управление документацией	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
	Сокращение объема работ на стадии эксплуатации	— низкий	P (R) низкий	KP (HR) средний	KP (HR) высокий
	Защита от ошибок оператора	— низкий	P (R) низкий	KP (HR) средний	KP (HR) высокий
	Эксплуатация только квалифицированным оператором	— низкий	P (R) низкий	P (R) средний	KP (HR) высокий

Примечания

1 Пояснение обозначений, приведенных под каждым уровнем полноты безопасности (SIL), приведено в тексте, предшествующем настоящей таблице.

2 Все методы/средства, обозначенные «P (R)» в настоящей таблице, заменяемые, но требуется применение хотя бы одного из них.

Таблица Б.5 — Рекомендации по предотвращению ошибок на стадии подтверждения соответствия E/E/PE СБЗС-систем

Вид заливки	Метод/средство предотвращения ошибок на стадии подтверждения соответствия	Уровень эффективности методов /средств для			
		SIL1	SIL2	SIL3	SIL4
	Функциональное тестирование	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Функциональные испытания в условиях окружающей среды	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Испытания на устойчивость к пиковым выбросам внешних электромагнитных воздействий	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Испытание с введением неисправностей (при требуемом охвате диагностикой ≥ 90 %)	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный	КР (HR) обязательный
	Управление проектами	КР (HR) низкий	КР (HR) средний	КР (HR) средний	КР (HR) высокий
	Документирование	КР (HR) низкий	КР (HR) средний	КР (HR) средний	КР (HR) высокий
	Статический анализ, динамический анализ, анализ отказов	— низкий	Р (R) средний	Р (R) средний	Р (R) высокий
	Моделирование и анализ отказов	— низкий	Р (R) средний	Р (R) средний	Р (R) высокий
	Анализ наихудшего случая, динамический анализ и анализ отказов	— низкий	— средний	Р (R) средний	Р (R) высокий
	Статический анализ и анализ отказов (см. примечание 3)	Р (R) низкий	Р (R) средний	НР (NR) не рекомендуемый	НР (NR) не рекомендуемый
	Расширенное функциональное тестирование	— низкий	КР (HR) средний	КР (HR) средний	КР (HR) высокий
	Тестирование методом «черного ящика»	Р (R) низкий	Р (R) средний	Р (R) средний	Р (R) высокий
	Испытания с введением неисправностей (при требуемом охвате диагностикой < 90 %)	Р (R) низкий	Р (R) средний	Р (R) средний	Р (R) высокий
	Статистическое тестирование	— низкий	— средний	Р (R) средний	Р (R) высокий
	Испытания в наихудших случаях	— низкий	— средний	Р (R) средний	Р (R) высокий
	Полевые испытания	Р (R) низкий	Р (R) средний	Р (R) средний	НР (NR) не рекомендуемый

Примечания

1 Пояснение обозначений, приведенных под каждым уровнем полноты безопасности (SIL), приведено в тексте, предшествующем настоящей таблице.

2 Статистический анализ и анализ отказов не рекомендуется для SIL3 и SIL4, т.к. эти методы недостаточны, если они не используются в комбинации с динамическим анализом.

Таблица Б.5 разделена на три группы, помеченные белой, серой и черной заливкой. Все рекомендуемые методы/средства «Р (R)» в группах, помеченных белой и черной заливкой, могут быть заменены другими методами/средствами в пределах каждой из групп, но требуется применение, по крайней мере, одного метода/средства из группы, помеченной серой заливкой (аналитические методы) и, как минимум, одного метода/средства из группы, помеченной черной заливкой (средства испытаний).

Эффективность методов/средств для предотвращения систематических ошибок приведена в таблице Б.6.

Таблица Б.6

Метод/средство предотвращения систематических ошибок	Описание метода/средства предотвращения систематических ошибок для	
	низкого уровня эффективности	высокого уровня эффективности
Управление проектами *	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; статистика отказов; автоматизированные расчеты; автоматизированная разработка программного обеспечения
Документирование*	Применение графических и естественных языков, например, блок-схем, потоковых диаграмм	Использование правил, описывающих: порядок прохождения и размещения документации в организации, содержимое таблиц контрольных проверок; автоматизированное управление документацией; формальный контроль изменений
Разделение E/E/PE СБЗС- систем и систем, не связанных с безопасностью	Четкое разделение интерфейсов между E/E/PE СБЗС-системами и системами, не связанными с безопасностью	Полное отделение E/E/PE СБЗС-систем от систем, не связанных с безопасностью, т.е. предотвращение доступа систем, не связанных с безопасностью, к E/E/PE СБЗС-системам; физическое разделение в пространстве во избежание влияний по общей причине
Структурирование спецификации требований	Иерархическое разделение вручную требований на подтребования; описание интерфейсов	Формирование иерархически разделенных компьютерных средств проектирования; автоматический контроль последовательности; доведение усовершенствования до функционального уровня
Формальные методы	Использование формальных методов персоналом, имеющим опыт в их применении	Использование формальных методов персоналом, имеющим опыт в их применении в аналогичных областях с использованием автоматизированных средств поддержки
Полуформальные методы	Использование полуформальных методов для описания некоторых критических составляющих	Полное описание СБЗС E/E/PE-систем, связанных с безопасностью, различными полуформальными методами для представления различных аспектов; проверка согласованности между методами
Компьютерные средства разработки спецификации	Применение средств разработки спецификации без предпочтения одного конкретного метода проектирования	Применение модельно-ориентированных процедур с иерархической структурой; описание всех объектов и их отношений; применение общей базы данных; автоматический контроль непротиворечивости
Таблицы контрольных проверок	Подготовка таблиц контрольных проверок для всех стадий жизненного цикла; концентрация внимания на главных проблемах безопасности	Подготовка подробных таблицы контрольных проверок для всех стадий жизненного цикла систем

Продолжение таблицы Б.6

Метод/средство предотвращения систематических ошибок	Описание метода/средства предотвращения систематических ошибок для	
	низкого уровня эффективности	высокого уровня эффективности
Экспертиза спецификации	Проведение экспертизы спецификации требований безопасности независимым лицом	Проведение экспертизы и повторной экспертизы независимой организацией, использующей формальную процедуру с исправлением всех обнаруженных ошибок
Структурное проектирование	Проектирование иерархических схем, выполняемое вручную	Повторное использование проверенных компонентов; отслеживание взаимосвязи между спецификацией, проектом, принципиальными схемами и перечнем компонентов системы; использование компьютеров; применение определенных методов (см. также 5.9)
Использование достоверно испытанных компонентов*	Обоснованная перепроверка; проверка конструктивных характеристик	«Проверено на практике» (см. 5.12.6)
Модульное проектирование *	Применение модулей ограниченных размеров; функциональное изолирование каждого модуля	Повторное использование хорошо проверенных модулей; модулей с ясными свойствами; модулей, имеющих максимум один вход, один выход и один выход сигнализации об отказе
Средства компьютерного проектирования	Компьютерная поддержка безопасности на сложных стадиях жизненного цикла	Использование средств, хорошо проверенных на практике (см. 5.12.6), или средств с подтвержденным соответствием; полностью компьютерное проектирование всех стадий жизненного цикла системы
Моделирование	Моделирование на модульном уровне, включая предельные условия для периферийных устройств	Моделирование на уровне компонентов, включая предельные условия
Инспектирование АС	Инспектирование лицом, не связанным с проектированием системы	Инспектирование и повторное инспектирование независимой организацией, использующей формальные процедуры с исправлением всех обнаруженных ошибок
Сквозной анализ аппаратных средств	Проведение сквозного анализа аппаратных средств лицом, не зависимым от проектирования	Проведение сквозного анализа аппаратных средств независимой организацией, действующей по формальной процедуре с исправлением всех обнаруженных ошибок
Ограничение эксплуатационных возможностей *	Применение ключа или пароля для управления изменением режима работы	Применение установленной жесткой процедуры, разрешающей выполнение действий
Эксплуатация исключительно квалифицированными операторами	Базовое обучение по используемому типу систем безопасности плюс два года соответствующего опыта работы	Ежегодное обучение всех операторов; привлечение к работе операторов с опытом эксплуатации E/E/PE СБЗС-систем с более низким уровнем полноты безопасности — не менее пяти лет
Защита от ошибок оператора*	Применение подтверждения входного сообщения	Применение подтверждения и проверки согласованности каждой входной команды
Тестирование методом «черного ящика»*	Применение классов эквивалентности и тестирования по отдельным диапазонам входных сигналов, тестирование по граничным значениям, использование предписанных условий испытаний	Применение условий испытаний по диаграммам последствий причин (отказов) в комбинации с критическими случаями в экстремальных диапазонах работы

Окончание таблицы Б.6

Метод/средство предотвращения систематических ошибок	Описание метода/средства предотвращения систематических ошибок для	
	низкого уровня эффективности	высокого уровня эффективности
Статистическое тестирование*	Использование статистических распределений для всех входных данных	Получение результатов испытаний автоматическими средствами; применение большого числа тестовых испытаний; распределение входных данных в соответствии с условиями реального применения и принятыми моделями отказов
Полевые испытания*	10000 часов эксплуатации; по крайней мере, один год эксплуатации как минимум десяти устройств в различных применениях; статистическая точность 95 %; отсутствие каких-либо критических отказов	10 миллионов часов эксплуатации; по крайней мере, два года эксплуатации как минимум десяти устройств в различных применениях; статистическая точность 99,9 %; подробное документирование всех изменений (включая мельчайшие) в период предыдущей эксплуатации
Испытания на устойчивость к пикам воздействий	—	Должна быть явно продемонстрирована более высокая устойчивость, чем устойчивость для граничных значений реальных режимов эксплуатации
Статический анализ	Проведение статического анализа блок-схем; выявление слабых точек; задание условий испытаний	Проведение статического анализа принципиальных схем; предсказание ожидаемого поведения систем при испытаниях; применение инструментальных средств испытаний
Динамический анализ	Анализ, основанный на блок-схемах; выявление слабых точек; задание условий испытаний	Анализ, основанный на подробных схемах; предсказание ожидаемого поведения в случаях испытаний; применение инструментальных средств испытаний
Анализ отказов	Анализ отказов на уровне модулей, включая анализ граничных данных периферийных устройств	Анализ отказов на уровне компонентов, включая анализ при граничных условиях
Анализ при наихудшем случае	Анализ наихудшего случая для функций безопасности; проводимый с использованием комбинаций граничных значений, соответствующих реальным условиям эксплуатации	Анализ наихудшего случая для функций, не относящихся к безопасности; проводимый с использованием комбинаций граничных значений, соответствующих реальным условиям эксплуатации
Расширенное функциональное тестирование	Проведение испытаний, при которых все функции безопасности проверяются при таких же статических входных состояниях, как и в случаях, вызванных процессами отказов, или условиями эксплуатации	Проведение испытаний, при которых все функции безопасности проверяются при таких же статических входных состояниях, и/или необычных входных изменениях, как и в случаях, вызванных процессами отказов, или условиями эксплуатации (включая те, которые могут возникать очень редко)
Испытания в наихудших случаях	Проведение испытаний, при которых функции безопасности проверяются для таких комбинаций граничных значений, какие встречаются в реальных условиях эксплуатации	Проведение испытаний, при которых функции, не связанные с безопасностью, проверяются для таких комбинаций граничных значений, какие встречаются в реальных условиях эксплуатации
Испытания с введением неисправностей	Проведение испытаний на уровне составляющих устройств, включая граничные данные периферийных устройств	Проведение испытаний на уровне компонентов, включая граничные данные

* В случаях применения этих методов/средств в качестве методов/средств с высоким уровнем эффективности предполагается, что они должны быть использованы и при низком уровне эффективности.

Приложение В
(справочное)

Охват диагностикой и доля безопасных отказов

В.1 Расчет охвата диагностикой и доли безопасных отказов

Охват диагностикой и долю безопасных отказов следует рассчитывать следующим образом:

а) реализовать режим отказа и провести анализ влияния для определения влияния отказов каждого вида каждого компонента или группы компонентов в подсистеме на действие E/E/PE СБЗС-системы в отсутствие диагностических проверок. Для проведения анализа влияния в наличии должна быть информация (см. примечания 1 и 2), достаточная для того, чтобы убедиться, что влияние видов отказов и результаты анализа этих влияний с достаточной степенью доверия соизмеримы с требованиями полноты безопасности.

Примечания

1 Для проведения анализа требуется следующая информация:

- подробная блок-схема E/E/PE СБЗС-системы, описывающая подсистемы с взаимосвязями для той части E/E/PE СБЗС-системы, которая затрагивает рассматриваемую(ые) функцию(ии) безопасности;
- схемные решения подсистем АС, описывающие каждый компонент или группу компонентов и взаимосвязи между компонентами;
- виды отказов и значения частоты (интенсивности) отказов для каждого компонента или группы компонентов и связанных с ними процентных отношений безопасных и опасных отказов к полной средней интенсивности отказов.

2 Требуемая строгость анализа влияния изменяется в зависимости от ряда факторов. При выборе строгости анализа должен быть принят во внимание уровень полноты безопасности рассматриваемых функций безопасности. Для более высоких уровней полноты безопасности предполагается, что виды отказов и анализ влияний будут очень специфичны в соответствии с конкретными типами компонентов и применяемым окружением системы. Очень важен полный и подробный анализ для подсистемы, которая должна использоваться в структуре АС, имеющей нулевую устойчивость к отказам АС;

б) категорировать каждый вид отказа по признаку, приводит ли он (в отсутствие диагностических испытаний):

- к безопасному отказу (т.е. не приводящему к снижению полноты безопасности E/E/PE СБЗС-системы, например, приводящий к безопасному отключению дополнительного источника света или не влияющий на полноту безопасности E/E/PE СБЗС-системы); или
- к опасному отказу (т.е. отказу, приводящему к отказу выполнения функции безопасности E/E/PE СБЗС-системой или ее частью, либо к невыполнению полноты безопасности E/E/PE СБЗС-системы);

в) вычислить вероятность безопасных отказов λ_S и вероятность опасных отказов λ_D, используя оценку вероятности отказов каждого компонента или группы компонентов λ (см. примечание 2 перечисления а) и примечание 1 настоящего перечисления) и результаты режимов отказов и анализа влияния для каждого компонента или группы компонентов.

Примечания

1Вероятность отказов каждого из компонентов или группы компонентов — это вероятность отказов λ, которые происходят в течение относительно небольшого промежутка времени t, в случаях, когда λ_i значительно меньше 1.

2 Интенсивность отказов каждого компонента или группы компонентов может быть оценена с использованием данных от признанного промышленного источника с учетом окружающей среды применения. Однако применение точных данных предпочтительнее, особенно в случаях, когда подсистема состоит из небольшого числа компонентов и когда любая ошибка в оценке вероятности безопасных и опасных отказов отдельного компонента могла бы иметь существенное влияние на оценку безопасной составляющей отказа;

г) для каждого компонента или группы компонентов оценить долю опасных отказов, которые могут быть обнаружены диагностическими тестами (см. приложение В.2) и, следовательно, частоту опасных отказов, обнаруженных диагностическими тестами λ_{DD};

д) для подсистемы вычислить полную вероятность опасных отказов $\Sigma\lambda_D$, полную вероятность опасных отказов, обнаруженных диагностическими тестами $\Sigma\lambda_{DD}$, и полную вероятность безопасных отказов $\Sigma\lambda_S$;

е) вычислить охват подсистемы диагностикой как $\Sigma\lambda_{DD} / \Sigma\lambda_D$;

ж) вычислить долю безопасных отказов подсистемы как $(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

Примечание — Охват диагностикой каждой подсистемы в E/E/PE СБЗС-системе должен учитываться в вычислении случайных отказов АС. Доля безопасных отказов должна приниматься во внимание при определении структурных ограничений на полноту безопасности аппаратных средств.

Анализ, используемый для вычисления охвата диагностикой и доли безопасных отказов, должен включать все компоненты, в том числе электрические, электронные, электромеханические, механические и т.п., которые используются в подсистеме для выполнения функции(ий) безопасности, реализуемых E/E/PE СБЗС-системой. Для каждого из компонентов должны быть рассмотрены все возможные виды опасных отказов, которые приводят к опасному состоянию, ограничивая диапазон безопасности, когда такой диапазон установлен или, иными словами, ставит под угрозу полноту безопасности E/E/PE СБЗС-системы.

В таблице А.1 приведены ошибки и отказы, которые как минимум должны быть обнаружены для достижения необходимого охвата диагностикой или которые как минимум должны быть включены в определение безопасной составляющей отказа.

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

В.2 Определение факторов охвата диагностикой

При вычислении охвата диагностикой для подсистемы (см. приложение В.1) для каждого компонента или группы компонентов необходимо оценить долю опасных отказов, которые обнаруживаются диагностическими тестами. Диагностические тесты, которые могут внести вклад в диагностический охват, включают в себя, но не ограничиваются такими мерами как:

- осуществление сравнительных проверок, например, контроля и сравнения избыточных (резервных) сигналов;

- применение дополнительных встроенных тестовых программ, например, осуществляющих вычисление контрольных сумм в устройстве памяти;

- проведение контроля с использованием внешних воздействий, например, путем пропускания импульсного сигнала через контролируемые тракты;

- осуществление непрерывного контроля аналогового сигнала, например, для обнаружения выхода за допустимые пределы уровней показаний сенсора.

Для вычисления охвата диагностикой необходимо определить виды отказов, которые обнаруживаются диагностическими тестами. Для простейших компонентов (резисторов, конденсаторов, транзисторов) отказы, связанные с разомкнутыми или короткозамкнутыми цепями, могут быть с большой степенью вероятности обнаружены путем стопроцентного охвата диагностикой. Однако для более сложных компонентов типа Б (см. 5.18.1.3) должны быть учтены ограничения охвата диагностикой для различных компонентов, указанных в таблице А.1. Этот анализ должен быть выполнен для каждого компонента или группы компонентов каждой подсистемы и для каждой E/E/PE СБЗС-системы.

Примечания

1 В таблицах А.2 — А.15 приведены рекомендуемые методы/средства, применяемые для диагностических проверок, и рекомендуемые максимальные охваты диагностикой, которые могут потребоваться. Эти проверки могут проводиться непрерывно или периодически (в зависимости от интервала диагностических проверок). Таблицы не заменяют любое из требований приложения В.

2 Диагностическое тестирование может обеспечить значительные выгоды в достижении функциональной безопасности E/E/PE СБЗС-систем. Однако, следует избегать излишнего увеличения сложности, которое может привести к увеличению трудностей при осуществлении действий по проверке, подтверждению соответствия, оценке функциональной безопасности, технической поддержке и модификации. Увеличение сложности может также затруднить долгосрочное поддержание функциональной безопасности E/E/PE СБЗС-систем.

3 При расчетах для получения необходимого охвата диагностикой и путей его реализации предполагается, что E/E/PE СБЗС-системы нормально работают при наличии другого опасного дефекта, который обнаружен диагностическими тестами. Если это предположение неверно, то E/E/PE СБЗС-систему следует рассматривать как систему, действующую в режиме с высокой частотой запросов или с непрерывным запросом (см. 5.11.3 и 5.8.2.5).

4 Диагностическое тестирование, используемое для обнаружения опасных отказов внутри подсистемы, может быть осуществлено другой подсистемой внутри E/E/PE СБЗС-системы.

5 Диагностические тесты могут действовать непрерывно или периодически в зависимости от интервала диагностических проверок. Возможны случаи или интервалы времени, когда запуск диагностического теста невозможен из-за того, что тестируемая система находится в неблагоприятном состоянии. Для таких случаев результаты расчета охвата диагностикой не являются корректными.

Приложение Г
(справочное)

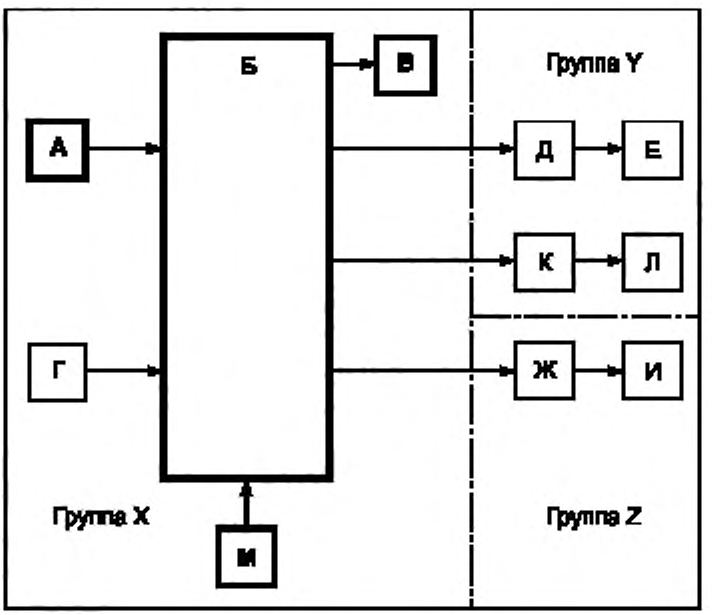
Состав и интеграция E/E/PE СБЗС-систем

Г.1 Состав систем

E/E/PE СБЗС-системы, перечень которых приведен в ГОСТ Р 53195.1 (подраздел А.2), состоят из различных составляющих (устройств, оборудования, систем, подсистем) и выполняют различные функции безопасности.

Г.1. 1 Системы тревожной сигнализации

Системы тревожной (пожарной, охранной, охранно-пожарной, аварийной и иной) сигнализации вне зависимости от вида опасности (природного, техногенного, антропогенного происхождения) строят по единому принципу из сходных по своему функциональному назначению составляющих (см. схему на рисунке Г.1). Человек может входить в состав системы тревожной сигнализации как составная часть.



Обозначения.

А — автоматический тревожный извещатель; Б — оборудование контроля и управления; В — устройство тревожной сигнализации; Г — ручной тревожный извещатель; Д — маршрутизатор сигналов тревоги; Е — внешний пульт приема сигналов тревоги; Ж — оборудование управления автоматическим средством защиты; И — автоматическое средство защиты; К — маршрутизатор сигналов неисправности системы тревожной сигнализации; Л — станция (пульт) приема сигналов неисправности системы тревожной сигнализации; М — источник питания

Рисунок Г.1 — Структурная схема системы тревожной сигнализации

Состав системы тревожной сигнализации: автоматические (А) и ручные (Г) тревожные извещатели; оборудование контроля и управления (Б); устройство (система) звукового оповещения об опасности (В), средства маршрутизации (передачи) сигналов тревоги (Д); станция (пульт) приема сигналов тревоги (Е); оборудование управления автоматическими средствами защиты (Ж), автоматические средства защиты (И); средства маршрутизации сигналов неисправности системы тревожной сигнализации (К); станция (пульт) приема сигналов неисправности системы тревожной сигнализации (Л); средства ведения и сохранения журнала тревожных событий и журнала неисправностей системы тревожной сигнализации (обычно входящие в состав оборудования контроля и управления); источник (источники) электропитания (М).

Основные функции безопасности: обнаружение опасного события — автоматическое или ручное извещение об опасном событии — передача сигнала извещения на вход оборудования контроля и управления — анализ (автоматическая обработка) сигнала извещения об опасном событии — формирование сигналов управления УО — передача сигналов управления на УО или систему управления УО — выполнение действия УО, снижающего риск и/или тяжесть последствий опасного события. Основным УО системы тревожной сигнализации служит оборудование системы оповещения об опасности. Снижение риска причинения вреда и тяжести последствий в результате реализации опасного события снижается благодаря своевременному оповещению людей об опасности, что позволяет им принять необходимые адекватные меры защиты.

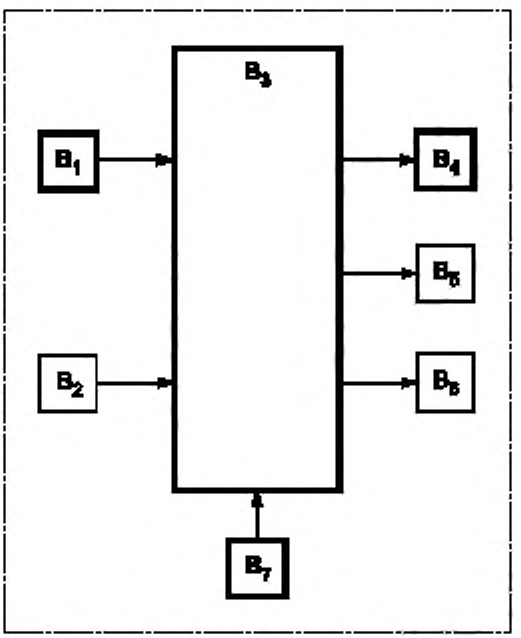
Расширение функций безопасности системы достигается путем доведения сигналов тревоги с помощью средства маршрутизации и станции приема сигналов тревоги до внешних служб поддержки, а также путем активизации УО автоматических средств защиты с помощью сигналов, подаваемых на оборудование управления средствами защиты.

В зависимости от назначения системы тревожной сигнализации и вида опасности в качестве УО могут быть использованы различные технические средства:

- в случае пожарной опасности — автоматические средства пожаротушения, дымоудаления, аварийного освещения и т.п.;
- в случае опасности несанкционированного вторжения — автоматические средства закрывания ворот, дверей системы контроля и управления доступом, иные защитные средства.

К системам тревожной сигнализации могут быть отнесены системы мониторинга конструкций и оборудования; системы контроля воздушно-газовой среды, уровня жидкости в бассейнах, давления в сосудах под давлением и другие системы, перечисленные в ГОСТ Р 53195.1 (раздел А.2 приложения А).

Оборудование А, Б, В, М и соединения АБ, БВ, МБ, показанные на рисунке Г.1 сплошной линией, всегда присутствуют в системе тревожной сигнализации. Оборудование и соединения, показанные штриховой линией, могут присутствовать в системе тревожной сигнализации. Группы оборудования, показанные на рисунке Г.1, имеют следующее назначение:



Обозначения.

B_1 — инициатор тревожного запуска; B_2 — ручное устройство вызова; B_3 — система контроля и управления звуком; B_4 — громкоговоритель; B_5 — визуальное устройство оповещения об опасности; B_6 — тактильное устройство оповещения об опасности; B_7 — источник электропитания (может быть использовано устройство М, рисунок Г.1)

Рисунок Г.2 — Структурная схема системы звукового оповещения об опасности

Группа X — управляемое оборудование, требующееся для местного оповещения об опасности;

Группа Y — управляемое оборудование, требующееся для оказания помощи извне;

Группа Z — управляемое оборудование, требующееся для реализации функции локальной защиты.

Примечание — Передача и прием сигналов тревожной сигнализации от защищаемых помещений (зон, территорий) и сигналов отказов системы тревожной сигнализации могут осуществляться по общему каналу связи.

Г.1.2 Системы звукового оповещения об опасности

В состав полной системы звукового оповещения об опасности (рисунок Г.2) в общем случае входят: средства инициирования тревожного запуска системы (B_1) (например, инициирующие элементы систем тревожной, пожарной, охранной сигнализации, систем мониторинга и др. либо ручные устройства вызова (B_2)); система контроля и управления звуком (B_3) (включая накопители сигналов оповещения, входящие в их состав); громкоговорители (звуковые оповещатели) (B_4); визуальные устройства оповещения об опасности (B_5); тактильные устройства оповещения об опасности (B_6); источник (источники) электропитания (B_7); средства ведения и сохранения журнала тревожных событий и журнала неисправностей.

Вибрационные тактильные устройства оповещения применяются дополнительно в составе систем звукового оповещения об опасности в случаях, когда на объекте могут находиться люди с пониженным зрением и слухом или шумовые характеристики и характеристики освещенности объекта затрудняют слуховое и зрительное восприятие звуковой и визуальной информации.

Оборудование и соединения, показанные на рисунке Г.2 сплошной линией, всегда присутствуют в системе звукового оповещения об опасности, а показанные штриховой линией — могут присутствовать в системе.

Системы звукового оповещения об опасности должны удовлетворять требованиям [1]. Одним из важных требований к системе звукового оповещения об опасности является наличие в ней средств автоматического мониторинга и отображения неисправностей во всех элементах системы — от микрофона вызывной станции до обмотки громкоговорителя, включая соединительные цепи между ними, и ПО системы контроля и управления звуком.

Г.1.3 Системы контроля и управления доступом

В состав системы контроля и управления доступом входят: автоматические идентификаторы, сенсоры, анализаторы сигналов; оборудование контроля и управления; устройства тревожной сигнализации; средства маршрутизации (передачи) сигналов тревоги; станция (пульт) приема сигналов тревоги; оборудование управления автоматическими средствами защиты; автоматические средства защиты; средства маршрутизации сигналов неисправности системы контроля и управления доступом; станция приема сигналов неисправности системы контроля и управления доступом; средства ведения и сохранения журнала тревожных событий и журнала неисправностей системы контроля и управления доступом; источник (источники) электропитания.

Г.1.4 Системы телевизионного наблюдения

В состав системы телевизионного наблюдения входят: телевизионные камеры (микрофоны), анализаторы сигналов; система обнаружения опасности (например, система тревожной сигнализации, система контроля и управления доступом и т.п.); оборудование контроля (отображения, идентификации) изображения, звука и управления; устройства тревожной сигнализации; средства маршрутизации (передачи) сигналов тревоги; станция (пульт) приема сигналов тревоги; оборудование управления автоматическими средствами защиты; автоматические средства защиты; средства маршрутизации сигналов неисправности системы телевизионного наблюдения; станция приема сигналов неисправности системы телевизионного наблюдения; средства записи, перезаписи, воспроизведения сигналов изображения, звука, данных; средства ведения и сохранения журнала тревожных событий и журнала неисправностей системы телевизионного наблюдения; источник (источники) электропитания.

Г.1.5 Системы интегрированные комплексные

В состав интегрированной комплексной системы безопасности (например, системы управления кризисными ситуациями, в том числе системы управления эвакуацией людей) входят: системы тревожной сигнализации (Г.1.1), система контроля и управления доступом (Г.1.3); система телевизионного наблюдения (Г.1.4); система звукового оповещения об опасности (Г.1.2); средства приема сигналов неисправности систем; оборудование (автоматизированное рабочее место) оператора центра контроля и управления; средства маршрутизации (передачи) сигналов тревоги; станция (пульт) приема сигналов тревоги; средства ведения и сохранения журналов тревожных событий, включая сигналы оповещения и действия операторов; средства ведения и сохранения журналов неисправностей (отказов) элементов интегрированной комплексной системы; источники электропитания.

На особо опасных, технически сложных и уникальных объектах управление кризисными ситуациями должно осуществляться из центров управления кризисными ситуациями (приложение Д).

Приложение Д
(справочное)

Организация центров управления кризисными ситуациями и размещение аппаратуры E/E/PE СБЗС-систем

Д.1 Основные понятия и общие положения

На особо опасных, технически сложных и уникальных объектах управление кризисными ситуациями должно осуществляться из центров управления кризисными ситуациями (далее — ЦУКС).

На других объектах по требованию заказчика управление кризисными ситуациями также может осуществляться из ЦУКС.

Настоящее приложение содержит общие положения по организации ЦУКС и принципам размещения в них аппаратуры контроля и управления E/E/PE СБЗС-систем.

Д.2 Принципы организация ЦУКС и общие требования

Д.2.1 ЦУКС должен быть организован на базе комплекта помещений управления, в которых размещается основное оборудование контроля и управления E/E/PE СБЗС-систем, дополнительное, вспомогательное оборудование и персонал для обеспечения централизованного управления системами, связанными с безопасностью.

Д.2.2 Помещения комплекта помещений безопасности, представляющие собой отдельные функциональные единицы, должны быть расположены в непосредственной близости от аппаратной управления и соответствовать их функциональному назначению.

Д.2.3 На стадии разработки концепции ЦУКС должны быть определены функциональные зоны, составляющие комплект помещений управления; оценены и установлены требования к пространству каждой функциональной зоны (например зоны управления, зоны администрации, зоны отдыха, зоны приема посетителей и т. п.); оценена пригодность запланированного участка (с учетом пространственных ограничений, местных опасностей, окружающей среды).

При этом должны быть предусмотрены помещения и участки следующего функционального назначения (см. рисунок Д.1):

- аппаратная управления,
- комната для собраний,
- комната со средствами обучения (тренинга),
- техническая аппаратная (с оборудованием),
- помещение технического обслуживания,
- комната отдыха персонала,
- участок приема пищи,
- кухня,
- раздевалки и туалеты,
- библиотека руководств и технической документации,
- инструментальная (участок с инструментами),
- комната для приема посетителей.

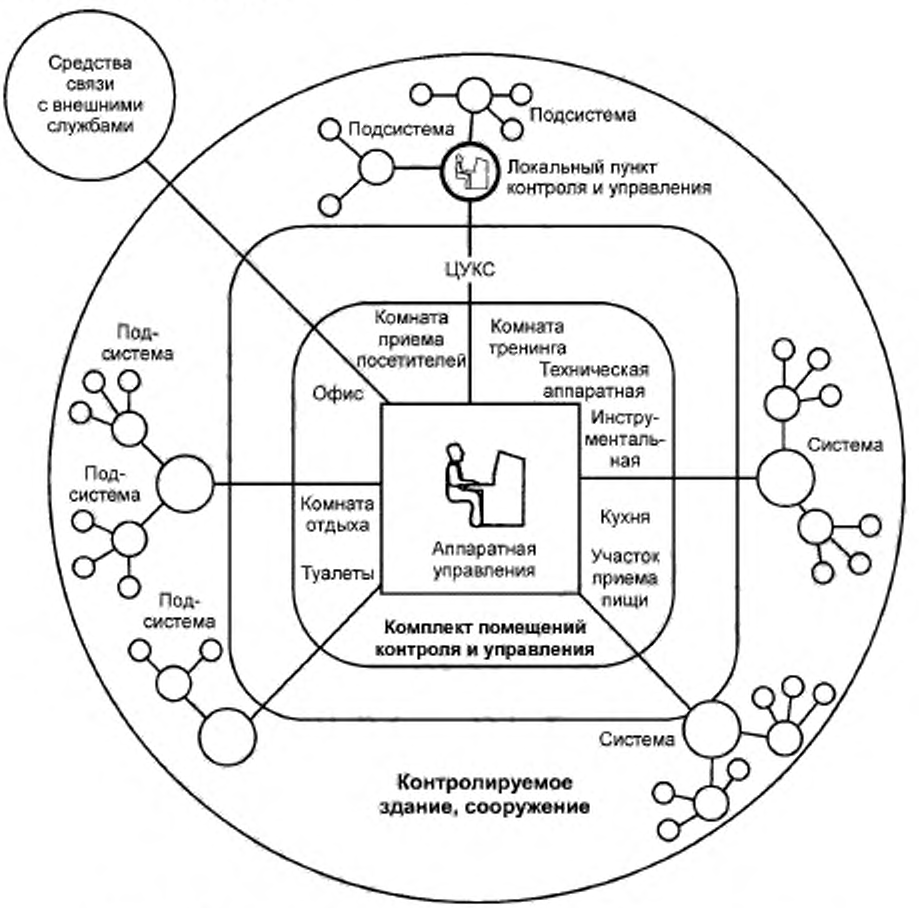


Рисунок Д.1 — Пример структуры центра управления кризисными ситуациями

Примечание — В зданиях и сооружениях, в которых предусмотрена служба физической защиты или другие внутренние службы защиты, в составе ЦУКС должны быть предусмотрены дополнительные помещения соответствующего функционального назначения, например, оружейная комната, склад средств химической защиты, пожарной защиты и т.п.

Д.2.4 При проектировании ЦУКС в зависимости от особенностей защищаемого здания и сооружения, характера предполагаемых угроз должны быть учтены:

- пригодность места расположения центра управления на объекте для обеспечения выполнения его задач;
- состав и численность персонала, режим работы;
- цели приема посетителей и максимальное возможное число посетителей;
- маршруты перемещения персонала и посетителей на территории ЦУКС, возможные ограничения доступа.

Дополнительно должны быть предусмотрены возможности:

- организации обучения и тренинга персонала;
- организации технического обслуживания;
- смены дежурного персонала без перерыва в работе;
- изменения режимов работы;
- контактов персонала вне аппаратной управления.

Д.2.5 Для управления безопасностью зданий и сооружений и обеспечения внешней поддержки должен быть предусмотрен двухсторонний обмен данными между ЦУКС и локальными пунктами контроля и управления объектом, а также между ЦУКС и постами внешних служб поддержки и администрирования: муниципальных и/или территориальных медицинских служб, служб МЧС, МВД, ФСБ, администрации.

Д.3 Требования к организации аппаратной управления

Д.3.1 При проектировании аппаратной управления должны быть определены:

- место, пригодное для размещения аппаратной;
- мебель и оборудование, которые должны быть размещены в аппаратной управления;
- эксплуатационные связи, которые должны быть обеспечены между позициями размещения аппаратуры и средств в аппаратной управления, включая позиции размещения персонала;
- требования к перемещению персонала и посетителей в пределах аппаратной управления;
- требования доступа к оборудованию и коммуникациям при техническом обслуживании.

Д.3.2 С учетом разных сроков службы оборудования, линий связи E/E/PE СБЗС-систем и системы конструкций зданий и сооружений при проектировании объекта должны быть выполнены следующие требования:

- каналы для прокладки линий связи и места доступа к ним должны быть устроены таким образом, чтобы была обеспечена возможность прокладки новых линий связи без извлечения существующих линий связи и прерывания работы существующего оборудования E/E/PE СБЗС-систем;
- должны быть предусмотрены пространства для размещения и ввода в действие нового оборудования E/E/PE СБЗС-систем без прерывания работы существующего оборудования, подлежащего замене в связи с завершением срока его эксплуатации;

Д.3.3 При планировании аппаратной управления должно быть учтено взаимное расположение как минимум следующих единиц оборудования и средств:

- автоматизированных рабочих мест (далее — АРМ);
- стоек с оборудованием;
- полок и стеллажей на АРМ и вне них;
- досок для объявлений и оперативных заметок;
- столов, картотечных блоков, информационных CD/DVD-блоков, книжных шкафов и т.п.;
- стендов (подставок) для принтера и других устройств оргтехники;
- входов в помещение и выходов из него.

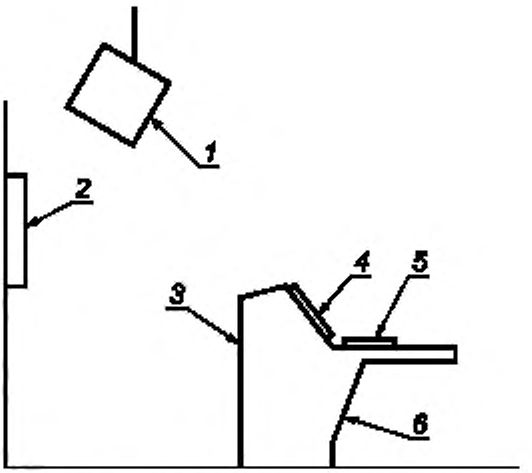
Д.3.4 Планируемое расположение оборудования и элементов должно обеспечить возможность:

- поддержания предусмотренной оперативной визуальной и вербальной связи между операторами (лицом к лицу);
- распределения оборудования между персоналом;
- индивидуальной работы операторов и работы группой (командой).

Д.3.5 В аппаратной управления должны быть предусмотрены свободные проходы к входам и выходам (необходимые в случае эвакуации персонала).

Д. 4 Требования к размещению оборудования и организации АРМ

Д.4.1 Размещение оборудования контроля и управления и организация АРМ с элементами контроля и управления (рисунок Д.2) должны осуществляться на основе эргономического проектирования.



1 — внешний дисплей; *2* — настенная панель управления; *3* — пульт контроля и управления; *4* — дисплей АРМ; *5* — панель управления; *6* — АРМ (включает 3, 4 и 5)

Рисунок Д.2 — Пример размещения средств контроля и управления на АРМ и вне него

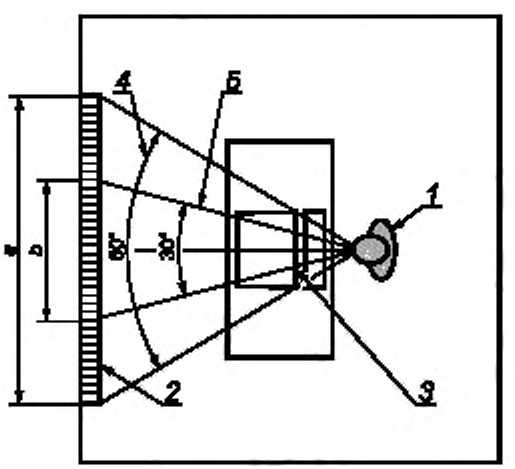
Д.4.2 При проектировании должны быть:

- проанализированы все задачи, которые должны выполняться оператором на АРМ при эксплуатации оборудования в обычном режиме, в критических ситуациях и при техническом обслуживании;
- идентифицированы необходимые функциональные элементы АРМ;
- определены необходимые размеры и положение АРМ.

При этом должны быть учтены все эргономические требования к следующим элементам:

- дисплеям,
- органам управления,
- рабочей области,
- устройствам связи,
- креслу,
- подлокотникам, подставке для ног.

Д.4.3 В дополнение к основным эргономическим требованиям (оптимальный угол обзора экрана (см. рисунок Д.3), подходящее устройство для действий по управлению и т.д.) особое внимание должно быть уделено когнитивным (познавательным) характеристикам, интенсивности потока информации, содержанию, качеству отображения поступающей информации и своевременному ее представлению.



1 — оператор; *2* — внешний экран; *3* — экран дисплея АРМ; *4* — угол обзора экрана; *5* — угол обзора рабочей зоны экрана

Рисунок Д.3 — Углы обзора экранов оператором

Примечание — Поскольку усталостные характеристики человека — оператора как части системы управления в значительной степени зависят от интенсивности потока информации и качества ее представления, необходимо стремиться к отображению на дисплеях только самой существенной информации. Детальную информацию следует отображать только по запросу оператора, а для отображения визуальной информации следует использовать дисплеи (мониторы) с высоким разрешением.

Д.4.4 При проектировании места расположения устройств и оборудования должны быть выбраны с учетом их размеров так, чтобы элементы оборудования не закрывали зону обзора оператора (см. рисунок Д.4).

Примечание — Для расчета мест расположения оборудования рекомендуется использовать антропометрические характеристики человека.

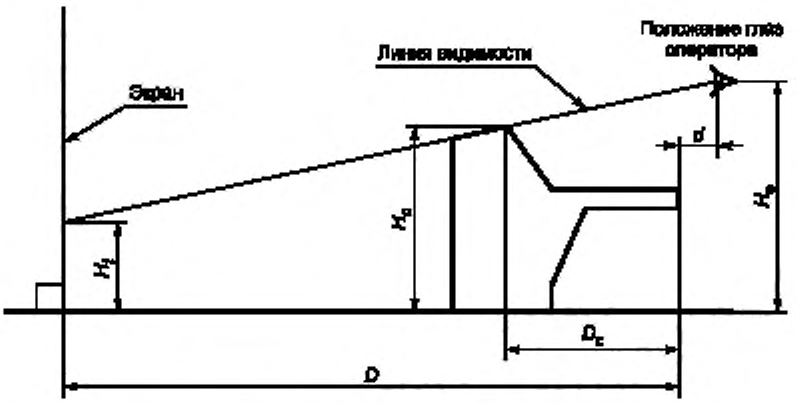


Рисунок Д.4 — Элементы оборудования АРМ

Пример — Расчет положения нижнего края экрана настенного дисплея (см. рисунок Д.4) может быть выполнен по формуле

$$H_l = H_c - (D + d)\,(H_e - H_c) / (D_c + d), \qquad (Д.1)$$

где H_l — наименьшая высота, на которой может быть виден внешний экран;

H_e — расчетное положение высоты глаз оператора, измеренное от поверхности пола до внешнего уголка глаза сидящего человека (приложение Е);

H_c — высота пульта управления;

D — расстояние по горизонтали между передним краем пульта управления и поверхностью настенного дисплея;

D_c — глубина пульта управления;

d — расстояние по горизонтали между расчетным положением глаз оператора и передним краем пульта управления.

Д.4.5 При расстановке оборудования и выборе мест доступа к коммуникациям в аппаратной управления должна быть предусмотрена возможность доступа к оборудованию и коммуникациям для осуществления их технического обслуживания, а также для уборки помещения.

Примечание — Для расчета мест расположения оборудования и доступа к коммуникациям следует использовать антропометрические характеристики человека (см. приложение Е).

Д.4.6 Строительные конструкции, основное, дополнительное и вспомогательное оборудование в аппаратной управления должно быть установлено так, чтобы не создавать помех перемещению операторов в аппаратной.

Д.4.7 При проведении расчетов размещения оборудования и АРМ в аппаратной управления и технической аппаратной должны быть проанализированы вербальные и визуальные связи операторов, возможные маршруты их перемещения и использованы антропометрические характеристики человека.

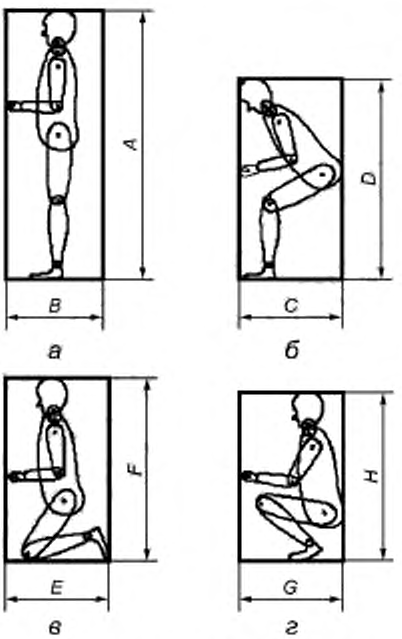
Д.4.8 При проектировании и реализации аппаратной управления должны быть предприняты акустические мероприятия по выравниванию в ней частотной зависимости времени реверберации для обеспечения приемлемой разборчивости речи.

Приложение Е
(справочное)

Применение антропометрических характеристик человека для расчетов аппаратных управления

Среднестатистические антропометрические характеристики относятся к двум группам населения земного шара. Первая группа, «высокорослых» людей, составляет 95 % населения; вторая группа, «низкорослых» людей составляет 5 % населения земного шара.

Минимальные размеры свободного пространства, необходимого для выполнения работ техником по техническому обслуживанию оборудования E/E/PE СБЗС-систем, находящегося в положениях, показанных на рисунке Е.1, приведены в таблице Е.1. Эти размеры должны быть приняты для расчетов при проектировании ЦУКС. Обозначение «p95» указывает, что данные относятся к группе «высокорослых» людей, к которым относится и основное население Российской Федерации.



а — положение стоя, *б* — полусогнутое положение; *в* — положение на коленях; *г* — положение на корточках

Рисунок Е.1 — Минимальные размеры пространств, необходимых для выполнения работ по техническому обслуживанию оборудования

Таблица Е.1 — Минимальные размеры свободного пространства для выполнения работ техником в зависимости от его положения

Обозначение размера свободного пространства	Минимальный требуемый размер, мм	Положение техника (p95) по обслуживанию оборудования, примечание
A	1910	Положение стоя, рисунок Е.1*а*
	30	Пространство для обуви, рисунок Е.1*а*
B	700	Положение стоя, рисунок Е.1*а*
C	1500	Положение согнувшись, рисунок Е.1*б*
D	1500	Положение согнувшись, рисунок Е.1*б*
E	760	Положение на коленях, рисунок Е.1*в*
F	1370	Положение на коленях, рисунок Е.1*в*
	30	Пространство для обуви, рисунок Е.1*в*
G	760	Положение на корточках, рисунок Е.1*г*
H	1220	Положение на корточках, рисунок Е.1*г*

Библиография

[1] ИСО 7240-16—2007 «Системы пожарной сигнализации. Часть 16. Управление звуковыми системами и средства индикации» (ISO 7240-16:2008 Fire detection and alarm systems — Part 16: Sound system control and indicating equipment)

УДК 621.5:814.8:006.354	ОКС	13.110; 13.220.01; 13.310; 13.320; 29.130.20; 35.240	Ж20	ОКП 43 7000 43 7100 73 7200 43 7280 70 3000

Ключевые слова: безопасность функциональная; связанные с безопасностью зданий и сооружений системы; требования к системам

Редактор *Л. И. Нахимова*
Технический редактор *В. Н. Прусакова*
Корректор *С. И. Фирсова*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 19.11.2009. Подписано в печать 17.02.2010. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 7,44. Уч.-изд. л. 6,90. Тираж 218 экз. Зак. 2347.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru